ISSN 2522-9842 (online)



Public organization
Ukrainian Scientific Community

Journal of Scientific Papers

Social Development *and* Security

Volume 15, Issue 2, April, 2025

OPEN ACCESS

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. of Law, Prof, Slovak Republic.
Mikhail **Divizinyuk,** 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 **Kurseeitov,** Dr. Sc. (Technical), Prof, Ukraine.
Ribeiro **Luís Frölén,** 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.
Курсеітов 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, Арменія.
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.
Волошенко 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	
NATO's New Force Model and Partner Engagement in an Evolving Security Landscape *Khayal Iskandarov, Piotr Gawliczek, Mahammad Akbarov*	1
Ukraine's Postwar Recovery Strategy: a Systemic Model for Integrating Economy, Governance, and Security *Oleh Semenenko, Ivan Havryliuk, Olexii Solomitsky, Yurii Kliat, Yuzef Dobrovolskyi, Alevtyna Hetman*	12
The Geopolitical Dynamics of Asia-Europe's Diplomatic Economic Relations in 21st Century: Opportunities and Challenges for Global Cooperation *Sarah Abdullah Alazwari*	20
Military Security	
Organization of the resistance movement in the territory of Ukraine and territory of the enemy country to counter the armed forces of the aggressor country *Oleg Sokolovsky*	41
Methodology for Implementing Artificial Intelligence Technologies in the Recruitment Process of the Armed Forces of Ukraine *Oleksandr Sampir, Ilona Sampir, Anna Fedorenko*	50
Adaptation of Fuel and Lubricant Logistics in Modern Warfare: Experience and Prospects for Ukraine *Andriy Ventsyuk, Oleksii Zaruchynskyi, Nadiya Burdeyna, Oleksandr Fedchenco*	63
Regulatory Framework for the Military Information Systems Support and Operation: Problems and Ways of Improvement *Andrii Diadechko, Galyna Rudenska*	74
Definition of a System of Indicators and Assessment Criteria for Military Service Under a Contract in the Armed Forces Taking Into Account the Level of Education *Denis Ivanin, Andrii Strepetov, Serhii Rudoi*	87
The Relativeness of Risks and Threats to Implementation of the (Military) Personnel Policy of Ukraine and the State of Israel Citizens in Terms of (Military) Training *Andrii Byelik*	95
Evolution of Chemical, Biological, Radiological and Nuclear Hazards. New Challenges and Threats National Security *Oleksii Solomytskyi, Andrii Bachynskyi*	119
Civil Security	
Emergency Evacuation Management System *Oleh Bashynskyi, Marta Peleshko, Taras Berezhanskyi, Andrii Beseda*	140
Improving the Method of Preventing Local Emergencies Based on the Results of Acoustic Space Monitoring *Vadym Tiutiunyk, Dmytro Usachov*	153
An Integrated Approach to Training Specialists in Critical Infrastructure Protection in Ukraine *Roman Yakovchuk, Vasyl Karabyn, Andrii Tarnavskyi*	165
Engineering and Technology	
Enhancing Methods of Protection in the Amazon Web Services Cloud with Artificial Intelligence and Machine Learning *Vitalii Molnar, Dmytro Sabodashko*	174

Application of Multimodal LLMs for Identifying Military Individuals in Mobile-Captured Images within Digital Forensics *Taras Fedynyshyn, Serhii Vysotskyi, Mariia Khomik, Oleksandr Hymza , Anastasia Vasylytsia, Bohdan Harasymchuk*	185
Study of the Vulnerabilities of the RSA Algorithm Through Factorization Attacks Implemented with Quantum Computing Techniques *Roman Shkliarskyy, Danyil Zhuravchak*	197
Study of the Influence of Generative Artificial Intelligence on the Analysis of Static Code Scanning Results Using the Bearer CLI Static Analyzer *Roman Zhyshko, Ihor Kos, Yelyzaveta Cheremnykh, Danyil Zhuravchak, Vitalii Susukailo*	208
Clustering and Classification of Enemy Group Targets Based on Neural Networks *Yurii Husak, Olha Vasylenko*	220
Analysis of Methods for Conducting Cloud Security Audits According to International Standards *Vladyslav Frankevych, Solomiia Dolishnia, Viktoriia Savchuk, Yevhenii Kurii, Vitalii Susukailo*	233
Social Sciences	
The Probability of the Military Potential Increase: Financial and Economic Factors *Oleksandr Ostapenko, Oles Koval*	248
Human Security at the Helm of the Socio-Economic Development *Primrose Thandekile Sabela, Mfundo Mandla Masuku, Mbongeni Shadrack, Livhuwani Ramphabana*	264
Analysis of Regulatory and Legal Documents on Internal Audit *Oleksandr Shpytal*	281
Improving the method of assessing the level of military threat based on the experience of the russian-ukrainian war *Mykola Tkach, Stanislav Slobodianyk, Igor Hablo, Natalia Honcharuk, Pavlo Makoshenets*	295
Resilience and Sustainability: Key Theoretical-Practical Narratives and War-Economic Lessons *Oleh Semenenko, Maryna Abramova, Oleh Tarasov, Serhii Mytchenko, Roman Dziubchuk, Denys Fomkin*	314
Psychological and Pedagogical Support for Children and Youth in Martial Law. Focus: Emotional Recovery, Safety in Education, Adaptation to Change *Oleh Semenenko, Lilia Semenenko, Oleksandr Vodchyts, Mariia Yarmolchyk, Stanislav Petrenko, Maksym Polyvoda*	327
On the Issue of Military Education Transformation in the Context of Military Specialists Training with Higher Education at the Tactical Level *Anatolii Loishyn*	336
The Global South as a Mega Subject of the New World Order *Sergii Mokliak, Nataliia Konopka*	350
Resilience of the Ukrainian Dairy Product Market In the Context of Achieving Sustainable Development Goals *Oleksandr Laiko*	358
Theoretical Platform for Integrating the Defense-Industrial Complex into the National Economic System *Volodymyr Koval*	379

ЗМІСТ

Національна безпека	
Нова модель сил НАТО та взаємодія партнерів у умовах мінливого безпекового ландшафту *Хаял Іскандаров, Пьотр Гавлічек, Мухаммед Акбаров*	1
Стратегія повоєнного відновлення України: системна модель інтеграції економіки, управління та безпеки *Олег Семененко, Іван Гаврилюк, Олексій Соломицький, Юрій Клят, Юзеф Добровольський, Алевтина Гетьман*	12
Геополітична динаміка дипломатичних економічних відносин між Азією та Європою у 21 столітті: можливості та виклики для глобальної співпраці *Сара Абдулла Алазварі*	20
Воєнна безпека	
Організація руху опору на території України та території країни противника для протидії збройним силам країни агресора *Олег Соколовський*	41
Методика впровадження технологій штучного інтелекту в процес рекрутингу в Збройних Силах України *Олександр Сампір, Ілона Сампір, Анна Федоренко*	50
Адаптація логістики пально-мастильних матеріалів в умовах сучасної війни: досвід та перспективи для України *Андрій Венцюк, Олексій Заручинський, Надія Бурдейна, Олександр Федченко*	63
Нормативне регулювання супроводження експлуатації інформаційних систем військового призначення: проблеми та шляхи вдосконалення *Андрій Дядечко, Галина Руденська*	74
Визначення системи показників та критерію оцінювання проходження військової служби за контрактом збройних сил з урахуванням рівня навченості *Денис Іванін, Андрій Стрепетов, Сергій Рудой*	87
Дотичність ризиків та загроз реалізації (військової) кадрової політики України та держави Ізраїль щодо (військової) підготовки громадян *Андрій Бєлік*	95
Еволюція хімічних, біологічних, радіологічних та ядерних небезпек. Нові виклики та загрози національній безпеці. *Олексій Соломицький, Андрій Бачинський*	119
Цивільна безпека	
Система управління евакуацією населення під час надзвичайних ситуацій *Олег Башинський, Марта Пелешко, Тарас Бережанський, Андрій Беседа*	140
Удосконалення методу запобігання виникненню надзвичайних ситуацій місцевого рівня за результатами моніторингу акустичного простору *Вадим Тютюник, Дмитро Усачов*	153
Інтегрований підхід до підготовки фахівців із захисту критичної інфраструктури в Україні *Роман Яковчук, Василь Карабин, Андрій Тарнавський*	165
Техніка і технології	
Покращення методів захисту у хмарному середовищі Amazon Web Services за допомогою штучного інтелекту та машинного навчання *Віталій Молнар, Дмитро Сабодашко*	174

Використання мультимодальних великих мовних моделей для цифрової криміналістики з метою виявлення військовослужбовців на зображеннях із мобільних пристроїв
Тарас Фединишин, Сергій Висоцький, Марія Хомік, Олександр Гимза, Анастасія Василиця, Богдан Гарасимчук 185

Дослідження вразливостей алгоритму RSA через атаки на факторизацію, реалізовані за допомогою квантових обчислень
Роман Шклярський, Даниїл Журавчак 197

Дослідження впливу генеративного штучного інтелекту на аналіз результатів статичного сканування коду за допомогою статичного аналізатора Bearer CLI
Роман Жишко, Ігор Кос, Єлизавета Черемних, Даниїл Журавчак, Віталій Сусукайло 208

Кластеризація та класифікація об'єктів групових цілей противника на основі нейронних мереж
Юрій Гусак, Ольга Василенко 220

Аналіз методів проведення аудиту безпеки хмарного середовища відповідно до міжнародних стандартів
Владислав Франкевич, Соломія Долішня, Вікторія Савчук, Євгеній Курій, Віталій Сусукайло 233

Суспільні науки

Ймовірність підвищення рейтингу військового потенціалу: фінансові та економічні фактори
Олександр Остапенко, Олесь Коваль 248

Безпека людини як визначальний чинник соціально-економічного розвитку
Примула Тандекіле Сабела, Мфундо Мандла Масуку, Мбонгені Шедрак, Livhuwani Ramphabana 264

Аналіз нормативно-правових документів з внутрішнього аудиту
Олександр Шпиталь 281

Удосконалення методу оцінювання рівня воєнної небезпеки з урахуванням досвіду російсько-української війни
Микола Ткач, Станіслав Слободяник, Ігор Хабло, Наталія Гончарук, Павло Макошенець 291

Резильєнтність і стійкість економіки: ключові теоретико-практичні наративи та воєнно-економічні уроки
Олег Семененко, Марина Абрамова, Олег Тарасов, Сергій Митченко, Роман Дзюбчук, Денис Фомкін 314

Психолого-педагогічна підтримка дітей і молоді в умовах воєнного стану. Фокус: емоційне відновлення, безпека в освіті, адаптація до змін
Олег Семененко, Лілія Семененко, Олександр Водчиць, Марія Ярмольчик, Станіслав Петренко, Максим Поливода 327

Щодо питання трансформації військової освіти в контексті підготовки військових фахівців з вищою освітою на тактичному рівні
Анатолій Лойшин 336

Глобальний Південь як мегасуб'єкт нового світового порядку
Сергій Мокляк, Наталя Конопка 350

Резільєнтність ринку молочних продуктів України в контексті досягнення цілей сталого розвитку
Олександр Лайко 358

Теоретична платформа інтеграції оборонно-промислового комплексу в загальнонаціональну економічну систему
Володимир Коваль 379

NATO's New Force Model and Partner Engagement in an Evolving Security Landscape

Нова модель сил НАТО та взаємодія партнерів у умовах мінливого безпекового ландшафту

Khayal Iskandarov [A]
Corresponding author: PhD in National Security and Military Sciences, e-mail: xayal1333@gmail.com, ORCID: 0000-0001-8975-6530

Piotr Gawliczek [B]
PhD, Assoc. Prof., e-mail: pgawliczek@gmail.com, ORCID: 0000-0002-0462-1168

Mahammad Akbarov [A]
e-mail: xayal1333@gmail.com, ORCID: 0009-0007-6863-9707

[A] War College of the Armed Forces, Republic of Azerbaijan
[B] University of Warmia and Mazury, Poland

Хаял Іскандаров [A]
Corresponding author: К. наук з національної безпеки та військових наук, e-mail: xayal1333@gmail.com, ORCID: 0000-0001-8975-6530

Пьотр Гавлічек [B]
Доктор філософії, доцент, e-mail: pgawliczek@gmail.com, ORCID: 0000-0002-0462-1168

Мухаммед Акбаров [A]
e-mail: xayal1333@gmail.com, ORCID: 0009-0007-6863-9707

[A] Військовий коледж Збройних Сил, Азербайджан
[B] Вармінсько-Мазурський університет, Польща

Received: February 25, 2025 | Revised: Aprile 15, 2025 | Accepted: Aprile 30, 2025

DOI: 10.33445/sds.2025.15.2.1

Purpose: is to justify the importance of partner engagement in the new model against the backdrop of ever-changing security environment. The hypothesis of the paper is that partner engagement plays a crucial role in ensuring the effectiveness of NFM within the evolving security environment. The paper tries to find answers to the following research questions: 1. What role do NATO's partners play in the New Force Model, and why is their engagement important? 2. What benefits and challenges do partner nations face when engaging with NATO under the NFM?

Method: Qualitative research methods, such as Comparative Analysis, Synthesis and Case Studies.

Theoretical implications: The theoretical implications of this paper lie in its contribution to the broader discourse on alliance dynamics, military interoperability, and cooperative security frameworks. By examining partner engagement within NATO's NFM, the study enhances our understanding of how non-member states contribute to and benefit from NATO's partnership initiatives. The paper bridges gaps in the literature by addressing the underexplored aspects of partner engagement within the NFM. It offers a foundation for future research on the role of partnerships in NATO's NFM in an increasingly complex and unpredictable global landscape.

Practical implications: The practical implications of this paper extend to policymaking, military strategy, and international security cooperation. By analyzing partner engagement within NATO's NFM, the study provides insights that can guide NATO and its partner nations in enhancing collaboration, interoperability, and strategic alignment. The study can serve as a reference for defense planners and decision-makers by identifying best practices for military cooperation and joint operational readiness.

Paper type: theoretical.

Key words: NATO, transformation, New Force Model, Old Force Model, NRF, ARF, PAF-N, partner.

Мета дослідження: обґрунтувати важливість участі партнерів у новій моделі сил (NFM) на тлі постійно змінного безпекового середовища. Гіпотеза статті полягає в тому, що залучення партнерів відіграє вирішальну роль у забезпеченні ефективності NFM в умовах еволюції системи безпеки. У дослідженні поставлено такі запитання: 1. Яку роль відіграють партнери НАТО в Новій моделі сил і чому їхня участь є важливою? 2. Які вигоди та виклики постають перед країнами-партнерами у процесі взаємодії з НАТО в межах NFM?

Метод дослідження: якісні методи дослідження, зокрема порівняльний аналіз, синтез та кейс-стаді.

Теоретична цінність дослідження: полягає у внеску до ширшого наукового дискурсу щодо динаміки альянсів, військової взаємосумісності та рамок кооперативної безпеки. Дослідження участі партнерів у NFM НАТО сприяє кращому розумінню того, як держави-партнери, що не є членами Альянсу, роблять внесок у партнерські ініціативи НАТО та отримують з них користь. Робота заповнює прогалини в науковій літературі, аналізуючи маловивчені аспекти партнерської участі в межах NFM, і формує підґрунтя для подальших досліджень ролі партнерства в NFM НАТО в умовах дедалі складнішого та менш передбачуваного глобального середовища.

Практична цінність дослідження: значення статті поширюється на сфери вироблення політики, військової стратегії та міжнародної безпекової співпраці. Аналізуючи участь партнерів у NFM НАТО, дослідження надає висновки, які можуть бути корисними для НАТО та його партнерів у зміцненні співробітництва, взаємосумісності та стратегічної узгодженості. Результати дослідження можуть слугувати орієнтиром для військових планувальників і політичних керівників, визначаючи найкращі практики військової кооперації та спільної оперативної готовності.

Тип статті: теоретичний.

Ключові слова: НАТО, трансформація, Нова модель сил, Стара модель сил, NRF, ARF, PAF-N, партнер.

Introduction

NATO has undergone significant transformations since the collapse of the communist regimes in Europe, particularly in integrating various partners into its structures. To adapt to the post-Cold War era and strengthen its crisis management capabilities, NATO prioritized the development of

multinational force projection by adopting a New Strategic Concept in 1991. Achieving future strategic objectives required NATO to expand its cooperation beyond traditional borders, underscoring the urgent need to engage with partners. This approach made collaboration between partner and member forces essential for out-of-area operations (Nasirov & Iskandarov, 2017). Partnership frameworks such as the Partnership for Peace and the Mediterranean Dialogue emerged as key initiatives, fostering cooperation with neighboring countries and supporting their efforts to enhance national capabilities. Over the ensuing years, the Alliance initiated new partnership frameworks (such as the Istanbul Cooperation Initiative and Partners Across the Globe) in order to expand its geographical reach and engage with different partners to build cooperative security together. Subsequently, NATO introduced new programs and mechanisms (Operational Capabilities Concept, Membership Action Plan, DEEP, Individual Partnership Action Plan, etc.) for closer and deeper cooperation with its partners (Iskandarov et al., 2023). To adapt to the evolving security environment, NATO has successfully implemented its transformation process by adopting new Strategic Concepts approximately every ten years. This evolution, along with its support for various regions, has enabled the Alliance to benefit from the financial and military capabilities of its partner countries in efforts to combat terrorism, promote stability beyond Europe, and engage in operations in Kosovo, Afghanistan, and Iraq.

Numerous academic studies examine NATO's transformation and partnership policies, tracing its shift from a Cold War alliance to a global security actor. Throughout history, many prominent figures have both supported and opposed NATO enlargement, underscoring the continued relevance of this issue. John S. Duffield (1994) explores the factors contributing to NATO's resilience and continued relevance in the immediate aftermath of the Cold War. Jamie Shea (2012) examines NATO's role in a vastly different geopolitical landscape following the fall of the Berlin Wall in 1989. Ruiz Palmer (2019) discusses NATO's post-Cold War transformation, outlining its objectives, achievements, and challenges. Andrea Gilli et al. (2020) focus on the Alliance's technological advancements.

Several studies on NATO's transformation and partnerships highlight the competition for power and influence across different regions. In particular, Khayal Iskandarov and Piotr Gawliczek analyze Russia's security interests in relation to NATO's enlargement policy and assess how NATO's partnership mechanisms enhance cooperation in education and force interoperability (Nasirov & Iskandarov, 2017; Sadiyev & Iskandarov, 2018; Iskandarov & Gawliczek, 2018; Hasanov et al., 2019; Iskandarov, 2019a; Iskandarov, 2019b; Iskandarov et al., 2019b; Iskandarov & Gawliczek, 2019; Iskandarov & Gawliczek, 2020; Iskandarov & Gawliczek, 2021; Iskandarov et al., 2023).

Additionally, the book *NATO 2030: Towards a New Strategic Concept and Beyond*, edited by Jason Blessing et al. (2021), offers fresh perspectives on NATO's evolving threat landscape, shifting internal dynamics, and the transformation of warfare, providing insights into the Alliance's future strategic direction.

A number of studies focus on NATO's New Force Model (NFM), analyzing its impact on the Alliance's defense posture in response to emerging security threats. For example, Zoltan Szenes (2023) analyzes NATO's evolving approach to deterrence and defense, assessing planned measures and comparing the 2010 and 2022 Strategic Concepts. He argues that the latter has ushered NATO into a new era of great power competition. Similarly, a report by Sean Monaghan et al. (2024) evaluates allied efforts to reinforce collective defense in response to new threats. The report poses a crucial question: while NATO may be prepared for the onset of conflict, is it adequately equipped to endure and ultimately succeed in a prolonged war? Based on commitments made at the Madrid Summit, the report assesses NATO's readiness to sustain and prevail in extended conflicts.

John R. Deni (2024) explores the rationale behind the introduction of the NFM and outlines its core components, including force organization, management, and command-and-control structures. Meanwhile, Jacopo Maria Bosica (2024) examines the key features of the NFM,

highlighting its improvements and distinctions from the previous model. He argues that the NFM enhances the rapid deployment capabilities of European Allies, allowing them to defend themselves without having to wait for U.S. leadership.

Nicolò Fasola (2024) contends that NATO's evolving mission is not sufficiently addressed by its current partnership policies, processes, and mechanisms. Given the ongoing global competition, he suggests that NATO should rethink its approach to partner engagement to better align with its strategic objectives. Beyond offering a critical analysis of NATO's cooperative security policies, Fasola also proposes ways to modernize the Alliance's partnership mechanisms.

The literature review reveals that the prospects and challenges of partner engagement within the NFM have not yet been studied. The purpose of this paper is to justify the importance of partner engagement in the new model against the backdrop of an ever-changing security environment.

Results

Partner Engagement in the New Force Model: Current and Future Prospects

As expressed in all four of the post-Cold War Strategic Concepts, NATO's goal is to collectively safeguard security. The three core tasks of NATO, as stated in the present Strategic Concept (2022), are crisis prevention and management, cooperative security, and deterrence and defense. Among these, cooperative security primarily involves partnerships. Consequently, cooperative security encompasses several components: building partnerships, supporting non-proliferation, disarmament, and arms control, and assisting prospective new NATO members in their accession process. Ensuring interoperability is a crucial aspect of building partnerships and preparing new nations for NATO membership (Nasirov & Iskandarov, 2017). In short, the new NATO missions and engagements in operational theatres have led to a dramatic shift from individual nations fighting alone to coalitions where multinational units—even down to the platoon level—work together. The current Strategic Concept also underscores the critical role that partners play in maintaining peace and stability across Europe, the Middle East, North Africa, and the Indo-Pacific, as well as the importance of partner states in strengthening the Alliance's resilience against current and emerging security threats. Additionally, it reiterates that strengthening practical cooperation and political-military interaction with partners enables them to interoperate more effectively with Allied forces in pursuit of NATO's core tasks (Fasola, 2024).

The NFM, unveiled at the Madrid Summit in June 2022, marks a key transformation in NATO's military framework to address emerging security challenges, particularly following the onset of the Russia-Ukraine war. This model significantly strengthens the Alliance's defense strategy, emphasizing rapid deployment and scalable forces across member nations. The NFM prioritizes integrated operations across multiple domains—including land, air, sea, cyber, and space—ensuring NATO can address threats across different regions and operational environments simultaneously. This framework combines national forces maintained at high readiness with multinational NATO forces capable of deploying together. Experts such as Sven Biscop (2022) and Jacopo Maria Bosica (2024) suggest that the NFM will grant the Supreme Allied Commander Europe (SACEUR) greater discretion in contingency operational planning, thereby enhancing NATO's overall agility and effectiveness.

Some may argue that NATO's adoption of a new force model was unnecessary, considering Russia's declining power since its engagement in a large-scale war with Ukraine. However, an important reality remains: regardless of how well-prepared an army might be, forces with real combat experience are invariably more formidable than those without. The Russian military applied lessons learned from its operations in Syria to further its objectives in Ukraine. Without this prior experience, Russia would likely have faced greater difficulty sustaining its momentum against

Ukraine's determined resistance (Hasan et al., 2024). Thus, despite its losses, it would be unwise to assume that Russia will remain weak in the near or long term. According to Global Firepower 2024, Russia continues to possess the world's second most powerful military (globalfirepower.com, 2024). The simple answer to this issue is that NATO now faces a higher risk of direct conflict with Russia than at any time since the Soviet Union's collapse. The perceived threat is especially acute for allies bordering Russia, prompting major changes in force structure, defense spending, operational planning, and overall foreign and security policies (Hooker, 2024). Additionally, Russia has managed to double its military budget despite experiencing only modest economic growth (Hooker, 2024).

NATO's NFM represents a significant evolution in the Alliance's approach to collective defense and deterrence. It aims to provide a more robust and scalable force structure, thereby enhancing NATO's ability to respond swiftly to emerging threats. The NFM also allows partner nations to augment NATO forces in specific regions or roles, further enhancing flexibility. The NFM ensures deeper integration of partner nations' forces into NATO's operational plans. Partners contribute considerably to NATO by providing extensive regional and cultural knowledge, specialized skills and capabilities, and access to staging locations, which enhance the Alliance (Andrews, 2024). NATO, in turn, has much to offer its partners. Partner forces are now viewed as a critical component of NATO's overall capacity, especially in augmenting high-readiness forces. These changes ensure that NATO is better prepared to respond quickly and effectively to modern security challenges, with a larger and more agile force structure capable of addressing both conventional and unconventional threats. NATO can achieve its strategic objectives by fostering partnerships driven by a proactive, long-term vision backed by committed resources, sustained engagement, and resilience. Ensuring flexibility, responsiveness, and adaptability is essential, with measurable activities aligned to clear benefits and metrics. To maintain relevance and agility, NATO should reassess legacy arrangements, strengthen ongoing cooperation, and establish clear baselines for long-term partnerships. Additionally, granting NATO authorities greater autonomy in collaborating with partners and non-NATO entities could enhance the effectiveness of these engagements (Andrews, 2024).

Partner countries, in turn, will continue to support the Alliance in the future at the aforementioned tiers and in all three tasks. The participation of partner countries in NATO operations will remain one of the fundamental principles of the Alliance. However, partner engagement in NATO activities has faced challenges and inconsistencies over the past decades, largely influenced by the geostrategic location of each partner. According to Nicolò Fasola (2024), the lack of progress between NATO and its partners can generally be attributed to several key factors:

1. A lack of enthusiasm among partners for deeper cooperation;
2. Limited domestic funding to support NATO-related engagement;
3. Insufficient capacities to fully benefit from NATO training opportunities and
4. Challenges in identifying qualified personnel for essential cooperation activities and bilateral discussions.

We could introduce the sensitivity of geostrategic locations of partner nations as a fifth factor, since security challenges vary significantly among regions. For instance, the South Caucasus countries face entirely different security concerns compared to Austria and Switzerland. Furthermore, NATO's expanding membership and evolving responsibilities have created significant challenges in allocating adequate resources to help partners address regional security issues effectively.

In the new force model, the mechanism ensuring partner engagement is called the Partner Augmentation Force-N (PAF-N). While participation in this concept does not impose any automatic obligations or commitments on a nation joining it, it offers extensive access to NATO programs, mechanisms, training, and exercises. During peacetime, PAF-N units will train with NATO, focusing on multidomain and multinational training to enhance interoperability and maintain operational flexibility. In crisis prevention or management scenarios, with North Atlantic Council (NAC) approval, PAF-N units may reinforce NATO forces deployed in a crisis area or contribute to any NATO-led

response operation during crises or conflicts. Additionally, PAF-N units can provide support to Allied forces engaged in ongoing NATO operations, missions, and activities.

In general, joining the PAF-N concept is a lengthy process that encompasses four stages:

1. Political acceptance and military assessment;
2. Political (NAC) approval;
3. PAF-N preparation (including caveats and conditions);
4. Force tailoring (according to NATO requirements).

Although the tasks of the NATO Response Force (NRF) were diverse and participation was determined on a case-by-case basis through agreements between NATO and partner countries, the PAF-N concept appears more attractive to partners—particularly those in politically sensitive regions—because it mitigates associated risks. The main tasks in the new force model will largely align with those of the NRF. However, while joining the NRF was a sensitive decision for countries not seeking NATO membership, participation in the PAF-N concept—or declaring a unit to the PAF-N Pool of Forces—provides a more flexible and less politically sensitive alternative. For instance, if a partner country expresses its intention to join the PAF-N concept and successfully completes the first three stages, it retains full discretion in phase four, as the PAF-N does not impose automatic obligations. A partner country may choose to contribute at a specific tier (e.g. Tier 3, 30–180 days), and even then, participation in any operation would still require a separate agreement between NATO and the partner country. Further augmentation of the ARF or any tier (1, 2, or 3) within the PAF-N concept will be implemented in close coordination with allies, Joint Force, and Single Service Commands through individual agreements with partners.

Units declared to the PAF-N Pool of Forces may be used for the following purposes:

1. Participation in selected NATO exercises in support of NATO's core task of Deterrence and Defense;
2. Supporting NATO efforts to respond to or manage an ongoing crisis, including crisis deployment, non-combatant evacuation operations, humanitarian assistance, and limited embargo operations;
3. Supporting a NATO operation or mission;
4. Increasing interoperability and developing cooperation with NATO forces through capacity building and military exercises;
5. Strengthening NATO forces in deterrence and defense;
6. Strengthening NATO response operations, missions, and activities (subject to NAC agreement) in support of the core tasks of crisis prevention and management and collective security.

As evident from the list, the range of tasks that a declared unit can undertake within the PAF-N Pool of Forces is extensive and diverse.

In an increasingly contested global environment, both NATO and its strategic competitors naturally seek prospective partners, often with differing objectives. This dynamic introduces the potential for conflict, making a deliberate and strategic approach essential. NATO must carefully assess the purpose of such partnerships, balancing their risks and benefits. A key decision lies in whether to cultivate beneficial yet non-exclusive partnerships to outmaneuver adversaries or insist on exclusivity, which could potentially restrict adversaries' access to the same partners (Andrews, 2024). The NRF concept used to be a source of irritation for NATO's rivals, as it underscored NATO's rapid deployment capabilities and its commitment to collective defense, thereby challenging the strategic ambitions of its adversaries. A quick review of the partners involved in the NRF Concept shows examples such as Georgia, Ukraine, Jordan, and Bosnia and Herzegovina. Of these, Georgia and Ukraine are uniquely positioned between NATO and its prominent strategic rival, Russia. It is abundantly clear what transpired in Georgia in 2008 and what has been unfolding in Ukraine since 2014; consequently, it is not surprising that any other country situated in such a sensitive geographic region and joining the NRF Concept would likely face a similar fate. The NATO PAF-N Concept

effectively mitigates the risks posed by NATO's rivals to its partners. As evident from its title, the PAF-N Concept indicates that partner participation augments NATO missions and operations. Partners have been enhancing and contributing to NATO operations for decades, demonstrating the value of collaboration in achieving shared security objectives. The PAF-N Concept will formalize and provide a framework for this longstanding contribution and collaboration, ensuring its alignment with NATO's strategic objectives. This arrangement may appeal to certain prospective partners who have reservations about fully aligning with NATO while offering flexibility along the partnership spectrum, thereby allowing individual nations greater freedom in their level of engagement (Andrews, 2024).

What does joining the PAF-N concept promise for partners? Considering that NATO has a 30-year history of a successful partnership policy, and during this period, partners have contributed to NATO's operations and missions, most of them currently do not participate in any NATO operation. This will inevitably have a negative effect on active cooperation because every effective cooperation is developed on the principle of reciprocity. NATO has proved its dedication to partnerships for decades, which in turn facilitated the incorporation of new members after the end of the Cold War as many as 16 countries, which account for 50 percent of overall NATO membership today. The best example is the case of Finland and Sweden, which had the longest preparation for integration and the shortest incorporation process.

As already mentioned, NATO's main focus should definitely be on collective security, defence, and deterrence. However, since security is indivisible, NATO is obliged to take stock of each and every security threat — both immediate and long-term — beyond its traditional or physical boundaries in order to project stability globally. This, in turn, highlights NATO's third core task: cooperative security. NATO's priorities for extensive partnerships are essential for strengthening its collective security and addressing global challenges. This policy promotes peace and stability in many areas by fostering interoperability, resilience, and capacity-building.

As already noted, interoperability between NATO and its partners is a cornerstone of the Alliance's ability to operate effectively in complex, multinational environments and to respond to security challenges with coordinated efforts. Therefore, the main focus of NATO's partnerships is on the improvement of interoperability with partners, which in turn encourages partner engagement in NATO-led activities.

In general, participation in NATO's activities is realized mainly on the basis of specific priorities. Currently, the following four (4) priorities apply:

Priority 1: In support of a NATO mission/operation;

Priority 2: In support of a High Readiness Force, e.g., NRF;

Priority 3: In support of a NATO (PSP) Position;

Priority 4: Professional Development / all other activities.

Having considered the first priority we may say that the number of partners participating in NATO missions has considerably decreased. There are three active operations and missions of NATO in which 9 partners are Operational partners – KFOR (Armenia, Austria, Ireland, Moldova, Switzerland), Operation Sea Guardian (Georgia) and NMI (Austria and Australia). However, the past operations, such as ISAF and Operation Unified Protector are the perfect examples where the interoperability of forces proved successful. Approximately 20 out of overall 51 nations in ISAF and 5 out of 18 nations in Operation Unified Protector were partners. It was Operation Unified Protector, where Sweden – the most recent member of NATO tested its capabilities at the technical, tactical and operational levels. Regarding the second priority alone, only four countries – Georgia, Ukraine, Jordan, and Bosnia and Herzegovina were part of the NRF. Now, three of them, excluding Ukraine, have transitioned to the PAF-N Concept. Given that NATO has 35 partners, this number is relatively small in comparison The third priority emphasizes partner contributions to NATO HQs. Several partners, such as Azerbaijan, Austria, Bosnia and Herzegovina, Colombia, Georgia, Republic of Korea, Switzerland and Ukraine, contribute to various NATO HQs, with the number of officers ranging from

a minimum of one (Colombia, Georgia, Republic of Korea, Switzerland) to a maximum of seven (Azerbaijan). Apart from it some nations contribute to different entities, such as NATO Defence College (Azerbaijan, Kuwait), NATO School Oberammergau (Austria, Switzerland, Bosnia and Herzegovina), etc., which support NATO education and training. However, this priority also remains limited compared to the total number of NATO partners. All nations may apply the last priority and take part in NATO courses, including seminars, workshops, exercises, and similar activities. However, this priority is obviously less significant than the first.

NATO remains the most effective military organization for enhancing interoperability both with and among its partners, despite political bureaucracy and conflicting interests among member states. It provides highly efficient tools that deliver tangible results within a specific timeframe. However, the extent of every cooperation depends on mutual benefits, and while NATO actively supports its partners, it does so in alignment with its own strategic interests. Therefore, it is crucial for partners to recognize these priorities and integrate them into their foreign policy strategies.

Conclusion

The adoption of the NFM has significantly transformed NATO's strategy for crisis response, deterrence, and collective defense. The model reaffirms the Alliance's capacity to react swiftly to new threats. Additionally, expanding alliances with non-member nations will be essential to enhancing NATO's strategic influence. Increased cooperation in training and exercises, intelligence sharing, and capacity-building initiatives will guarantee that partner countries successfully support regional and international stability. In the end, NATO's New Force Model's effectiveness will rely on member states' shared political will and level of adaptation. Additionally, while the NRF Concept in the Old Force Model exposed the nations with close proximity to NATO's adversaries to heightened political pressure, economic sanctions, or other forms of coercion and included only three partner nations, the PAF-N concept will involve more, as its notion and framework reduce the risks for those particular nations. To ensure the stability and security of the Euro-Atlantic region, NATO must remain committed to partnerships while strengthening its defensive posture in response to the evolving security environment. The PAF-N concept is an indispensable tool in achieving this goal, as it enhances force integration, improves operational readiness, and strengthens interoperability among allied and partner nations, ensuring a more cohesive and effective military response to emerging security challenges.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

Andrews, D. (2024). Improving NATO's Out-Partnering Function in *Alliances and Partnerships in a Complex and Challenging Security Environment*, R. Karp & R. W. Maass (Eds.). SACT NATO HQ, pp. 169-177. Available at: https://www.act.nato.int/wp-content/uploads/2024/06/NATO-AC24-Compendium.pdf (Accessed: January 31, 2025).

Biscop, S. (2022, September). *The New Force Model: NATO's European army?* (Egmont Policy Brief No. 285). Egmont Institute. Available at: https://www.egmontinstitute.be/app/uploads/2022/09/Sven-Biscop_PolicyBrief285_vFinal.pdf (Accessed: February 11, 2025).

Blessing, J., Elgin, K. K., & Ewers Peters, N. M. (Eds.). (2021). *NATO 2030: Towards a new strategic concept and beyond.* Foreign Policy Institute / Henry A. Kissinger Center for Global Affairs, Johns Hopkins University SAIS. Available at: https://sais.jhu.edu/sites/default/files/NATO2030AndBeyondAccessibleVersion.pdf (Accessed: January 11, 2025).

Bosica, J.M. (2024). *NATO's new force model: A watershed step for the alliance's deterrence, defence and crisis management missions in a complex Euro-Atlantic security landscape.* Atlantic Forum. Available at: https://www.atlantic-forum.com/atlantica/natos-new-force-model-a-watershed-step-for-the-alliances-deterrence-defence-and-crisis-management-missions-in-a-complex-euro-atlantic-security-landscape. (Accessed: January 20, 2025).

Deni, J.R. (2024). *The new NATO force model: Ready for launch?* NATO Defense College. Available at: http://www.jstor.org/stable/resrep60400 (Accessed: January 30, 2025).

Duffield, J. S. (1994). NATO's Functions after the Cold War. *Political Science Quarterly*, *109*(5), pp. 763–787. https://doi.org/10.2307/2152531

Edelman, E. S., Manning, D., & Miller, F. C. (2024, March 12). NATO's decision process has an Achilles' heel. Atlantic Council. Available at: https://www.atlanticcouncil.org/blogs/new-atlanticist/natos-decision-process-has-an-achilles-heel/ (Accessed: February 6, 2025).

Fasola, N. (2024). *Reforming and enhancing partnerships to strengthen NATO's strategic posture.* U.S. Army War College. Available at: https://publications.armywarcollege.edu/News/Display/Article/3974674/reforming-and-enhancing-partnerships-to-strengthen-natos-strategic-posture (Accessed: January 13, 2025).

Gilli, A., Gilli, M., Leonard, A.-S., & Stanley-Lockman, Z. (2020). "NATO-mation": preparing for technological transformation. In *"NATO-Mation": Strategies for Leading in the Age of Artificial Intelligence* (pp. 25–28). NATO Defense College. doi: http://www.jstor.org/stable/resrep27711.10

Global Firepower. (2024). *2024 military strength ranking: Russia.* Available at: https://www.globalfirepower.com/country-military-strength-detail.php?country_id=russia.

Hasan, A.H., Iskandarov, K., & Gawliczek, P. (2024). Azerbaijan's 2023 counterterrorism operation in Karabakh region: causes and consequences. *Social Development and Security*, *14*(3), pp. 1-13. doi: https://doi.org/10.33445/sds.2024.14.3.1.

Hasanov, A.H., Iskandarov, K.I., & Sadiyev, S.S. (2019). The evolution of NATO's cyber security policy and future prospects. *Journal of Defense Resources Management*, *10*(1), pp. 94-106. Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~2949059&id=GALE%7CA629148092&v=2.1&it=r&sid=googleScholar&asid=b1df5f56 (Accessed: January 30, 2025).

Hooker, R.D. (2024). *A new NATO command structure.* Atlantic Council. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2024/05/A-New-NATO-Command-Structure.pdf (Accessed: January 29, 2025).

Iskandarov, K. (2019a). NATO enlargement vis-a-vis Russian security policy (1999-2019) in *Security and Russian threats,* pp. 37-70. Uniwersytet Jana Kochanowskiego w Kielcach.

Iskandarov, K. (2019b). *The South Caucasus-NATO Cooperation*. LAP LAMBERT Academic Publishing.

Iskandarov, K., & Gawliczek, P. (2018). NATO's role in improving professional military education with a focus on the south Caucasus countries. *The Quarterly Journal*, *18*(3-4), 35-44. https://doi.org/10.11610/Connections.18.3-4.02

Iskandarov, K., & Gawliczek, P. (2020). The "new great game" in the South Caucasus: competition for power and influence. *Social Development and Security*, *10(1)*, pp. 25-33. https://doi.org/10.33445/sds.2020.10.1.4

Iskandarov, K., & Gawliczek, P. (2019). The south Caucasus and NATO's defence education enhancement programme. Retrospective analysis. *Social development and Security*, 9(5), pp. 3-14. https://doi.org/10.33445/sds.2019.9.5.1

Iskandarov, K., & Gawliczek, P. (2021). The south Caucasus and NATO's defence education enhancement programme. The measurement of its effectiveness. *Social Development and Security*, *11*(1), pp. 70-79. https://doi.org/10.33445/sds.2021.11.1.7

Iskandarov, K., Gawliczek, P., Mrozek, J. (2023). *NATO's partnership policy in a dynamic security landscape: A simple look at a complex picture*. Olsztyn: Centre for Eastern Europe Research UWM in Olsztyn.

Iskandarov, K., Mammadzada, V., Sadiyev, S. (2019a). 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.ceeol.com/search/article-detail?id=812186 (Accessed: February 11, 2025).

Iskandarov, K., Simons, G., & Gawliczek, P. (2019b). The South Caucasus: Stage for a 'New Great Game' between NATO and Russia?. *Connections: The Quarterly Journal*, *18*, pp. 3-4. doi: https://doi.org/10.11610/Connections.18.3-4.01.

Monaghan, S., Jakobsen, E., Martinez, S., Droin, M., Sanders, G., Velazquez, N., Cook, C., Dowd, A., & Sockwell, M. (2024). *Is NATO ready for war?* Center for Strategic and International Studies. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-06/240611_Monaghan_Ready_War_0.pdf (Accessed: January 26, 2025).

Nasirov, E., & Iskandarov, K. (2017). The prospects of Azerbaijan to enhance military interoperability with NATO. *Connections*, *16*(4), pp. 89-99. Available at: https://www.jstor.org/stable/26867928 (Accessed: January 12, 2025).

Palmer, D. A. R. (2019). NATO's post-Cold War "out-of-area" pivot (1990-2014). In *A Strategic Odyssey: Constancy of Purpose and Strategy-Making in NATO, 1949-2019* (pp. 73–90). NATO Defense College. http://www.jstor.org/stable/resrep19967.11

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: 01.02.2025).

Shea, J. (2012). *Keeping NATO Relevant*. Carnegie Moscow Center. Available at: http://www.jstor.org/stable/resrep26708

Szenes, Z. (2023). Reinforcing deterrence: assessing NATO's 2022 Strategic Concept. *Defense & Security Analysis*, *39*(4), pp. 539–560. https://doi.org/10.1080/14751798.2023.2270230 (Accessed: January 11, 2025).

Список використаних джерел

Andrews, D. (2024). Improving NATO's Out-Partnering Function in *Alliances and Partnerships in a Complex and Challenging Security Environment*, R. Karp & R. W. Maass (Eds.). SACT NATO HQ, pp. 169-177. Available at: https://www.act.nato.int/wp-content/uploads/2024/06/NATO-AC24-Compendium.pdf (Accessed: January 31, 2025).

Biscop, S. (2022, September). *The New Force Model: NATO's European army?* (Egmont Policy Brief No. 285). Egmont Institute. Available at: https://www.egmontinstitute.be/app/uploads/2022/09/Sven-Biscop_PolicyBrief285_vFinal.pdf (Accessed: February 11, 2025).

Blessing, J., Elgin, K. K., & Ewers Peters, N. M. (Eds.). (2021). *NATO 2030: Towards a new strategic concept and beyond.* Foreign Policy Institute / Henry A. Kissinger Center for Global Affairs,

Johns Hopkins University SAIS. Available at: https://sais.jhu.edu/sites/default/files/NATO2030AndBeyondAccessibleVersion.pdf (Accessed: January 11, 2025).

Bosica, J.M. (2024). *NATO's new force model: A watershed step for the alliance's deterrence, defence and crisis management missions in a complex Euro-Atlantic security landscape.* Atlantic Forum. Available at: https://www.atlantic-forum.com/atlantica/natos-new-force-model-a-watershed-step-for-the-alliances-deterrence-defence-and-crisis-management-missions-in-a-complex-euro-atlantic-security-landscape. (Accessed: January 20, 2025).

Deni, J.R. (2024). *The new NATO force model: Ready for launch?* NATO Defense College. Available at: http://www.jstor.org/stable/resrep60400 (Accessed: January 30, 2025).

Duffield, J. S. (1994). NATO's Functions after the Cold War. *Political Science Quarterly*, *109*(5), pp. 763–787. https://doi.org/10.2307/2152531

Edelman, E. S., Manning, D., & Miller, F. C. (2024, March 12). NATO's decision process has an Achilles' heel. Atlantic Council. Available at: https://www.atlanticcouncil.org/blogs/new-atlanticist/natos-decision-process-has-an-achilles-heel/ (Accessed: February 6, 2025).

Fasola, N. (2024). *Reforming and enhancing partnerships to strengthen NATO's strategic posture.* U.S. Army War College. Available at: https://publications.armywarcollege.edu/News/Display/Article/3974674/reforming-and-enhancing-partnerships-to-strengthen-natos-strategic-posture (Accessed: January 13, 2025).

Gilli, A., Gilli, M., Leonard, A.-S., & Stanley-Lockman, Z. (2020). "NATO-mation": preparing for technological transformation. In *"NATO-Mation": Strategies for Leading in the Age of Artificial Intelligence* (pp. 25–28). NATO Defense College. doi: http://www.jstor.org/stable/resrep27711.10

Global Firepower. (2024). *2024 military strength ranking: Russia.* Available at: https://www.globalfirepower.com/country-military-strength-detail.php?country_id=russia.

Hasan, A.H., Iskandarov, K., & Gawliczek, P. (2024). Azerbaijan's 2023 counterterrorism operation in Karabakh region: causes and consequences. *Social Development and Security*, *14*(3), pp. 1-13. doi: https://doi.org/10.33445/sds.2024.14.3.1.

Hasanov, A.H., Iskandarov, K.I., & Sadiyev, S.S. (2019). The evolution of NATO's cyber security policy and future prospects. *Journal of Defense Resources Management*, *10*(1), pp. 94-106. Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~2949059&id=GALE%7CA629148092&v=2.1&it=r&sid=googleScholar&asid=b1df5f56 (Accessed: January 30, 2025).

Hooker, R.D. (2024). *A new NATO command structure.* Atlantic Council. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2024/05/A-New-NATO-Command-Structure.pdf (Accessed: January 29, 2025).

Iskandarov, K. (2019a). NATO enlargement vis-a-vis Russian security policy (1999-2019) in *Security and Russian threats,* pp. 37-70. Uniwersytet Jana Kochanowskiego w Kielcach.

Iskandarov, K. (2019b). *The South Caucasus-NATO Cooperation*. LAP LAMBERT Academic Publishing.

Iskandarov, K., & Gawliczek, P. (2018). NATO's role in improving professional military education with a focus on the south Caucasus countries. *The Quarterly Journal*, *18*(3-4), 35-44. https://doi.org/10.11610/Connections.18.3-4.02

Iskandarov, K., & Gawliczek, P. (2020). The "new great game" in the South Caucasus: competition for power and influence. *Social Development and Security*, *10(1)*, pp. 25-33. https://doi.org/10.33445/sds.2020.10.1.4

Iskandarov, K., & Gawliczek, P. (2019). The south Caucasus and NATO's defence education enhancement programme. Retrospective analysis. Social development and Security, 9(5), pp. 3-14. https://doi.org/10.33445/sds.2019.9.5.1

Iskandarov, K., & Gawliczek, P. (2021). The south Caucasus and NATO's defence education enhancement programme. The measurement of its effectiveness. *Social Development and Security*, *11*(1), pp. 70-79. https://doi.org/10.33445/sds.2021.11.1.7

Iskandarov, K., Gawliczek, P., Mrozek, J. (2023). *NATO's partnership policy in a dynamic security landscape: A simple look at a complex picture*. Olsztyn: Centre for Eastern Europe Research UWM in Olsztyn.

Iskandarov, K., Mammadzada, V., Sadiyev, S. (2019a). 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.ceeol.com/search/article-detail?id=812186 (Accessed: February 11, 2025).

Iskandarov, K., Simons, G., & Gawliczek, P. (2019b). The South Caucasus: Stage for a 'New Great Game' between NATO and Russia?. *Connections: The Quarterly Journal*, *18*, pp. 3-4. doi: https://doi.org/10.11610/Connections.18.3-4.01.

Monaghan, S., Jakobsen, E., Martinez, S., Droin, M., Sanders, G., Velazquez, N., Cook, C., Dowd, A., & Sockwell, M. (2024). *Is NATO ready for war?* Center for Strategic and International Studies. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-06/240611_Monaghan_Ready_War_0.pdf (Accessed: January 26, 2025).

Nasirov, E., & Iskandarov, K. (2017). The prospects of Azerbaijan to enhance military interoperability with NATO. *Connections*, *16*(4), pp. 89-99. Available at: https://www.jstor.org/stable/26867928 (Accessed: January 12, 2025).

Palmer, D. A. R. (2019). NATO's post-Cold War "out-of-area" pivot (1990-2014). In *A Strategic Odyssey: Constancy of Purpose and Strategy-Making in NATO, 1949-2019* (pp. 73–90). NATO Defense College. Available at: http://www.jstor.org/stable/resrep19967.11

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: 01.02.2025).

Shea, J. (2012). *Keeping NATO Relevant*. Carnegie Moscow Center. Available at: http://www.jstor.org/stable/resrep26708

Szenes, Z. (2023). Reinforcing deterrence: assessing NATO's 2022 Strategic Concept. *Defense & Security Analysis*, *39*(4), pp. 539–560. https://doi.org/10.1080/14751798.2023.2270230 (Accessed: January 11, 2025).

Стратегія повоєнного відновлення України: системна модель інтеграції економіки, управління та безпеки

Ukraine's postwar recovery strategy: a systemic model for integrating economy, governance, and security

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

Іван Гаврилюк [B]
к. військ. наук, старший дослідник, перший заступник Міністра оборони України, e-mail: ivan_havryliuk@ukr.net, ORCID: 0000-0002-3514-0738

Олексій Соломицький [A]
д. військ. наук, старший науковий співробітник, начальник відділу, e-mail: solosa1@gmail.com, ORCID: 0000-0001-8061-8895

Юрій Клят [A]
к. тех. наук., доцент, начальник Центрального науково-дослідного інституту Збройних Сил України, e-mail: klyatt@ukr.net, ORCID: 0000-0002-8267-3748

Юзеф Добровольський [C]
к. тех. наук., доцент, заступник начальника кафедри з навчальної роботи – начальник навчальної частини кафедри військової підготовки, e-mail: kataza@i.ua, ORCID: 0000-0002-1077-1402

Алевтина Гетьман [D]
старший науковий співробітник, e-mail: getman2017@gmail.com, ORCID: 0000-0002-6397-7412

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

Ivan Havryliuk [B]
Ph.D., associate professor, First Deputy Minister of Defense of Ukraine, e-mail: ivan_havryliuk@ukr.net, ORCID: 0000-0002-3514-0738

Olexii Solomitsky [A]
Dr of Military Sciences, Senior Research Fellow, Head of Department, e-mail: solosa1@gmail.com, ORCID: 0000-0001-8061-8895

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

Юзеф Добровольський [C]
Candidate of Technical Sciences, Associate Professor, Deputy Head of the Department of Academic Affairs – Head of Training Department of Military Training, e-mail: kataza@i.ua, ORCID: 0000-0002-1077-1402

Alevtyna Hetman [D]
Senior Research Fellow, e-mail: getman2017@gmail.com, ORCID: 0000-0002-6397-7412

[A] Центральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна
[B] Міністерство оборони України, Київ, Україна
[C] Кафедра військової підготовки Національного авіаційного університету, Київ, Україна
[D] Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна

[A] Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine
[B] Ministry of Defense of Ukraine, Kyiv, Ukraine
[C] Department of Military Training of the National Aviation University, Kyiv, Ukraine
[D] Military Institute of Telecommunications and Informatization named after Heroes of Kruty, Kyiv, Ukraine

Received: April 11, 2025 | Revised: April 20, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.2

Мета роботи: визначення основних етапів та заходів повоєнного відновлення України.

Метод дослідження: використовувалися системний аналіз, експертне опитування, порівняльно-історичний метод, контент-аналіз нормативно-правової бази, метод моделювання сценаріїв та SWOT-аналіз.

Практична цінність дослідження: запропоновано структуровану модель поетапного післявоєнного відновлення України, яку можна використовувати як основу для державного планування, розробки національних політик, координації міжнародної допомоги та оцінки ефективності реалізації заходів у сферах економіки, безпеки й управління.

Тип статті: теоретична.

Purpose: to identify the main stages and measures of post-war recovery of Ukraine.

Method: systematic analysis, expert survey, comparative historical method, content analysis of the legal framework, scenario modeling method and SWOT analysis were used.

Practical implications: a structured model of the phased post-war recovery of Ukraine is proposed, which can be used as a basis for state planning, development of national policies, coordination of international assistance and evaluation of the effectiveness of measures in the areas of economy, security and governance.

Paper type: theoretical.

Ключові слова: повоєнне відновлення, національна безпека, етапи відбудови, інституційна стійкість, міжнародна допомога, економіка, розвиток, відновлення.

Key words: post-war reconstruction, national security, stages of reconstruction, institutional stability, international assistance, economy, development, recovery.

Вступ

Україна зіткнеться з одним із найскладніших викликів у своїй новітній історії — післявоєнним

відновленням. Внаслідок збройної агресії російської федерації було зруйновано або пошкоджено значну частину критичної інфраструктури, промислових об'єктів, житлового фонду, а також порушено соціальну й економічну стабільність у багатьох регіонах. Станом на 2025 рік Україна зіткнулася з необхідністю одночасного проведення термінової реконструкції та стратегічної трансформації державного управління, економіки, оборонного сектора й суспільних інститутів.

Комплексне бачення та структуроване планування цього процесу є ключовими для формування сталого миру, відновлення державного суверенітету, а також інтеграції України в європейське безпекове, правове та економічне середовище. У цьому контексті важливою є систематизація заходів відновлення з урахуванням досвіду інших країн, адаптації найкращих практик та розробки власної моделі, яка відповідатиме особливостям національного безпекового й політичного ландшафту.

Теоретичні основи дослідження

Питання повоєнного відновлення широко досліджується як вітчизняними, так і зарубіжними науковцями. Значну увагу цьому приділено у звітах Світового банку, Програми розвитку ООН та Київської школи економіки, де наголошується на потребі у прозорості, децентралізації управління коштами донорів, а також стійкості інституційної моделі відбудови [1, 2]. Досвід повоєнного відновлення Німеччини, Японії, Південної Кореї вивчали українські аналітики, зокрема у працях І. Гриценка та О. Мельника, які акцентують на необхідності координації між секторами безпеки, економіки та правосуддя [3; 4]. Дослідники відзначають важливість впровадження принципів "build back better", як це реалізовано в міжнародних програмах з подолання наслідків збройних конфліктів (UNDP, USAID), із пріоритетами на відбудову людського капіталу, цифрової трансформації та безпеки [5, 6].

Різноманітні аспекти повоєнного відновлення також розглядаються у працях [7–16].

Постановка проблеми

Мета статті полягає у розробленні пропозицій щодо створення гнучкої, але структурованої системи реалізації заходів відновлення, що враховує ризики, міжнародний досвід і особливості поточного безпекового середовища України.

Результати

Повоєнне відновлення України є складним, багаторівневим процесом, який охоплює не лише фізичну реконструкцію зруйнованої інфраструктури, а й глибокі трансформації в економічній, соціальній, інституційній та безпековій сферах. Успішна реалізація цього завдання вимагає чіткого визначення пріоритетів, координації між органами влади, громадянським суспільством і міжнародними партнерами, а також ефективного використання ресурсів. Порядок організації заходів відновлення України пропонується прив'язати до змісту Законів України, а саме: Закон України від 12.05.2015 № 389-VIII "Про правовий режим воєнного стану"; Закон України від 06.12.1991 № 1932-XI "Про оборону України"; Закон України від 21.10.1993 № 3543-XII "Про мобілізаційну підготовку та мобілізацію".

Повоєнне відновлення України після підписання домовленостей щодо припинення вогню доцільно розбити на три етапи (рис. 1, рис. 2):

підготовчий етап – етап переходу з воєнного стану (або до кінця особливого періоду) в період відновлення основних сфер діяльності країни (відбудовчий період – відповідно до нормативно-правової бази не має офіційного визначення в згаданих Законах України). Цей період охоплює кінцеву стадію воєнного стану та частину відбудовного періоду;

відновлювальний етап – це етап безпосереднього відновлення (відбудови) країни після закінчення підготовчого етапу та досягнення певної стабілізації зовнішньої воєнно-політичної та воєнно-економічної обстановки навколо держави;

перехідний етап – це етап переходу від стану відбудовного періоду до стану мирного часу, тобто коли держава понад 70-80% здатна функціонувати сама без значної допомоги та впливу інших держав на її зовнішньо та внутрішньо політичний курс.

На (рис. 1–2) наведено, за досвідом відновлення інших країн після війн та збройних конфліктів, можливі часові проміжки тривалості того чи іншого періоду із урахуванням загроз національній безпеці України. Перехід до наступного етапу має відбуватися за умови практичної реалізації 80% зазначених основних та хоча б 60-70% другорядних заходів відновлення на попередньому етапі.

Найбільш важливими основними та другорядними заходами за напрямами є:

Економічний напрям

Основні заходи:

пошук гарантій (досягнення домовленостей) економічної підтримки державами-партнерами для зменшення негативних наслідків закінчення війни, а саме: припинення військової та гуманітарної допомоги; значна інфляція або дефолт; неспроможність утримувати на достатньому рівні необхідну чисельність сил оборони; продовольча та промислова криза внаслідок втрати ринків збуту;

стабілізація або нарощування людського капіталу, а саме: впровадження нормативно-правових актів щодо мінімізації міграції, а особливо еміграції населення країни після припинення воєнних дій та відміни режиму воєнного стану;

створення чіткого плану відновлення ключових інфраструктурних об’єктів, які є основою наповнення Державного бюджету України та спрощення умов ведення малого та середнього бізнесу на період відновлення.

Другорядні заходи:

пошук шляхів інвестицій в національну економіку держави як країн-партнерів, так і країн з нейтральним статусом. Надання пріоритетів інвестування в розвиток економіки України як в податковій сфері, так і нормативно-правовому полі;

створення умов щодо можливості часткового відновлення людського капіталу держави через повернення іммігрантів шляхом популяризації можливості їх соціальної підтримки та нормативно-правової захищеності;

пошук шляхів першочергового забезпечення сімей загиблих військовослужбовців житлом, а також формування програми забезпечення військовослужбовців, які зазнали каліцтва, та учасників бойових дій житлом;

недопущення зниження рівня економічної та соціальної захищеності військово-службовців в суспільстві, бо це є пряма загроза дестабілізації обстановки всередині країни тощо.

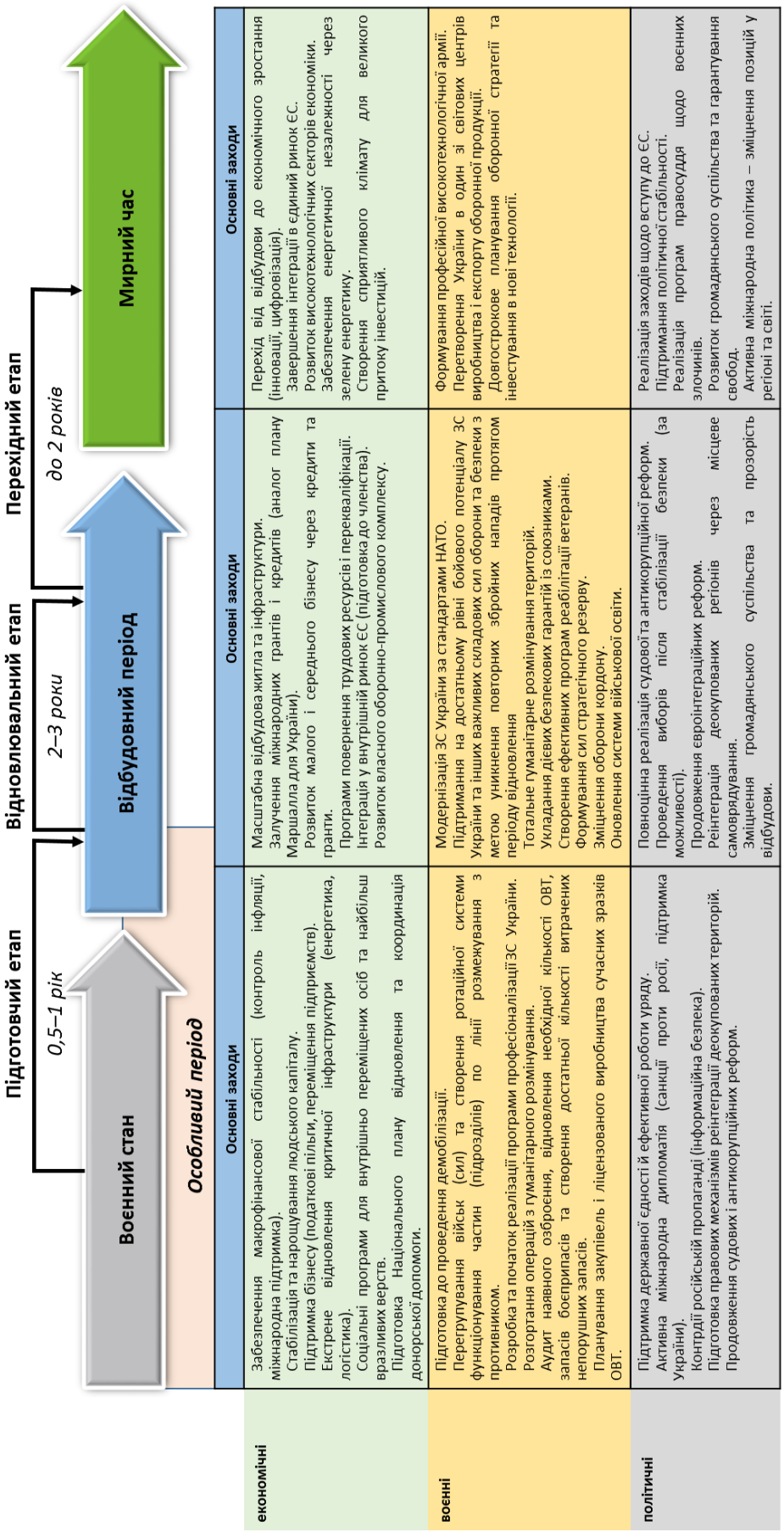
Військовий напрям

Основні заходи:

підтримання на достатньому рівні бойового потенціалу Збройних Сил України та інших важливих складових сил оборони та безпеки з метою уникнення повторних збройних нападів протягом періоду відновлення (не менше 2-3 роки);

відновлення необхідної кількості озброєння та військової техніки; запасів боєприпасів та створення достатньої кількості витрачених непорушних запасів;

перегрупування військ (сил) та створення ротаційної системи функціонування частин (підрозділів) по лінії розмежування з противником;



	Основні заходи	Основні заходи	Основні заходи
економічні	Забезпечення макрофінансової стабільності (контроль інфляції, міжнародна підтримка). Стабілізація та нарощування людського капіталу. Підтримка бізнесу (податкові пільги, переміщення підприємств). Екстрене відновлення критичної інфраструктури (енергетика, логістика). Соціальні програми для внутрішньо переміщених осіб та найбільш вразливих верств. Підготовка Національного плану відновлення та координація донорської допомоги.	Масштабна відбудова житла та інфраструктури. Залучення міжнародних грантів і кредитів (аналог плану Маршалла для України). Розвиток малого і середнього бізнесу через кредити та гранти. Програми повернення трудових ресурсів і перекваліфікації. Інтеграція у внутрішній ринок ЄС (підготовка до членства). Розвиток власного оборонно-промислового комплексу.	Перехід від відбудови до економічного зростання (інновації, цифровізація). Завершення інтеграції в єдиний ринок ЄС. Розвиток високотехнологічних секторів економіки. Забезпечення енергетичної незалежності через зелену енергетику. Створення сприятливого клімату для великого притоку інвестицій.
воєнні	Підготовка до проведення демобілізації. Перегрупування військ (сил) та створення ротаційної системи функціонування частин (підрозділів) по лінії розмежування з противником. Розробка та початок реалізації програми професіоналізації ЗС України. Розгортання операцій з гуманітарного розмінування. Аудит наявного озброєння, відновлення необхідної кількості ОВТ, запасів боєприпасів та створення достатньої кількості витратних непорушних запасів. Планування закупівель і ліцензованого виробництва сучасних зразків ОВТ.	Модернізація ЗС України за стандартами НАТО. Підтримання на достатньому рівні бойового потенціалу ЗС України та інших важливих складових сил оборони та безпеки з метою уникнення повторних збройних нападів протягом періоду відновлення Тотальне гуманітарне розмінування територій. Укладання дієвих безпекових гарантій із союзниками. Створення ефективних програм реабілітації ветеранів. Формування сил стратегічного резерву. Зміцнення оборони кордону. Оновлення системи військової освіти.	Формування професійної високотехнологічної армії. Перетворення України в один зі світових центрів виробництва і експорту оборонної продукції. Довгострокове планування оборонної стратегії та інвестування в нові технології.
політичні	Підтримка державної єдності й ефективної роботи уряду. Активна міжнародна дипломатія (санкції проти росії, підтримка України). Контрдії російській пропаганді (інформаційна безпека). Підготовка правових механізмів реінтеграції деокупованих територій. Продовження судових і антикорупційних реформ.	Повноцінна реалізація судової та антикорупційної реформ. Проведення виборів після стабілізації безпеки (за можливості). Продовження євроінтеграційних реформ. Реінтеграція деокупованих регіонів через місцеве самоврядування. Зміцнення громадянського суспільства та прозорість відбудови.	Реалізація заходів щодо вступу до ЄС. Підтримання політичної стабільності. Реалізація програм правосуддя щодо воєнних злочинів. Розвиток громадянського суспільства та гарантування свобод. Активна міжнародна політика – зміцнення позицій у регіоні та світі.

Рисунок 1 – Схема порядку організації заходів відновлення України (основні заходи)

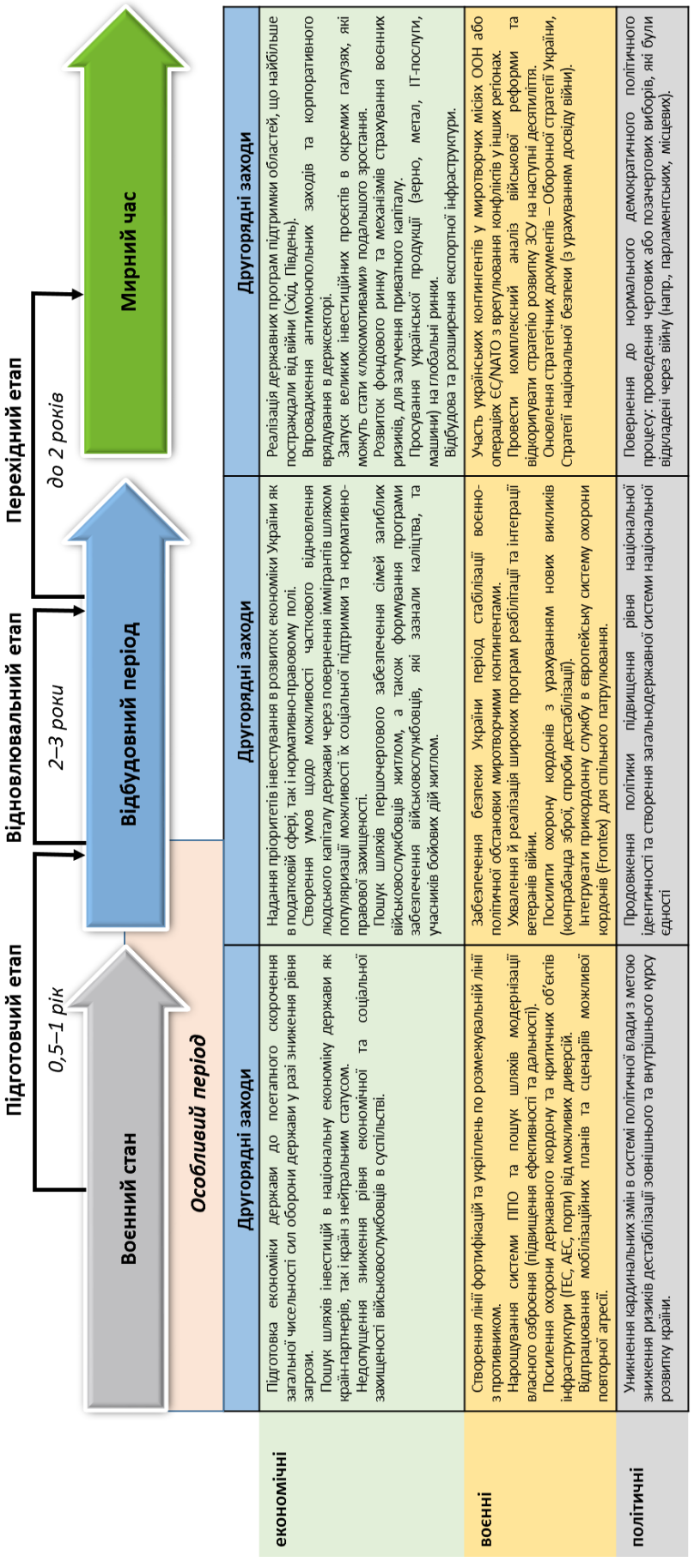


Рисунок 2 – Схема порядку організації заходів відновлення України (другорядні заходи)

намагання як сторони, яка зазнала агресії від більш потужного противника забезпечити свою безпеку на певний період стабілізації воєнно-політичної обстановки миротворчими контингентами.

Другорядні заходи:

створення лінії фортифікацій та укріплень по розмежувальній лінії з противником;

нарощування системи ППО та пошук шляхів модернізації власного озброєння (підвищення ефективності та дальності);

підготовка економіки держави до поетапного скорочення загальної чисельності сил оборони держави у разі зниження рівня загрози (не раніше 2-3 років після закінчення воєнного стану). Для забезпечення плавної реалізації цих заходів, недопущення значного зниження вимог до рівня воєнної та національної безпеки держави, а також соціального колапсу щодо захищеності прав військовослужбовців процес повинен бути детально спланований та контрольований.

Політичний напрям

Основні заходи:

уникнення кардинальних змін в системі політичної влади з метою зниження ризиків дестабілізації зовнішнього та внутрішнього курсу розвитку країни;

продовження до моменту початку реалізації економічних та військових гарантій від країн-партнерів (США, Франція, Німеччина тощо) воєнного стану, а також продовження особливого періоду навіть після закінчення воєнного стану поки не будуть хоча б на 50-60% реалізовані заходи забезпечення безпеки держави;

Другорядні заходи:

продовження політики підвищення рівня національної ідентичності та створення загальнодержавної системи національної єдності тощо.

Відновлення країни має ґрунтуватися на принципах стійкості, інклюзивності та довгострокової безпеки. Кожен захід має розглядатися не ізольовано, а в контексті взаємопов’язаності з іншими напрямами – економічним зростанням, соціальною стабільністю, розвитком людського потенціалу та зміцненням державних інституцій. Особлива увага приділяється заходам, які сприяють зміцненню обороноздатності та запобіганню можливим загрозам у майбутньому.

Крім того, визначені шляхи практичної реалізації заходів враховують необхідність залучення інвестицій, розвитку міжнародного співробітництва, застосування інноваційних технологій та кращих світових практик. Окремі ініціативи орієнтовані на швидкий ефект (“швидкі перемоги”), тоді як інші вимагають тривалого системного впровадження. Таким чином, наведена структура заходів має стати основою для поетапної реалізації державної політики післявоєнного відновлення.

Висновки

Аналіз заходів повоєнного відновлення України, структурованих за етапами та основними напрямами, дає змогу сформувати цілісне бачення системного підходу до трансформації держави в умовах постконфліктного періоду. Поділ на підготовчий, відновлювальний і перехідний етапи дозволяє логічно впорядкувати зусилля держави та партнерів у часі, забезпечуючи поступовий перехід від базової стабілізації до довгострокового розвитку. Водночас поділ заходів за економічним, військовим і політичним напрямами відображає комплексність відновлювальних процесів, що охоплюють як матеріальні, так і інституційні засади державного функціонування. Такий підхід дає змогу не лише реагувати на першочергові виклики, а й створювати умови для стійкого миру, ефективного управління та зміцнення національного потенціалу в усіх сферах. Взаємозв’язок між етапами та напрямами заходів забезпечує їхню узгодженість, мінімізує дублювання зусиль і підвищує ефективність

використання ресурсів. Такий підхід формує основу для розробки цільових політик і програм, які можуть бути адаптовані відповідно до динаміки безпекового середовища, внутрішніх потреб держави та міжнародної підтримки.

Таким чином, скоординоване виконання заходів повоєнного відновлення, з активною участю суспільства та міжнародних партнерів, дозволить мінімізувати ризики перехідного періоду і закласти міцну основу для сталого розвитку і зміцнення національної безпеки України.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Світовий банк. Оцінка потреб у відновленні України. Вашингтон: World Bank Group, 2023. 220 с.
2. Програма розвитку ООН. Відбудова після війни: Підходи, засновані на правах людини. Київ, 2022. 95 с.
3. Гриценко І. Повоєнне відновлення: уроки для України // Економіка і держава. 2022. № 11. С. 5–12.
4. Мельник О. Моделі реконструкції держав після конфлікту: світовий досвід і українські реалії. Київ, 2023. 118 с.
5. United Nations Development Programme. Resilient Recovery: Global Lessons for Ukraine. UNDP, 2023. 64 p.
6. USAID. Post-Conflict Recovery Frameworks. — Washington, 2022. 78 p.
7. Єрмоленко С. В. Післявоєнна трансформація економіки України: виклики та пріоритети // Фінанси України. 2023. № 3. С. 19–33.
8. Романенко Є. Публічне управління у воєнний і повоєнний період: порівняльний аналіз // Державне управління: теорія та практика. 2023. № 2. С. 45–52.
9. Anderson R. Post-Conflict Economic Reconstruction: Priorities for Ukraine. London: Chatham House, 2023. 81 p.
10. Kovalchuk M., Danyliuk O. Resilient Infrastructure Recovery in Ukraine: Policy Notes. Berlin: German Marshall Fund, 2023. 48 p.
11. Шевченко Н. Роль громадянського суспільства у забезпеченні прозорості відбудови України // Гуманітарний вісник. 2023. № 6. С. 27–35.
12. Кравченко В. Безпекова архітектура після війни: контури нової доктрини // Національна безпека і оборона. 2023. № 5. С. 3–9.
13. NATO. Building Sustainable Peace and Security in Post-War Environments: Lessons Learned. Brussels, 2023. 102 p.
14. OECD. Ukraine’s Recovery and Reconstruction: Governance and Funding Models. Paris: OECD Publishing, 2023. 115 p.
15. Василенко Т. Європейський досвід інтеграції сектору безпеки у політику відновлення // Українська дипломатія. 2022. № 4. С. 40–49.
16. Вісник РНБО України. Повоєнна безпека: виклики гібридного середовища. Київ: РНБО, 2023. Вип. 2. 94 с.

References

1. Svitovij bank. Ocinka potreb u vidnovlenni Ukrayini. Vashington: World Bank Group, 2023. 220 s.
2. Programa rozvitku OON. Vidbudova pislya vijni: Pidhodi, zasnovani na pravah lyudini. Kyiv, 2022. 95 s.
3. Gricenko I. Povoyenne vidnovlennya: uroki dlya Ukrayini // Ekonomika i derzhava. 2022. № 11. S. 5–12.
4. Melnik O. Modeli rekonstrukciyi derzhav pislya konfliktu: svitovij dosvid i ukrayinski realiyi. Kyiv, 2023. 118 s.
5. United Nations Development Programme. Resilient Recovery: Global Lessons for Ukraine. UNDP, 2023. 64 p.
6. USAID. Post-Conflict Recovery Frameworks. — Washington, 2022. 78 p.
7. Yermolenko S. V. Pislyavoyenna transformaciya ekonomiki Ukrayini: vikliki ta prioriteti // Finansi Ukrayini. 2023. № 3. S. 19–33.
8. Romanenko Ye. Publichne upravlinnya u voyennij i povoyennij period: porivnyalnij analiz // Derzhavne upravlinnya: teoriya ta praktika. 2023. № 2. S. 45–52.
9. Anderson R. Post-Conflict Economic Reconstruction: Priorities for Ukraine. London: Chatham House, 2023. 81 p.
10. Kovalchuk M., Danyliuk O. Resilient Infrastructure Recovery in Ukraine: Policy Notes. Berlin: German Marshall Fund, 2023. 48 p.
11. Shevchenko N. Rol gromadyanskogo suspilstva u zabezpechenni prozorosti vidbudovi Ukrayini // Gumanitarnij visnik. 2023. № 6. S. 27–35.
12. Kravchenko V. Bezpekova arhitektura pislya vijni: konturi novoyi doktrini // Nacionalna bezpeka i oborona. 2023. № 5. S. 3–9.
13. NATO. Building Sustainable Peace and Security in Post-War Environments: Lessons Learned. Brussels, 2023. 102 p.
14. OECD. Ukraine’s Recovery and Reconstruction: Governance and Funding Models. Paris: OECD Publishing, 2023. 115 p.
15. Vasilenko T. Yevropejskij dosvid integraciyi sektoru bezpeki u politiku vidnovlennya // Ukrayinska diplomatiya. 2022. № 4. S. 40–49.
16. Visnik RNBO Ukrayini. Povoyenna bezpeka: vikliki gibridnogo seredovisha. Kyiv: RNBO, 2023. Vip. 2. 94 s.

The Geopolitical Dynamics of Asia-Europe's Diplomatic Economic Relations in 21st Century: Opportunities and Challenges for Global Cooperation

Геополітична динаміка дипломатичних економічних відносин між Азією та Європою у 21 столітті: можливості та виклики для глобальної співпраці

Sarah Abdullah Alazwari
PhD candidate Faculty of political science and international relations, e-mail: sarahalazwari@gmail.com

Warsaw University, Warsaw, Poland

Сара Абдулла Алазварі
Аспірант Факультет політології та міжнародних відносин, e-mail: sarahalazwari@gmail.com

Варшавський університет, Варшава, Польща

Received: February 25, 2024 | Revised: Aprile 15, 2025 | Accepted: Aprile 30, 2025

DOI: 10.33445/sds.2025.15.2.3

Purpose: explores the evolving relationship between Asia and Europe in the 21st century, examining the prospects for collaboration and the obstacles that impede joint global problem-solving.

Method: historical analysis, discursive analysis, and thematic analysis of historical trajectories and contemporary examples.

Findings: 1. The Power of Cooperation: Trust-based alliances, particularly in trade (e.g., EU-Japan FTA) and environmental policy (Paris Agreement), are vital for tackling transnational challenges. 2. The Shadow of Rivalry: U.S.-China tensions—visible in trade wars, technological restrictions, and cybersecurity conflicts—disrupt Asia-Europe collaboration, generating spillover effects in diplomacy and economics. 3. Unity Amid Diversity: Despite differing governance models and human rights perspectives, pragmatic cooperation remains achievable when mutual interests take precedence. 4. Navigating the Digital Age: Breakthroughs in AI and 5G demand agile policymaking to capitalize on innovation while preventing global fragmentation. 5. The Imperative of Stability: Regional conflicts—from territorial disputes to political upheaval—endanger collective objectives, underscoring the need for structured dialogue. 6. Bridging Divides Through Exchange: Cultural and academic engagement fosters mutual understanding, laying the groundwork for enduring partnerships.

Theoretical implications: By reinforcing neoliberal institutionalism, this study underscores the significance of trust and multilateralism in sustaining cooperation despite power disparities. It contests realist skepticism by proving that ideological differences (e.g., democracy vs. authoritarianism) need not obstruct collaboration when aligned goals—such as climate mitigation and economic resilience—are prioritized. Furthermore, it weaves from constructivist perspectives, illustrating how shared norms (e.g., environmental stewardship and global health) can transcend political and cultural divides, fostering deeper solidarity.

Paper type: theoretical.

Key words: Asia and Europe, trade relationships, opportunities, collaborations, political systems, global tensions, climate change, Asian-European relations, Diplomatic economic relations, global cooperation, public health, trade relationships, cultural exchanges, regional stability, global prosperity.

Мета дослідження: досліджує змінні взаємини між Азією та Європою у XXI столітті, розглядаючи перспективи співробітництва та перешкоди, що ускладнюють спільне вирішення глобальних проблем.

Метод дослідження: історичний аналіз, дискурсивний аналіз та тематичний аналіз історичних шляхів розвитку та сучасних прикладів.

Результати дослідження: 1. Сила співпраці: Альянси, засновані на довірі, особливо в торгівлі (наприклад, Угода про вільну торгівлю між ЄС та Японією) та екологічній політиці (Паризька угода), є важливими для вирішення транскордонних викликів. 2. Тінь суперництва: Напруга між США та Китаєм — помітна в торгових війнах, технологічних обмеженнях та конфліктах у сфері кібербезпеки — заважає співпраці між Азією та Європою, породжуючи відлуння у сфері дипломатії та економіки. 3. Єдність у різноманітності: Незважаючи на різні моделі управління та погляди на права людини, прагматична співпраця залишається можливою, коли на першому місці стоять спільні інтереси. 4. Орієнтація в цифрову епоху: Прориви у сфері ШІ та 5G вимагають гнучкої політики, щоб скористатися інноваціями та запобігти глобальній фрагментації. 5. Імператив стабільності: Регіональні конфлікти — від територіальних суперечок до політичних заворушень — загрожують колективним цілям, підкреслюючи необхідність структурованого діалогу. 6. Подолання розбіжностей через обмін: Культурні та академічні контакти сприяють взаєморозумінню, закладаючи основу для міцних партнерств.

Теоретична цінність дослідження: Підтримуючи неоліберальний інституціоналізм, це дослідження підкреслює важливість довіри та багатосторонності у підтримці співпраці, незважаючи на різницю в рівнях впливу. Воно спростовує скептицизм реалістів, доводячи, що ідеологічні відмінності (наприклад, демократія проти авторитаризму) не обов'язково перешкоджають співпраці, коли спільні цілі, такі як пом'якшення кліматичних змін і економічна стійкість, стають пріоритетними. Крім того, воно інкорпорує конструктивістські перспективи, ілюструючи, як спільні норми (наприклад, екологічне управління та глобальне здоров'я) можуть долати політичні та культурні відмінності, сприяючи глибшій солідарності.

Тип статті: теоретичний.

Ключові слова: Азія та Європа, торговельні відносини, можливості, співпраця, політичні системи, глобальна напруженість, зміна клімату, азіатсько-європейські відносини, дипломатичні економічні відносини, глобальна співпраця, охорона здоров'я, торговельні відносини, культурний обмін, регіональна стабільність, глобальне процвітання.

Introduction

Historical background and evolving diplomatic ties

The Asia-Europe connection has spanned centuries, marked by the ancient Silk Road, which facilitated cross-cultural, economic, and technological exchange between the two regions. European trade with Asia in silk, porcelain, and spices, along with the exchange of ideas related to philosophy, mathematics, and medicine, facilitated by empires in India, Persia, and China, fostered the development of new Asian-European relations.

From the 15th to the 20th century, Europe experienced the Age of Exploration and the period of colonization, and European interests shifted towards Asia. This resulted in Asian empires increasingly using Europe as a trade route. China, India, and Persia expanded their territories and empires through conquest and trade across significant areas of Asia, from India to Southeast Asia.

The history of Asia and Europe spans centuries, with the most notable connection being the ancient Silk Road. This network facilitated technological and economic exchange between the two regions.

India, Persia, and China were among the most important regions contributing to this trade. European trade with Asia consisted of silk, porcelain, and spices, as well as an exchange of ideas related to philosophy, mathematics, and medicine. However, trade did not establish the Silk Road; its construction occurred during the Han Dynasty between 206 BCE and 220 CE, intended to connect China to the Mediterranean.

The mid-20th century was marked by Indian independence and the economic conflict between capitalism and Soviet communism. From 1947 to 1991, Canada maintained a peaceful stance between the two ideological blocs. Canada made efforts to cultivate strong relations with both superpowers and remained non-aligned.

Ideological competition

Europe's diplomatic strategy shifted significantly after World War II. This shift involved forming alliances like NATO to contain Soviet influence globally. The Korean War exemplifies this, with European nations sending troops to fight alongside South Korea against the communist North, which was backed by the Soviet Union and China. In contrast, countries like India adopted a policy of neutrality, enabling them to maintain diplomatic relations with both the Western bloc and the Soviet Union while advocating for the interests of developing nations [Millett, A. R., 2024].

Regional conflicts and their impact

The Korean and Vietnamese Wars played a critical role in Asia and significantly impacted relations between Asian and European countries. The Korean War, beginning in 1950 with North Korea's invasion of South Korea, pitted North Korea against the United States and its allies, including European nations that joined the conflict to combat the global spread of communism. This surge in communist activity escalated tensions among the three major powers: the United States, China, and the Soviet Union.

The Vietnam War (1955-1975), another global conflict, saw China and the Soviet Union supporting North Vietnam against South Vietnam, which was allied with the United States and South Korea. These events exacerbated existing East-West tensions stemming from the Cold War.

Results

Lasting effects on diplomatic relations

The political assertiveness and military interactions of this era have left a lasting impact on the relationship between Asia and Europe. Increased political integration within NATO enabled

European countries to engage more deeply in Asian conflicts, affecting Asian perceptions of these countries. These conflicts also prompted some Asian nations to reassess their foreign policies, incorporating regional integration and multilateralism to seek balance between superpowers. These conflicts have gradually shaped the contemporary geopolitical landscape of Asia-Europe relations, including the South China Sea dispute, cybersecurity threats, and human rights issues.

After the Cold War, relations between Asia and Europe became more balanced. Both regions shifted their focus toward economic interaction and partnerships for development and political stability. The creation of inter-regional forums like Association of South East Asian Nations (ASEAN) in 1996 paved the way for the Asia-Europe Meeting (ASEM), promoting trade, cultural exchange, and addressing global challenges such as climate change and security issues.

EU-ASEAN Economic Cooperation: The collaboration between the EU and ASEAN represents a significant economic force, accounting for a substantial portion of global GDP and trade. ASEAN is the EU's third-largest trading partner outside Europe, after China and the US, with trade in goods reaching approximately €252.5 billion in 2023. Bilateral trade in services between the EU and ASEAN reached €126.1 billion in 2022. ASEAN represents approximately 8% of the EU's total trade and is its third-largest trading partner after China and the US. The EU has significant investments in ASEAN countries, with Foreign Direct Investment (FDI) totaling €400.1 billion in 2022. ASEAN investment in Europe has also increased recently, reaching over €195.6 billion in 2021.

The EU's primary exports to ASEAN are chemicals, industrial machinery, and transport equipment. ASEAN's primary exports to the EU include machinery, agricultural goods, and other manufactured products. These trade flows are illustrated in Figure 1, which displays trade in goods in billions of euros.

The EU's Global Gateway initiative aims to enhance connectivity and sustainable development in the region, emphasizing the importance of mutual economic growth between Europe and Asia [Economic cooperation – EU-ASEAN, October 27, 2024].

The ASEM was established to encourage open dialogue and interaction between Asian and European countries on political, economic, and socio-cultural matters. This intergovernmental initiative emphasizes the growing importance of economic relations between the two continents, facilitating their engagement in the global economy [ASEM InfoBoard, October 27, 2024].

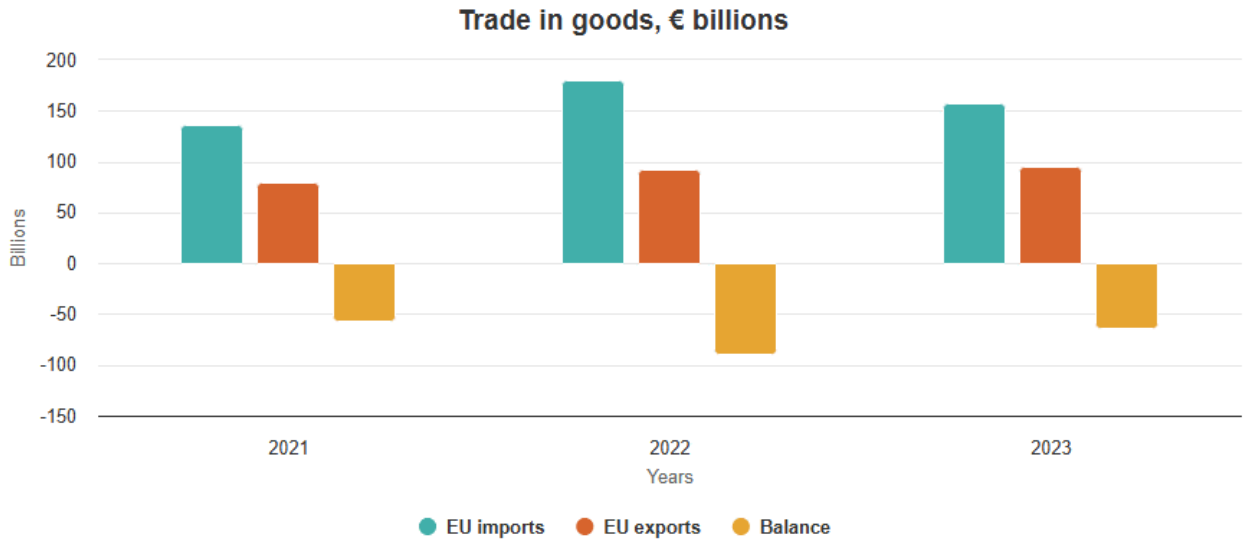


Figure 1 – EU imports and Exports with ASEAN in Euros

Strategic Partnership: The EU's Indo-Pacific cooperation strategy, which emphasizes ASEAN centrality, demonstrates Europe's view of cooperation with Asia as crucial for addressing global issues and fostering economic growth. This strategy aims to support global economic recovery and promote economic prosperity with various Indo-Pacific nations. New partnership treaties have been established with Indo-Pacific countries. These strategies target areas significantly affected by the COVID-19 pandemic, including sustainable and inclusive economic growth, support for the green economy, maritime governance, digital governance and partnerships, infrastructure development, military security, and human security.

Cooperation on infrastructure development, energy, and climate change policy has far-reaching global development consequences. China's Belt and Road Initiative (BRI), as shown in Figure 2, has promoted greater integration between Europe and Asia, enhanced connectivity, and improved trade infrastructure. However, these initiatives also highlight the need for diversification to prevent over-reliance and regional dominance. As Europe and Asia address the security of undersea cables amidst technological competition, their partnership is crucial for maintaining a multipolar and balanced international environment that promotes global peace and prosperity [Deudney, D. H., 2024].

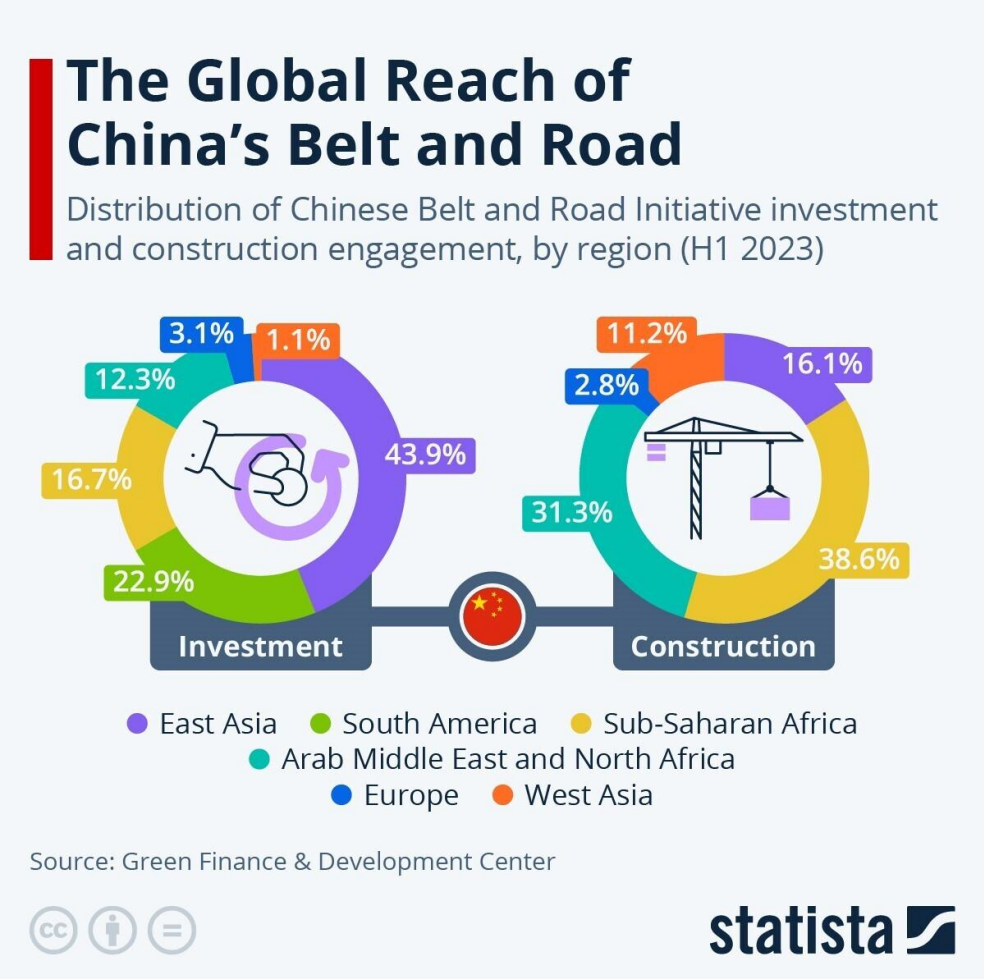


Figure 2 – China's Belt and Road Investment Map by Katharina Buchholz

Economic interdependence and strategic trade alliances

In recent decades, trade between Asia and Europe has increased, largely due to Asia's economic development and Europe's strengthening of its trans-continental partnerships. The European Union has made progress in its trade relations with major Asian countries such as China,

Japan, India, and those in the ASEAN bloc, stressing access to markets, competitive neutrality, and healthcare. At the end of 2023, China emerged as the third largest partner for EU exports (8.8%) and the largest partner for EU imports (20.5%), with a similar percentage share to India. The total trade volume between the EU and China stood at nearly €1,854.7 billion. The EU and Japan signed an Economic Partnership Agreement in 2018, which greatly enhanced trade between the two countries. In 2023, trade between the EU and Japan was around €125 billion. The EU is the largest trading partner of India, and trade between the two in 2023 was estimated to be around €80 billion. The total trade in goods between the EU and ASEAN was estimated at €252.5 billion in 2023, accounting for 76% of the total trade. This trade is dominated by manufactured goods; 82% of exports from the EU to ASEAN and 86% of exports from ASEAN to the EU are of these goods. The EU trade in goods with China, from 2013-2023, is shown in figure 3 [China-EU, 2024; ASEAN].

China is the EU's best bilateral trade partner for commodities, while Japan is an increasingly important economic partner for industrial and high-tech items.

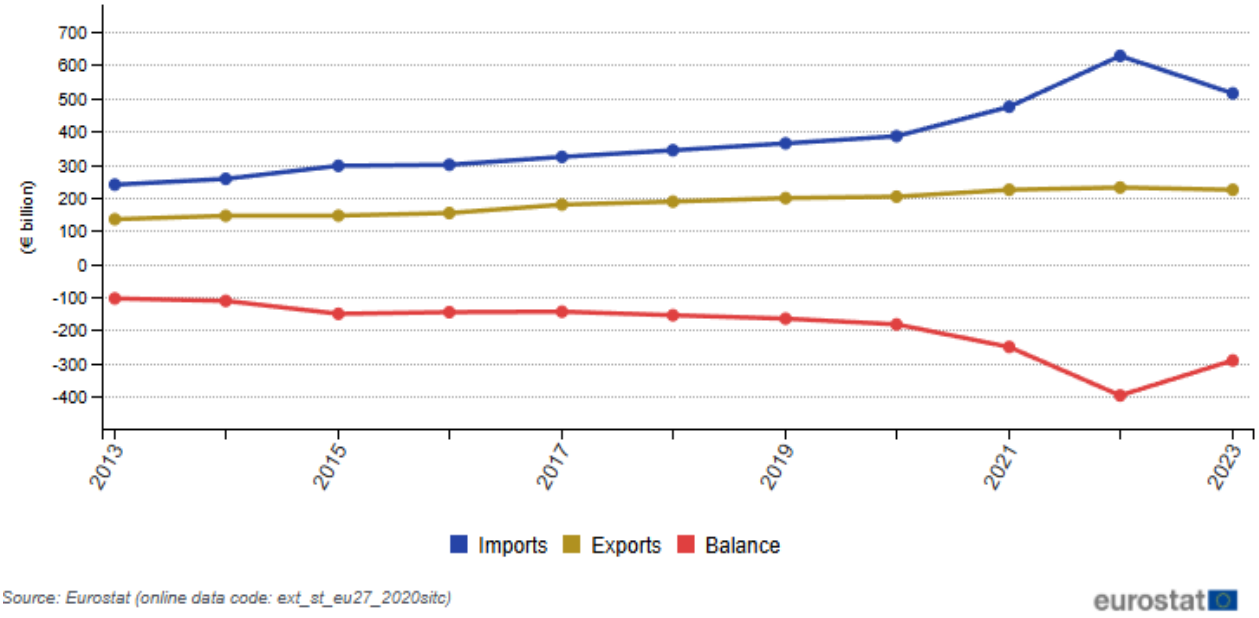


Figure 3 – EU trade in goods with China, 2013-2023 ASEAN

One of the largest free trade agreements, including the EU-Japan Economic Partnership Agreement of 2019 that eliminated tariffs on more than 90% of goods shipped between the two regions, focuses on developing relations with ASEAN, a rapidly growing region, through the EU-ASEAN Free Trade Agreement currently under negotiation. The FTA process remains lengthy, involving a large technological gap, which in turn does not undermine the EU's reliability as ASEAN's third most important trade partner. Countries like India present fair-trade barriers and taxes, and seek the right to negotiate; however, these claims create strained relationships and stifle efforts to build solid economic bridges with the promise of new free trade agreements on green technologies, digital trade, and pharmaceuticals. [Asia and Europe, 2018].

To enhance connectivity between Europe and Asia, the European Council launched the "Connecting Europe and Asia – Building blocks for an EU Strategy" initiative in September 2018. This strategy aims to improve connectivity through careful, comprehensive, and rules-compliant methods, focusing on transportation, energy, and digital systems. It emphasizes high social and environmental standards, alongside fiscal and financial accountability for infrastructure projects. Due to the need to maintain growth rates and adapt to climate change, Asia is projected to require over €1.3 trillion annually in infrastructure investments. The estimated cost of the EU's Trans-

European network between 2021 and 2030 is €1.5 trillion. The strategy includes specific policy initiatives to facilitate market access by promoting the free flow of goods, services, capital, and people across national borders.

Improved connectivity between Europe and Asia is expected to result in enhanced economic growth, increased global competitiveness, and expanded trade. The strategy aims to ensure the social and environmental sustainability of major projects that enhance international and regional connectivity. Furthermore, it is expected to foster stronger economic ties, collaboration on international and regional security, increased political goodwill, and the development of cooperative democracies [China-EU].

The prospect report indicates that the strategy suggests the EU should employ a comprehensive, principles-based approach to connectivity with its Asian partners, targeting existing and projected European Union networks. Importantly, the strategy aims to enhance sustainable connectivity eastward. The focus is on ensuring comprehensive connectivity through the development of transportation, environmental, and energy infrastructure.

This complements China's ambitious Belt and Road Initiative (BRI), which has invested billions of dollars in infrastructure across Asia and Europe, promoting a (ostensibly) transparent investment and sustainable approach.

Comprising ports, railways, and logistics hubs, BRI projects have facilitated trade between Europe and Asia but have also raised concerns about dependence, debt, and China's increasing geopolitical leverage over European countries, particularly regarding British dependence. In contrast, the EU's plan emphasizes the creation of just rules-based relations and cooperation, prioritizing environmental protection and the well-being of local populations [European Parliament, 2021].

Regarding these countries, Japan has partnered with the EU on infrastructure projects through the EU's Partnership on Sustainable Connectivity and Quality Infrastructure. This partnership has facilitated Asian development while promoting transparent and high-quality investment. These projects aim to limit over-reliance on any single trade partner, thereby strengthening a multipolar system of infrastructure development in the Eurasian region [Almora, I. R., & Almora's, I. R.,2023, November 23; Inforegio – EU Japan].

The strong trade interest between Asia and Europe extends beyond simple trade, encompassing various areas of economic competition. The high-technology sector is particularly competitive, with both regions vying for global leadership in the digital economy, artificial intelligence (AI), and 5G. AI is a key area, attracting significant investment from both regions for extensive research and development of new AI systems and their applications. The EU is prioritizing regulations that emphasize safety and ethical considerations for AI systems, while Asian countries are rapidly developing their AI capabilities. Similarly, 5G network development is underway in the EU, facing competition similar to that in the US. China and South Korea have a clear advantage in 5G deployment compared to other Asian countries, while the EU is focused on establishing robust infrastructure to ensure safety and competitiveness in the market.

These implications affected multiple areas, including economic impact, security concerns, intellectual property issues, and geopolitical tensions. A strong presence in high-technology sectors ensures a competitive advantage in the global marketplace, resulting in new job creation and increased productivity. Like other high-technology areas, this sector faces security challenges, particularly regarding data protection, privacy, cybersecurity, and intellectual property safeguarding. Competition for technological leadership can escalate geopolitical tensions, as evidenced by some countries already imposing restrictions and bans on certain technologies and corporations [Mischke, Massimo, Solveigh, & Smit, 2025].

Intellectual property (IP) rights have created challenges for European businesses and governments trading with the Asian market, particularly China. Consequently, policies protecting IP

rights and promoting fair competition have been strengthened to counter unfair trade practices like dumping and subsidizing, against which the EU has implemented trade defense measures. [Andrijanič, M. B., & Meissner, P., 2024; Johnson, J., & Szewczyk, B. M., 2024; Okolo, C. T., & Tano, M., 2023; Global Overview, 2024; The importance of high, 2020].

The political momentum of the EU-ASEAN Strategic Partnership was solidified at the Brussels EU-ASEAN Commemorative Summit in December 2022. The progress of the EU-ASEAN relationship is a result of the strategic partnership, the comprehensive plan of action for 2023–2027, the comprehensive air transport agreement, and the Brussels summit.

Competition for resources between the EU and some Asian nations, such as China, impacts global trade and economic relations. The EU's ability to function efficiently relies heavily on Asia for raw materials and semiconductors. To reduce this dependence, the EU is actively seeking alternative suppliers. Conversely, China and other Asian countries seek resources like rare earth elements, thereby participating in a resource trade competition that has shifted the flow of resource supply. This competition has implications for multiple fields, including economic security, geopolitical tensions, innovation and technology, and environmental impact. The EU aims to diversify its supply chains to safeguard economic security and minimize disruptions. Potential geopolitical conflict exists over competition for critical materials such as fuels, metals, and petroleum products. The availability of rare earth elements and other vital resources is essential for advancements in fields like renewable energy, electric vehicles, and advanced electronics. Because the extraction and processing of these resources can have significant environmental impacts, developing sustainable resource management practices is crucial. The intensifying competition highlights the need for strategic alliances and sustainable resource management to achieve long-term economic development.

The development of equitable and sustainable trade policies is underway to maintain the strategic security interests of both the EU and Asian economies. These dynamic offers insight into the importance Denmark places on international relations, as well as the challenges of simultaneously competing and cooperating, particularly when those interactions are adversarial [Liew D.]

Geopolitical tensions and security concerns

Asia and Europe have become increasingly important in the global arena due to the evolving geopolitical landscape. Increased trade and investment between these regions have fostered a strong economic relationship. However, this interdependence presents challenges, including geopolitical tensions and competition for resources and technology. Analyzing these issues is crucial for a comprehensive understanding of the Asia-Europe relationship.

The competitive landscape of the semiconductor market, particularly concerning China, is influenced by the EU's dependence on Asian resources due to Europe's limited raw materials. This dependence makes outsourcing costly for Europe, not Asia. Furthermore, it intensifies resource trade competition, likely increasing the flow of resources from Asia to Europe. The original phrasing "Me and the rest of Asia" is grammatically incorrect and has been replaced with a more formal tone.

In the 21st century, the relationship between Asia and Europe extends beyond trade and commerce, encompassing increasing geopolitical tensions and security concerns. These issues stem from shifts in the global balance of power, regional conflicts, and evolving security arrangements, all of which influence Euro-Asian policies and their respective global interests.

Security Alliances

Amidst a changing global security environment, Asia and Europe are increasingly aligned in their pursuit of regional order and global influence. Recognizing the impact of Asian security developments on Europe, NATO has expanded its focus to include Asia, particularly the Indo-Pacific

region. This increased attention stems from concerns about growing Chinese military strength and a commitment to supporting democracy and a rules-based order. Consequently, NATO has strengthened relations with South Korea, Australia, and Japan to enhance information sharing and defense cooperation. [Relations With Partners, 2024; Shetler, P., 2024].

Furthermore, the EU-Indo Pacific Strategy, introduced in 2021, expands on Europe's vision for a free and open Indo-Pacific. Figure 2 illustrates the Indo-Pacific's vital importance for EU economic growth. This EU policy aims to strengthen relations with key Asian democracies, such as Japan, India, and ASEAN nations, and foster partnerships in maritime and cybersecurity, as well as climate change mitigation. The strategy seeks to counter growing authoritarianism in the region, particularly from China, and bolster Europe's pursuit of regional stability to secure its trade routes and other interests [Grgić, G., 2024].

Objectives of the EU-Indo Pacific Strategy include sustainable and inclusive prosperity, green transition, ocean governance, digital governance and partnership, connectivity, security and defense, and human security (encompassing human rights, health, and education). The EU strategy and its accompanying policies prioritize promoting responsible international cooperation and cultivating a rules-based international order. By collaborating with Indo-Pacific countries, the EU aims to address global challenges while enhancing regional stability, security, and prosperity. The strategy particularly emphasizes rules-based multilateralism, liberal trade and investment policies, and EU-Nexus promotion.

A free and open Indo-Pacific encapsulates the strategies of these countries toward the Indo-Pacific region. These policies aim to ensure economic growth, development, and, crucially, peace, stability, and freedom of movement within the Indo-Pacific.

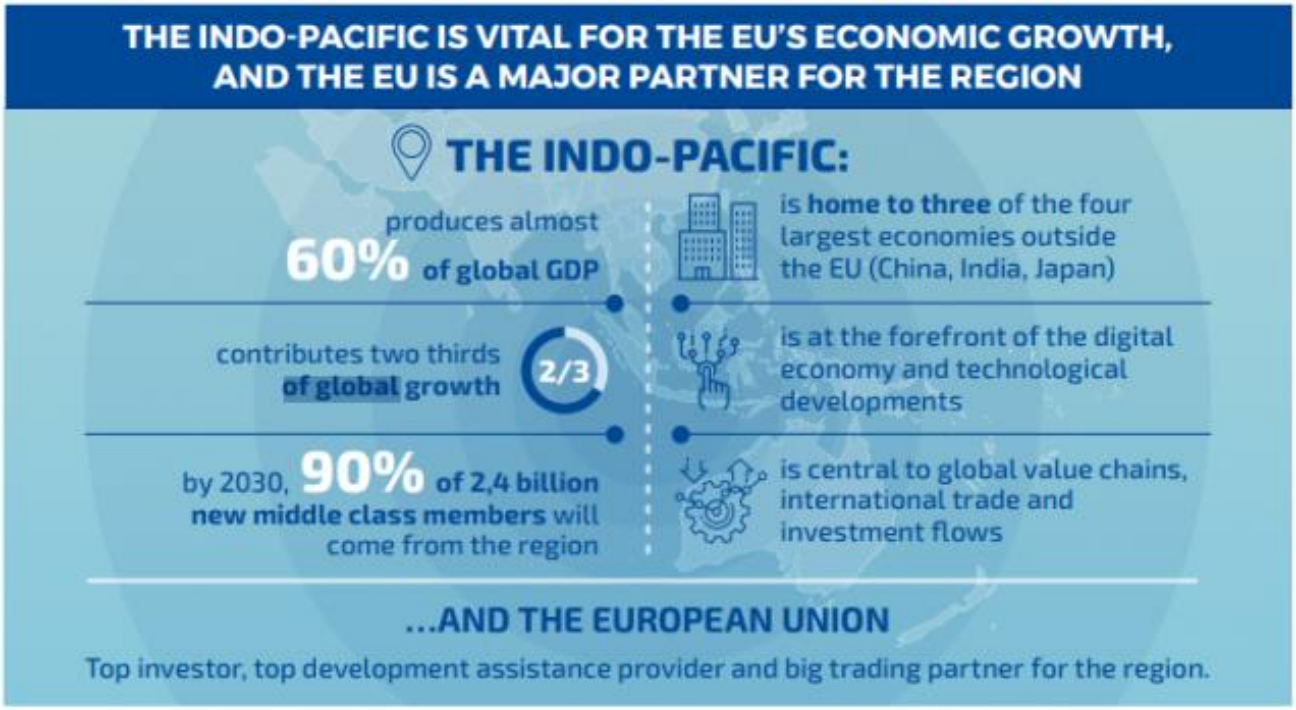


Figure 4 – The Indo-Pacific is vital for the EU's economic growth, and the EU is a major partner for the region

Source: EEAS Press Team

Rising tensions

Overlapping territorial claims in the South China Sea by the People's Republic of China, Vietnam, the Philippines, and other Southeast Asian countries have caused significant concern, as the region experiences ongoing military buildup and competition. While European countries have

no direct claims in the area, the EU is concerned about freedom of navigation and occasionally supports the United States in freedom of navigation operations intended to deter Chinese expansionism through soft power. The South China Sea also exacerbates concerns about potential military conflicts that could threaten critical trade routes between Asia and Europe, impacting their economies [Pletcher, K., 2024].

Both regions have experienced a rise in ransomware attacks targeting key infrastructure, commercial organizations, and government agencies. These attacks often demand cryptocurrency payments for the release of captured files. Phishing attempts remain rampant, with hackers using emails, text messages, and social media to trick individuals into divulging personal information. Cybercriminals are increasingly focused on extracting data from the Internet of Things (IoT) using spyware and hacking devices.

The EU introduced its technological security strategy to mitigate cyber*National Security*h further integration, including safeguarding essential industries, expanding cyber infrastructure, and fostering international cooperation. While cybersecurity improved in 2023, increasing cyber threats remain a significant concern. Globally, state-sponsored cyberattacks are increasingly prevalent, and the growing digitization of Asian and European economies exacerbates this risk. Attacks on critical infrastructure, financial systems, and political institutions pose significant threats to both Asia and Europe. The EU and its Asian counterparts are developing strategies to strengthen cybersecurity, establish responsible state cyber conduct, and cooperate on information exchange regarding critical infrastructure protection.

Military expansionism in the Indo-Pacific region, particularly by China, North Korea, and the United States, further complicates the security situation. North Korea's missile tests and nuclear ambitions pose a direct threat to its Asian neighbors and to European security, as any conflict in the area could escalate globally. While European countries have been hesitant to provide direct military support, they have increasingly supported sanctions and diplomatic initiatives aimed at denuclearization.

Russia's Role

Russia holds a unique position as a leader in Asia while maintaining strong ties with Europe. It exerts influence across the continent through geopolitics, energy, and defense, solidifying its role in shaping Asia-Europe relations. Sino-Russian cooperation has increased, particularly through joint military projects and economic initiatives, including energy and infrastructure development, within Asia. This strategic partnership represents a potential shift away from Western dominance, fostering a balance of power against perceived Western threats.

Russia's influence in Europe, especially regarding energy resources, is crucial for European energy policy formulation. The reliance of some EU countries on Russian gas and oil complicates Europe's security stance in relation to Japan and South Korea. European partners oppose Russia's military interventions. Following Russia's actions in Ukraine, Europe imposed numerous economic sanctions on Russia and sought to reduce its energy dependence on the country. These policies have consequences for European diplomacy and the region's economic stability [Katinas, P., 2024; The European Union-Russia Energy Divorce, 2024].

The Russo-Ukrainian War has resulted in significant territorial losses for Ukraine and exacerbated geopolitical rivalries between the two states, with implications for both Europe and Asia. The war has reshaped global power dynamics, supply chains, energy politics, and alliances. Asian regions reliant on Russian energy and commodities face economic challenges and increased food insecurity due to Russia's unilateral attack on Ukraine, which led to the blockade of crucial imports like wheat, corn, and sunflower oil.

The EU and its partners imposed unprecedented sanctions on Russia's economy in response to its undemocratic actions, particularly its military operations in Ukraine. These sanctions aimed

to cripple Russia's economy and military capabilities. However, they have been limited in their ability to significantly alter Russia's military actions, primarily serving as a deterrent against further escalation. While demonstrating Western unity, these sanctions have yielded limited tangible results in crippling the Russian economy. Russia is attempting to mitigate these challenges by establishing new trade routes and strengthening relations with China and India [Perga I., 2025].

Human Rights and Democratic Values

Conflicting Values

Divergent political values between Asia and Europe, particularly regarding governance, human rights, and democracy, create tension. While generalizations about "Asia" should be avoided as the continent is diverse, Europe is a staunch advocate of democracy, the rule of law, and individual freedom, consistently condemning the political systems and human rights records of countries like China and Myanmar. In China, Europe has strongly criticized restrictions on freedom of speech, the treatment of ethnic minorities, especially in Xinjiang, and the suppression of democracy in Hong Kong. The European Parliament has imposed targeted sanctions on Chinese officials and companies accused of human rights abuses, signaling Europe's commitment to upholding democratic principles globally [Talmon, S. 2023; Today, 2024].

Similarly, the EU has condemned human rights abuses in Myanmar, particularly the 2021 military coup and subsequent violent suppression of pro-democracy protests. Europe's support for sanctions and trade embargoes against Myanmar demonstrates its prioritization of democracy and human rights, even when such measures strain economic relations. These criticisms reinforce the EU's stance on democracy but are sometimes perceived as justification for strained relations with non-democratic Asian countries [Lester, M., & O'Kane, M., 2024; Crawford, J., & Tzinieris, S., 2024].

Diplomatic challenges

Peaceful relations between Asia and Europe are challenged by diverse values that sometimes create friction. The EU often imposes economic sanctions and travel bans on certain countries for violating international rules, often while pursuing other objectives. For example, the seizure of the CAI followed sanctions imposed on Chinese officials for human rights abuses in Xinjiang. In retaliation, China blacklisted EU politicians and scholars, escalating diplomatic tensions.

Sanctions can significantly impact a country's economy, as seen in East Asia, causing substantial trade disruption. Concerns about the political situations in China and Myanmar have influenced ASEAN countries. The already unstable environment in Myanmar became volatile after the 2021 military coup. China's support for the military regime raises concerns about a potential long-term conflict and humanitarian crisis. China has significant interests in Myanmar, including the China-Myanmar Economic Corridor (CMEC) and other infrastructure projects. These ongoing conflicts and political instability, with their inherent economic risks, have generated public backlash and resistance.

Restrictions on some ASEAN member states, even while strengthening economic ties with the bloc, hinder the free flow of trade and diplomatic engagement with all EU member states. Some Asian governments often resist clauses related to human rights in trade agreements due to disagreements.

These diplomatic disputes extend beyond sanctions. European countries and the EU regularly denounce human rights violations, potentially straining diplomatic relations. However, promoting democracy and human rights are central to European foreign policy, aiming to hold nations accountable. Balancing these principles with practical diplomatic goals remains a challenge as Europe strives to uphold its human rights commitments without compromising its strategic interests in Asia.

The role of international institutions

International institutions are crucial for establishing and strengthening relations between Asia and Europe. These organizations provide forums for discussion and cooperation on issues ranging from trade and economic development to sustainability, security, and environmental protection. By fostering communication and understanding, these institutions build trust, address shared challenges, and promote peace and stability. For Asia-Europe relations, international institutions are essential for navigating the complexities of globalization and fostering a more collaborative world.

ASEM and Beyond

The Asia-Europe Meeting (ASEM), established in 1996, plays a central role in fostering dialogue and cooperation between Asia and Europe. This multilateral initiative comprises 53 partners, including 30 European and 21 Asian countries, the European Union, and the ASEAN Secretariat. Beyond promoting political and economic cooperation, ASEM addresses social and cultural development. Its key goals are improving connectivity, strengthening partnerships, and providing a framework for enhanced dialogue on major international issues, enabling collaboration despite differences in governance and economic development [Parry, M., 2024].

ASEM's flexible approach facilitates informal dialogue on issues such as climate change, sustainable development, and security. This framework allows ASEM to serve as a valuable communication and coordination tool for both regions on international matters. Despite its informal nature, ASEM has significantly contributed to developing relations between Asia and Europe by promoting understanding and cooperation on key issues.

Multi-regional organizations like the United Nations and ASEM enhance relations between Asia and Europe.

To the UN's credit, Asian and European nations actively participate in initiatives like the Sustainable Development Goals, addressing global issues such as poverty, healthcare, and education. Similarly, UN members from both regions participate in philanthropic and environmental efforts. The World Trade Organization (WTO) supports open and competitive international markets, which are particularly important for Asia and Europe, given their significant reliance on international trade.

Multilateral Cooperation

Multilateral cooperation through organizations like ASEM, the WTO, and the United Nations is crucial for helping Asian and European nations address global issues such as climate change, clean energy, and emission control. For example, the EU-Asia Connectivity project aims to build sustainable infrastructure and digital networks aligned with the Paris Agreement, further supporting ASEM discussions.

ASEM is a forum for dialogue and cooperation between the two regions. Established in 1996, ASEM comprises 53 partners, representing over 65% of global GDP and nearly 60% of the global population. Since its inception, ASEM has launched various initiatives, such as the EU-Asia Connectivity Strategy, which aims to improve infrastructure, digital connectivity, and sustainable development within member regions. This strategy has fostered economic interaction and enhanced understanding between the EU and Asia [Asia-Europe Meeting, 2023].

The COVID-19 pandemic, among other health crises, highlighted the importance of a coordinated approach to problem-solving. The WHO facilitated Asian and European nations' efforts in vaccine distribution, allocation, and other crucial health initiatives, strengthening existing Asia-Europe partnerships and fostering future global public health collaborations.

Trade organizations like the WTO work to prevent economic imbalances and ensure fair trade by establishing rules and dispute resolution mechanisms. For example, the WTO addressed the dispute between Indonesia and the EU regarding Indonesia's restriction on raw nickel exports, which the EU challenged as violating WTO trade regulations. This case exemplifies the WTO's crucial role in resolving trade conflicts between Asia and Europe [Winkler, S., 2008].

While posing challenges, the rise of competition and protectionism has also benefited Asia and Europe by providing access to a rules-based trading system. This system facilitates the resolution of trade conflicts and promotes stability in global markets. The WTO's principles are particularly important for smaller economies in Asia and Europe, promoting fairer competition, stimulating economic growth, and alleviating poverty through trade [Pletcher, K., 2024].

The UN serves as a major body for global governance and intervention, fostering unparalleled cooperation among member states. China's position at the UN, particularly through the Belt and Road Initiative (BRI), has significantly increased infrastructure investment and policy cooperation between Asia and Europe. The BRI's integration into UN narratives and global development frameworks has deepened relations between the two regions [Garcia-Herrero, A., T. Storella and P. Weil, 2024].

Areas of Cooperation: Climate Change, Public Health, and Education

Climate Action

Asia and Europe have found common ground regarding climate change, prompting collaboration toward sustainable outcomes and environmental protection. This partnership is built upon Asian and European efforts in sustainability and renewable energy, as both regions strive to reduce greenhouse gas emissions and transition to clean energy sources. The EU is collaborating with Asian nations like China, India, and Japan to develop green technologies that optimize energy efficiency and promote wind, solar, and hydroelectric power. EU climate action initiatives, such as the European Green Deal, have inspired similar policies in some Asian regions, including circular economy, zero-waste initiatives, and green infrastructure projects. For example, the EU-Asia Clean Energy Technology Network facilitates knowledge exchange, promotes innovation, and conducts joint studies on clean energy technologies. Both Asia and Europe have made significant commitments under the Paris Agreement, and ASEM serves as a vital forum for these states to work towards achieving their climate targets. Furthermore, Europe's Green Deal has encouraged parts of Asia to adopt similar sustainability policies, particularly regarding circular economies, zero-waste initiatives, and green infrastructure projects. These programs aim to promote economic development by creating green jobs and improving energy resilience, in addition to addressing the effects of climate change.

Pandemic Preparedness

The COVID-19 pandemic highlighted the importance of global cooperation in maintaining robust health systems and pandemic preparedness. Since then, Asia and Europe have strengthened collaboration in healthcare, scientific research, and pandemic response mechanisms. Along with the WHO, both regions have implemented joint initiatives on vaccine implementation, resource sharing, and healthcare system strengthening. During the pandemic, European and Asian scientists and public health institutions exchanged information and resources, enabling rapid vaccine development and treatment protocols. Both Asia and Europe are exploring new frameworks for international health security, emphasizing that pandemic preparedness collaborations should extend beyond COVID-19. The EU and ASEAN Strategic Partnership in Health have outlined key areas of cooperation in their Joint Communique, including disease monitoring and control, joint research, and health system strengthening through human resource development. Further investments

include strengthened collaboration on infectious disease research, particularly zoonotic diseases with pandemic potential. Initiatives like the EU-supported GloPID-R network fund global preparedness research and foster greater intercontinental research collaboration, reducing response time and increasing healthcare capacity for future outbreaks.

Educational and cultural exchanges

The Asia-Europe dimension is also important, offering educational and cultural exchanges that promote soft power diplomacy and bilateral understanding. For example, the Erasmus+ program provides scholarships for students from Asia to study in Europe, and vice-versa, encouraging cultural and academic exchange between both regions. Similarly, the ASEF promotes and facilitates cultural exchange, youth programs, and collaborative research between Asia and Europe. Research collaborations between European and Asian universities, focusing on areas like technology, health science, and climate change, have led to the establishment of joint research centers and fostered innovation. Sustainable development benefits from these joint research centers, which provide opportunities for universities to further innovation, particularly in independent research. Cultural exchange and collaborations, including language, arts, and heritage programs, further enable Asia and Europe to leverage their soft power to strengthen mutual understanding and relations.

Education and cultural exchange encourage nations to overcome preconceptions and build enduring networks of individuals and organizations with shared goals. These programs not only unite people but also prepare them for a globalized world, fostering strong relationships with diverse stakeholders, including politicians, diplomats, and those involved in promoting beneficial economic ties between the two regions. For example, the European Union launched the EU-GCC Green Transition Project during the 2024 World Future Energy Summit.

Future prospects: toward a balanced partnership?

Potential scenarios

Currently, Asia and Europe are developing alliances that could reshape the global order. Several potential outcomes are possible in the coming years, depending on factors such as regional geostrategic stability, political and economic perspectives, and trade relations. One key scenario is a multipolar world where Asian and European states increase cooperation, reducing reliance on established powers like the US. In this scenario, Asian and European countries would likely prioritize their economic relationship, climate change collaboration, and regional security initiatives, strengthening ASEM and other multilateral forums.

Alternatively, a competitive alignment scenario could emerge where Asia-Europe relations are influenced by external pressures, such as deteriorating US-China relations. In this situation, Asian and European states might strengthen their allegiance with one side, impacting trade and diplomacy. However, if both regions adopt a more neutral stance, they could potentially maximize economic and diplomatic benefits while mitigating risks to their interests.

Finally, a potential scenario involves an Asia-led economic shift driven by growing Asian markets and initiatives in Europe like the Belt and Road Initiative. If European countries restructure their economies in response, the result could be increased economic and infrastructure connectivity across Eurasia.

Challenges Ahead

Despite the significant potential for development and partnerships, several challenges persist in Asia-EU relations. For instance, US-China tensions create trade barriers, technology limitations, and security issues for both Asia and Europe. If the US prioritizes human rights, cybersecurity, and intellectual property, both regions might face difficulties balancing trade with

China. The growing "tech decoupling" between the West and China is particularly challenging for Europe, which aims to maintain technological leadership while retaining access to Asian markets.

Technological innovations present both opportunities and challenges. The rise of the digital economy, AI, and green technology is transforming global supply chains and the competitive landscape. Both regions must adapt to these technological shifts and ensure responsible growth with appropriate regulations. While Asian nations have established practices regarding technology, Europe's stricter regulations on data privacy and digital rights will require careful consideration regarding implementation and potential impacts on technology ecosystems.

Furthermore, regional conflicts and political instabilities hinder a strong and balanced partnership between Asia and Europe. Disputes in the South China Sea, the Taiwan Strait, and other political disagreements within Asia affect diplomatic, economic, and security relations. For Europe, the ongoing conflict in Ukraine has raised significant security concerns, further complicated by Russia's influence in both Asia and Europe. Any political instability in either region can negatively impact trade, investment, and trust, which are essential for a robust partnership.

Moving forward

Resolving these problems requires strong collaboration between Asia and Europe, focusing on multilateralism, sustainable investment, and appropriate dialogue in sensitive areas. This shift will also strengthen the relationship as Europe and Asia focus on their shared climate, economic, and security interests. By collaborating to address these shared challenges, both regions can achieve greater stability and prosperity.

Multilateralism plays a pivotal role in addressing global issues and fostering cooperation among countries. Adopting this approach allows Asia and Europe to harness the capabilities and resources of numerous countries to formulate effective and multidimensional solutions. Consequently, every country is better represented in decision-making, which increases the sense of shared responsibility for the issues at hand. Using multilateral institutions such as the UN, WTO, and ASEM, both regions can collaborate on maintaining international norms and rules, resolving conflicts, and stimulating sustainable economic development. Strengthening multilateral relations will serve the interests not only of Asia and Europe but also of international peace and development.

These joint efforts regarding renewable energy resources, climate change mitigation, and sustainable development will benefit the environment while creating new economic prospects and increasing job opportunities. Furthermore, greater cooperation in security and intelligence sharing can help both regions address emerging threats, including cyberattacks and transnational crime. Additionally, exchanging ideas and information through educational programs and regional interactions will foster a stronger partnership and promote a sense of global community. Ultimately, this multidisciplinary cooperation will contribute to a better world where Asia and Europe can prosper together.

Conclusion

Asia and Europe, with their unique histories, have an opportunity to improve relations and address pressing issues. Both regions can engage in constructive dialogues through the ASEM, the United Nations, and other trade pacts, which will help develop best practices and partnerships, thereby boosting both regional and global economies.

However, to realize this ambition, both continents must balance intricate power relations, technological innovation, and regional tensions while working toward shared objectives. If all parties approached issues from a perspective of collaboration rather than competition, it would foster greater potential for future interactions.

As mentioned previously, the benefits of Asia and Europe working together converge on one key outcome: a more unified global society. A balance of appreciation, vision, and respect is essential for building a world that prioritizes equity and sustainability.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

Almora, I. R., & Almora's, I. R. (2023, November 23). EU-Japan Region-to-Region Innovation Cooperation: A culmination of project activities and results – International Urban and Regional Cooperation. International Urban and Regional Cooperation. Retrieved October 30, 2024, Available from : https://www.iurc.eu/2023/11/23/eu-japan-region-to-region-innovation-cooperationa-look-project-activities-and-results/

Andrijanič, M. B., & Meissner, P. (2024, June 17). Europe's at risk of losing the global tech race. Retrieved October 30, 2024, Available from : https://www.politico.eu/article/europe-global-tech-race-european-parliament-commission-government-digital-gdp/

ASEM InfoBoard. Retrieved October 27, 2024, Available from : https://aseminfoboard.org/overview/

ASEM InfoBoard. Retrieved October 30, 2024, Available from : https://aseminfoboard.org/overview/

Asia & the Indo-Pacific. (n.d.). Department of Energy. Retrieved October 30, 2024, Available from : https://www.energy.gov/ia/asia-indo-pacific

Asia and Europe can both gain from better trade links. But they need to cooperate, not compete. (2018, October 11). The World Economic Forum. Retrieved October 30, 2024, Available from : https://www.weforum.org/agenda/2018/10/asia-and-europe-can-both-gain-from-better-trade-links-here-s-the-key-to-success/

Association of South East Asian Nations (ASEAN) – EU – Trade and Economic Security. Available from : https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/association-south-east-asian-nations-asean_en

Buchholz K. (14 June, 2021). China's Belt and Road Investment Map.

China's Belt and Road Initiative turns 10. Here's what to know. (2023, November 20). The World Economic Forum. Retrieved October 30, 2024, Available from : https://www.weforum.org/agenda/2023/11/china-belt-road-initiative-trade-bri-silk-r oad/

China-EU – international trade in goods statistics. Available from : https://ec.europa.eu/eurostat/statistics-explained/index.php?title=China-EU_-_international_trade_in_goods_statistics.

Crawford, J., & Tzinieris, S. (2024, June 25). The EU's Evolving China Sanctions Strategy. Lawfare. Retrieved October 30, 2024, Available from : https://www.lawfaremedia.org/article/the-eu-s-evolving-china-sanctions-strategy

Deudney, D. H. (2024, October 16). Belt and Road Initiative (BRI) | Progress, Impact, China, & Facts. Britannica. Retrieved October 30, 2024, Available from : https://www.britannica.com/topic/Belt-and-Road-Initiative

Economic cooperation – EU-ASEAN. (n.d.). EU-ASEAN. Retrieved (October 27, 2024), Available from : https://euinasean.eu/cooperation/economic-cooperation/

EEAS Press Team – EU-Indo Pacific Strategy. Available from : https://www.eeas.europa.eu/eeas/eu-indo-pacific-strategy_en

European Parliament: European Parliamentary Research Service. (2021, April). Prospects for EU-Asia connectivity: The 'European way to connectivity'. Available from : www.europeansources.info. https://www.europeansources.info/record/prospects-for-eu-asia-connectivity-the-european-way-to-connectivity/

European Union Launches 'EU-GCC Green Transition Project' at the World Future Energy Summit. (2024, April 18). EEAS. Retrieved October 30, 2024, Available from : https://www.eeas.europa.eu/delegations/united-arab-emirates/european-union-launches-%E2%80%98eu-gcc-green-transition-project%E2%80%99-world-future-energysummit_en

Garcia-Herrero, A., T. Storella and P. Weil (2024) 'China's influence in the United Nations: words and deeds', Working Paper 19/2024, Bruegel.

Global Overview of the Hi-Tech Goods Industry. (n.d.). Euromonitor International. Retrieved October 30, 2024, Available from : https://www.euromonitor.com/global-overview-of-the-hi-tech-goods-industry/report

Grgić, G. (2024, August 7). *How NATO and its Indo-Pacific partners can work together in an era of strategic competition*. Atlantic Council. Retrieved October 30, 2024, Available from : https://www.atlanticcouncil.org/blogs/new-atlanticist/how-nato-and-its-indo-pacificpartners-can-work-together-in-an-era-of-strategic-competition/

Inforegio – EU-Japan cooperation on regional and urban policy. (n.d.). European Commission. Retrieved October 30, 2024, Available from : https://ec.europa.eu/regional_policy/policy/cooperation/international/japan_en

Johnson, J., & Szewczyk, B. M. (2024, July 26). *Europe's Tech Regulations Are Destroying Its Future*. Foreign Policy. Retrieved October 30, 2024, Available from : https://foreignpolicy.com/2024/07/26/europe-tech-regulation-apple-meta-google-competition/

Katinas, P. (2024, July 12). June 2024 — Monthly analysis of Russian fossil fuel exports and sanctions – Centre for Research on Energy and Clean Air. Centre for Research on Energy and Clean Air. Retrieved October 30, 2024, Available from : https://energyandcleanair.org/june-2024-monthly-analysis-of-russian-fossil-fuel-exports-and-sanctions/

Kennedy, S. U.S.-China Relations in 2024: Managing Competition without Conflict. Available from : – https://www.csis.org/analysis/us-china-relations-2024-managing-competition-without-conflict

Kurin, R. (n.d.). The Silk Road: Connecting People and Cultures | Smithsonian Folklife Festival. Smithsonian Folklife Festival. Retrieved October 27, 2024, Available from : https://festival.si.edu/2002/the-silk-road/the-silk-road-connecting-peoples-and-cultures/smithsonian

Lester, M., & O'Kane, M. (n.d.). *China / PRC*. Global Sanctions. Retrieved October 30, 2024, Available from : https://globalsanctions.com/region/china/

Liew D. – A closer EU-Asia partnership for stronger and more resilient supply chain – CEIAS.eu.

Maizland, L., & Chatzky, A. (2023, February 2). *China's Massive Belt and Road Initiative*. Council on Foreign Relations. Retrieved October 30, 2024, Available from :

https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative

Millett, A. R. (2024, October 27). Korean War | Combatants, Summary, Years, Map, Casualties, & Facts. Britannica. Retrieved October 30, 2024, Available from : https://www.britannica.com/event/Korean-War

Mischke, Massimo, Solveigh, and Smit (2025) – Europe in the intelligent age: From ideas to action – McKinsey & Company.

Okolo, C. T., & Tano, M. (2023, August 9). *Technology competition between nations: Views from industry leaders*. Brookings Institution. Retrieved October 30, 2024, Available from : https://www.brookings.edu/articles/technology-competition-between-nations-views-from-industry-leaders/

Parry, M. (2024). *Chinese counter-sanctions on EU targets*. European Parliament. Retrieved October 30, 2024, Available from : https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/690617/EPRS_ATA(2021)690617_EN.pdf

Perga I. (2025) – The International Implications of the Russo-Ukrainian War.

Pletcher, K. (2024, October 11). *Territorial disputes in the South China Sea | History, Maps, China, Vietnam, Taiwan, Philippines, Malaysia, & Facts*. Britannica. Retrieved October 30, 2024, Available from : https://www.britannica.com/topic/territorial-disputes-in-the-South-China-Sea

Relations with partners in the Indo-Pacific region. (2024, October 24). NATO. Retrieved October 30, 2024, Available from : https://www.nato.int/cps/en/natohq/topics_183254.htm

Shetler, P. (2024, September 2). NATO Emerges as a Platform for Coordinating Indo-Pacific Security Policies. RUSI. Retrieved October 30, 2024, Available from : https://www.rusi.org/explore-our-research/publications/commentary/nato-emerges-platform-coordinating-indo-pacific-security-policies

Talmon, S. (2023, April 25). Germany Defends Use of EU Global Human Rights Sanctions Regime Against China – GPIL. German Practice in International Law. Retrieved October 30, 2024, Available from : https://gpil.jura.uni-bonn.de/2023/04/germany-defends-use-of-eu-global-human-rights-sanctions-regime-against-china/

Territorial Disputes in the South China Sea | Global Conflict Tracker. (2024, September 17). Council on Foreign Relations. Retrieved October 30, 2024, Available from : https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea

The Asia-Europe Meeting (ASEM). (2023, July 26). Ministry of Foreign Affairs of Japan. Retrieved October 30, 2024, Available from : https://www.mofa.go.jp/policy/economy/asem/index.html

The European Union-Russia energy divorce: state of play. (2024, February 22). Bruegel. Retrieved October 30, 2024, Available from : https://www.bruegel.org/analysis/european-union-russia-energy-divorce-state-play

The importance of high – tech companies for EU economy – overview and the EU grand strategies perspective 1. Introduction. (2020, September 8). Sciendo. Retrieved October 30, 2024, Available from : https://intapi.sciendo.com/pdf/10.2478/rsc-2020-0013

The Silk Road: Bridging Middle East and Asia – AMEC. (2024, September 21). AMEC. Retrieved October 27, 2024, Available from : https://amecrd.com/the-silk-road-bridging-middle-east-and-asia/

Today: UN expert to declare illegal all US, EU, British, Canadian sanctions on China. (2024, September 13). UN Watch. Retrieved October 30, 2024, Available from : https://unwatch.org/today-un-expert-to-declare-illegal-all-us-eu-british-canadian-sanctions-on-china/

Voyakin, D. (n.d.). The Great Silk Roads | Silk Roads Programme. UNESCO. Retrieved October 27, 2024, Available from : https://en.unesco.org/silkroad/content/great-silk-roads U.S. – China Relations - https://www.gao.gov/u.s.-china-relations

Winkler, S. Can trade make a sovereign? Taiwan–China–EU relations in the WTO. Asia Europe J 6, 467–485 (2008).

Список використаних джерел

Almora, I. R., & Almora's, I. R. (2023, November 23). EU-Japan Region-to-Region Innovation Cooperation: A culmination of project activities and results – International Urban and Regional Cooperation. International Urban and Regional Cooperation. Retrieved October 30, 2024, Available from : https://www.iurc.eu/2023/11/23/eu-japan-region-to-region-innovation-cooperationa-look-project-activities-and-results/

Andrijanič, M. B., & Meissner, P. (2024, June 17). Europe's at risk of losing the global tech race. Retrieved October 30, 2024, Available from : https://www.politico.eu/article/europe-global-tech-race-european-parliament-commission-government-digital-gdp/

ASEM InfoBoard. Retrieved October 27, 2024, Available from : https://aseminfoboard.org/overview/

ASEM InfoBoard. Retrieved October 30, 2024, Available from : https://aseminfoboard.org/overview/

Asia & the Indo-Pacific. (n.d.). Department of Energy. Retrieved October 30, 2024, Available from : https://www.energy.gov/ia/asia-indo-pacific

Asia and Europe can both gain from better trade links. But they need to cooperate, not compete. (2018, October 11). The World Economic Forum. Retrieved October 30, 2024, Available from : https://www.weforum.org/agenda/2018/10/asia-and-europe-can-both-gain-from-better-trade-links-here-s-the-key-to-success/

Association of South East Asian Nations (ASEAN) – EU – Trade and Economic Security. Available from : https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/association-south-east-asian-nations-asean_en

Buchholz K. (14 June, 2021). China's Belt and Road Investment Map.

China's Belt and Road Initiative turns 10. Here's what to know. (2023, November 20). The World Economic Forum. Retrieved October 30, 2024, Available from : https://www.weforum.org/agenda/2023/11/china-belt-road-initiative-trade-bri-silk-r oad/

China-EU – international trade in goods statistics. Available from : https://ec.europa.eu/eurostat/statistics-explained/index.php?title=China-EU_-_international_trade_in_goods_statistics.

Crawford, J., & Tzinieris, S. (2024, June 25). The EU's Evolving China Sanctions Strategy. Lawfare. Retrieved October 30, 2024, Available from : https://www.lawfaremedia.org/article/the-eu-s-evolving-china-sanctions-strategy

Deudney, D. H. (2024, October 16). Belt and Road Initiative (BRI) | Progress, Impact, China, & Facts. Britannica. Retrieved October 30, 2024, Available from :

https://www.britannica.com/topic/Belt-and-Road-Initiative

Economic cooperation – EU-ASEAN. (n.d.). EU-ASEAN. Retrieved (October 27, 2024), Available from : https://euinasean.eu/cooperation/economic-cooperation/

EEAS Press Team – EU-Indo Pacific Strategy. Available from : https://www.eeas.europa.eu/eeas/eu-indo-pacific-strategy_en

European Parliament: European Parliamentary Research Service. (2021, April). Prospects for EU-Asia connectivity: The 'European way to connectivity'. Available from : www.europeansources.info. https://www.europeansources.info/record/prospects-for-eu-asia-connectivity-the-european-way-to-connectivity/

European Union Launches 'EU-GCC Green Transition Project' at the World Future Energy Summit. (2024, April 18). EEAS. Retrieved October 30, 2024, Available from : https://www.eeas.europa.eu/delegations/united-arab-emirates/european-union-launches-%E2%80%98eu-gcc-green-transition-project%E2%80%99-world-future-energysummit_en

Garcia-Herrero, A., T. Storella and P. Weil (2024) 'China's influence in the United Nations: words and deeds', Working Paper 19/2024, Bruegel.

Global Overview of the Hi-Tech Goods Industry. (n.d.). Euromonitor International. Retrieved October 30, 2024, Available from : https://www.euromonitor.com/global-overview-of-the-hi-tech-goods-industry/report

Grgić, G. (2024, August 7). *How NATO and its Indo-Pacific partners can work together in an era of strategic competition*. Atlantic Council. Retrieved October 30, 2024, Available from : https://www.atlanticcouncil.org/blogs/new-atlanticist/how-nato-and-its-indo-pacificpartners-can-work-together-in-an-era-of-strategic-competition/

Inforegio – EU-Japan cooperation on regional and urban policy. (n.d.). European Commission. Retrieved October 30, 2024, Available from : https://ec.europa.eu/regional_policy/policy/cooperation/international/japan_en

Johnson, J., & Szewczyk, B. M. (2024, July 26). *Europe's Tech Regulations Are Destroying Its Future*. Foreign Policy. Retrieved October 30, 2024, Available from : https://foreignpolicy.com/2024/07/26/europe-tech-regulation-apple-meta-google-competition/

Katinas, P. (2024, July 12). June 2024 — Monthly analysis of Russian fossil fuel exports and sanctions – Centre for Research on Energy and Clean Air. Centre for Research on Energy and Clean Air. Retrieved October 30, 2024, Available from : https://energyandcleanair.org/june-2024-monthly-analysis-of-russian-fossil-fuel-exports-and-sanctions/

Kennedy, S. U.S.-China Relations in 2024: Managing Competition without Conflict. Available from : – https://www.csis.org/analysis/us-china-relations-2024-managing-competition-without-conflict

Kurin, R. (n.d.). The Silk Road: Connecting People and Cultures | Smithsonian Folklife Festival. Smithsonian Folklife Festival. Retrieved October 27, 2024, Available from : https://festival.si.edu/2002/the-silk-road/the-silk-road-connecting-peoples-and-cultures/smithsonian

Lester, M., & O'Kane, M. (n.d.). *China / PRC*. Global Sanctions. Retrieved October 30, 2024, Available from : https://globalsanctions.com/region/china/

Liew D. – A closer EU-Asia partnership for stronger and more resilient supply chain – CEIAS.eu.

Maizland, L., & Chatzky, A. (2023, February 2). *China's Massive Belt and Road Initiative*. Council on

Foreign Relations. Retrieved October 30, 2024, Available from : https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative

Millett, A. R. (2024, October 27). Korean War | Combatants, Summary, Years, Map, Casualties, & Facts. Britannica. Retrieved October 30, 2024, Available from : https://www.britannica.com/event/Korean-War

Mischke, Massimo, Solveigh, and Smit (2025) – Europe in the intelligent age: From ideas to action – McKinsey & Company.

Okolo, C. T., & Tano, M. (2023, August 9). *Technology competition between nations: Views from industry leaders*. Brookings Institution. Retrieved October 30, 2024, Available from : https://www.brookings.edu/articles/technology-competition-between-nations-views-from-industry-leaders/

Parry, M. (2024). *Chinese counter-sanctions on EU targets*. European Parliament. Retrieved October 30, 2024, Available from : https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/690617/EPRS_ATA(2021)690617_EN.pdf

Perga I. (2025) – The International Implications of the Russo-Ukrainian War.

Pletcher, K. (2024, October 11). *Territorial disputes in the South China Sea | History, Maps, China, Vietnam, Taiwan, Philippines, Malaysia, & Facts*. Britannica. Retrieved October 30, 2024, Available from : https://www.britannica.com/topic/territorial-disputes-in-the-South-China-Sea

Relations with partners in the Indo-Pacific region. (2024, October 24). NATO. Retrieved October 30, 2024, Available from : https://www.nato.int/cps/en/natohq/topics_183254.htm

Shetler, P. (2024, September 2). NATO Emerges as a Platform for Coordinating Indo-Pacific Security Policies. RUSI. Retrieved October 30, 2024, Available from : https://www.rusi.org/explore-our-research/publications/commentary/nato-emerges-platform-coordinating-indo-pacific-security-policies

Talmon, S. (2023, April 25). Germany Defends Use of EU Global Human Rights Sanctions Regime Against China – GPIL. German Practice in International Law. Retrieved October 30, 2024, Available from : https://gpil.jura.uni-bonn.de/2023/04/germany-defends-use-of-eu-global-human-rights-sanctions-regime-against-china/

Territorial Disputes in the South China Sea | Global Conflict Tracker. (2024, September 17). Council on Foreign Relations. Retrieved October 30, 2024, Available from : https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea

The Asia-Europe Meeting (ASEM). (2023, July 26). Ministry of Foreign Affairs of Japan. Retrieved October 30, 2024, Available from : https://www.mofa.go.jp/policy/economy/asem/index.html

The European Union-Russia energy divorce: state of play. (2024, February 22). Bruegel. Retrieved October 30, 2024, Available from : https://www.bruegel.org/analysis/european-union-russia-energy-divorce-state-play

The importance of high – tech companies for EU economy – overview and the EU grand strategies perspective 1. Introduction. (2020, September 8). Sciendo. Retrieved October 30, 2024, Available from : https://intapi.sciendo.com/pdf/10.2478/rsc-2020-0013

The Silk Road: Bridging Middle East and Asia – AMEC. (2024, September 21). AMEC. Retrieved October 27, 2024, Available from : https://amecrd.com/the-silk-road-bridging-middle-east-

and-asia/

Today: UN expert to declare illegal all US, EU, British, Canadian sanctions on China. (2024, September 13). UN Watch. Retrieved October 30, 2024, Available from : https://unwatch.org/today-un-expert-to-declare-illegal-all-us-eu-british-canadian-sanctions-on-china/

Voyakin, D. (n.d.). The Great Silk Roads | Silk Roads Programme. UNESCO. Retrieved October 27, 2024, Available from : https://en.unesco.org/silkroad/content/great-silk-roads U.S. – China Relations - https://www.gao.gov/u.s.-china-relations

Winkler, S. Can trade make a sovereign? Taiwan–China–EU relations in the WTO. Asia Europe J 6, 467–485 (2008).

Організація руху опору на території України та території країни противника для протидії збройним силам країни агресора

Organization of the resistance movement in the territory of Ukraine and territory of the enemy country to counter the armed forces of the aggressor country

Олег Соколовський
старший науковий співробітник науково-дослідного відділу проблем розвитку та застосування частин і підрозділів військової розвідки та Сил спеціальних операцій, e-mail: bizoklop@ukr.net, ORCID: 0009-0002-5234-2590

Військова академія, м. Одеса, Україна

Oleg Sokolovsky
Senior Research Fellow of the Research Department on the Development and Employment of Military Intelligence Units and Special Operations Forces, e-mail: bizoklop@ukr.net, ORCID: 0009-0002-5234-2590

Military Academy, Odessa, Ukraine

Received: April 11, 2025 | Revised: April 20, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.4

Мета роботи: полягає в розкритті підходів до ефективного планування, організації та ведення діяльності руху опору в умовах збройної агресії. дослідження шляхів удосконалення існуючих механізмів опору, визначення ролі структур, залучених до його організації, а також формування практичних рекомендацій для дій на потенційно окупованих територіях.

Метод дослідження: Аналіз та синтез.

Результати дослідження: У процесі дослідження визначено яким чином повинна бути організована робота по плануванню та веденню діяльності руху опору та відпрацьовані пропозиції по її удосконаленню. Визначені завдання структурам, які беруть участь в організації руху опору та безпосередньо групам руху опору на територіях, які противник буде намагатись окупувати.

Цінність дослідження: Стаття може буде корисною як науковцям, що вивчають проблемні питання пов'язані з організацією і управлінням руху опору так і військовослужбовцям, державним управлінцям, що безпосередньо займаються оперативним та стратегічним плануванням та розвитком оборонного сектору.

Тип статті: теоретичний.

Purpose: is to reveal approaches to effective planning, organization and conduct of resistance activities in conditions of armed aggression. Research into ways to improve existing resistance mechanisms, determine the role of structures involved in its organization, and formulate practical recommendations for actions in potentially occupied territories.

Method: analysis and synthesis.

Research results: In the course of the study, the framework for organizing the planning and execution of resistance movement activities was defined, and proposals for its improvement were developed. The tasks of the structures involved in organizing the resistance movement, as well as those of the resistance groups operating in the territories the enemy may attempt to occupy, were identified.

Value: The article may be useful for both scholars studying issues related to the organization and management of resistance movements, as well as military personnel and public officials directly involved in operational and strategic planning and the development of the defense sector.

Type of article: theoretical.

Ключові слова: оборонна сфера, рух опору, групи руху опору, оперативне середовище, критичні об'єкти інфраструктури.

Key words: defense sphere, resistance movement, resistance movement groups, operational environment, critical infrastructure facilities.

Вступ

Організація руху опору проти окупаційних військ на території України становить ключовий елемент загальнонаціональної боротьби за збереження державного суверенітету та територіальної цілісності. Актуальність дослідження цієї проблематики зумовлена сучасними умовами війни, у яких існують райони, розташовані як на тимчасово окупованих територіях України, так і безпосередньо на території противника, де потенційно можливе формування осередків опору.

Незважаючи на практичну значущість вказаного напряму, чинні керівні документи, настанови та статути не містять достатньо повного та систематизованого викладу положень щодо організації руху опору на тактичному рівні. Внаслідок цього дії підрозділів Збройних Сил України тактичного й оперативного рівнів, а також органів місцевого самоврядування у межах

визначених районів не є належним чином нормативно врегульованими. Крім того, території територіальних громад переважно залишаються непідготовленими до організованого спротиву збройній агресії та дій диверсійно-розвідувальних груп противника.

У зв'язку з вищезазначеним виникає необхідність у проведенні ґрунтовного наукового аналізу проблем організації руху опору, зокрема на тактичному рівні, з метою розроблення відповідних пропозицій та внесення змін до керівних документів, що регламентують бойову діяльність. Окремої уваги потребує інтеграція результатів дослідження до освітніх програм та навчальних планів з підготовки офіцерського складу до виконання бойових завдань у специфічних умовах ведення операцій на тимчасово окупованих територіях та в районах активного спротиву.

Теоретичні основи дослідження

Рух опору є ключовим компонентом асиметричної боротьби в умовах збройного конфлікту, що передбачає ведення бойових дій поза межами традиційного фронту. Його належна організація на території України, а також потенційна активність на тимчасово окупованих територіях та в глибокому тилу країни-агресора, є стратегічно важливою складовою загальнодержавної системи оборони.

Дослідження цього феномену здійснюється в рамках військової науки, зокрема в аспектах стратегії ведення бойових дій, гібридної війни, інформаційно-психологічних операцій та національної безпеки. Незважаючи на наявність публікацій з окремих аспектів зазначеної проблематики, більшість ґрунтовних досліджень мають обмежений доступ у зв'язку з наданням грифу таємності. Відтак, постає необхідність у систематизації, узагальненні та адаптації наявних знань для підготовки фахівців, які будуть залучені до організації руху опору на рівні державних органів влади, місцевого самоврядування та закладів освіти.

Нормативну базу організації руху опору становлять, насамперед, Закон України "Про основи національного спротиву" (ВВР, 2021, № 41, ст.339), Закон України про внесення змін до деяких законів України щодо уточнення завдань та основ підготовки і ведення національного спротиву (ВВР, 2023, № 14, ст.35), а також наказ Міністерства оборони України від 26.03.2024 № 198 "Про затвердження змін до Переліку військово-облікових спеціальностей осіб офіцерського складу". Ці документи визначають цілі, завдання та механізми функціонування руху опору як інструмента забезпечення обороноздатності держави.

Згідно із чинним законодавством, до завдань руху опору належать: формування осередків спротиву та забезпечення їх спроможностей; протидія діям військ (сил) агресора; участь у проведенні спеціальних операцій (розвідувальних, інформаційно-психологічних тощо); а також підготовка громадян до участі у русі опору. Окрему увагу приділено формуванню національної готовності через систему підготовки цивільного населення — як в аспекті загальновійськових знань і навичок, так і у контексті військово-патріотичного виховання.

Підготовка громадян до спротиву поділяється на початкову та базову. Початкова організовується у закладах загальної середньої, професійної та фахової передвищої освіти за участю Міністерства оборони та центрального органу виконавчої влади у сфері освіти. Базова підготовка, що здійснюється для громадян віком від 18 років, які не проходять військову службу, включає проведення навчальних зборів, курсів та тренувань під егідою Міністерства оборони [1].

Командування Сил спеціальних операцій Збройних Сил України виконує функції органу управління рухом опору. Воно забезпечує планування, підготовку та контроль за реалізацією відповідних заходів, бере участь у розробці нормативних актів, організовує аналіз ситуації в районах можливого або актуального спротиву, а також відповідає за оперативне реагування, кадровий відбір і забезпечення ресурсами.

Важливим кроком на шляху удосконалення правової бази стало ухвалення Закону України № 7180 “Про внесення змін до деяких законодавчих актів України”, що набув чинності з метою адаптації оборонного законодавства до нових викликів. Закон створює правові умови для здійснення розвідувальної діяльності Силами спеціальних операцій на тимчасово окупованих територіях та покращення ефективності національного спротиву як системної відповіді на збройну агресію.

У контексті набутого бойового досвіду та трансформації характеру війни, питання організації руху опору потребує подальшого наукового осмислення, розробки методичних рекомендацій та впровадження відповідних змін до керівних документів. Це дозволить забезпечити стійкість оборони, активну участь населення у спротиві та посилення обороноздатності держави в умовах тривалого гібридного протистояння.

Постановка проблеми

Практичний досвід ведення бойових дій свідчить, що недооцінка значення підготовки населення та територій до діяльності груп руху опору у передвоєнний період не дозволила у перші дні широкомасштабного вторгнення завдати противнику таких втрат, які могли б змусити його відмовитися від досягнення поставлених цілей, принаймні на окремих оперативних напрямках.

Станом на сьогодні противник не відмовився від своїх зазіхань на нові території України, що обумовлює критичну необхідність системної та всебічної підготовки як населення, так і оперативного середовища для забезпечення ефективних дій груп руху опору в умовах гібридного збройного протистояння.

Результати

Організація руху опору проти окупаційної влади є складним і багатокомпонентним процесом, який охоплює заходи зі створення підпільної інфраструктури, протидії інформаційному впливу противника, забезпечення збройного спротиву, гуманітарної підтримки населення, а також налагодження взаємодії з державними інституціями та міжнародною спільнотою. Основною метою є збереження національної ідентичності, підрив стабільності окупаційного режиму та сприяння загальнодержавній обороні.

Робота з формування руху опору має розпочинатися у мирний час та активізуватися у загрозливий період, відповідно до оцінки ймовірного характеру дій противника і власних оборонних спроможностей. Це забезпечує можливість превентивного впливу на плани противника, зниження ефективності його наступальних дій та виграш у часі для сил оборони. Вказана діяльність повинна здійснюватися на всіх рівнях — як силами сектору безпеки і оборони, так і органами державної влади, місцевого самоврядування, системою освіти та керівництвом підприємств незалежно від форми власності. Важливою передумовою є дотримання принципів конспірації — залучення до діяльності обмеженого кола осіб, які інформуються виключно в межах необхідного знання (principle of need to know).

Ключові напрямки організації руху опору:

1. Створення підпільної мережі.
2. Інформаційний спротив.
3. Збройний спротив.
4. Гуманітарна діяльність.
5. Міжнародна підтримка.
6. Конспірація та заходи безпеки.
7. Координація з органами влади.
8. Морально-психологічна підтримка населення.
9. Підготовка територій до дій сил опору.

Створення підпільної мережі полягає у формуванні осередків спротиву на територіях, які мають оперативне або стратегічне значення для противника. Осередки мають чітку структуризацію за напрямами діяльності (інформаційна, збройна, гуманітарна тощо), а їх управління здійснюється із використанням сучасних технологій захищеного зв'язку (VPN, шифровані месенджери). Обов'язковим елементом є планування евакуаційних маршрутів для виведення груп з району операцій, у тому числі — на територію противника.

Інформаційний спротив включає протидію ворожій пропаганді шляхом створення альтернативних джерел інформації (соціальні мережі, підпільна преса), поширення достовірних відомостей про ситуацію в Україні як серед населення на окупованих територіях, так і на міжнародному рівні, а також здійснення інформаційно-психологічних операцій і кібератак проти окупаційних структур.

Збройний спротив передбачає організацію партизанських загонів, проведення диверсій на об'єктах інфраструктури противника, ліквідацію ворожих командних пунктів і ключових колаборантів, а також створення формувань, здатних діяти на шляхах просування противника до об'єктів критичної інфраструктури. Забезпечення таких формувань зброєю, вибуховими речовинами і спеціальними засобами є обов'язковою умовою їхньої ефективності.

Гуманітарна діяльність включає забезпечення цивільного населення життєво необхідними ресурсами (продукти, ліки, засоби гігієни), організацію безпечних маршрутів евакуації, підтримку родин загиблих, поранених та полонених учасників руху опору.

Міжнародна підтримка забезпечується через тиск на країну-агресора (санкції, дипломатичні заходи), взаємодію з правозахисними організаціями для документування воєнних злочинів, а також налагодження каналів постачання ресурсів та фінансової допомоги з-за кордону.

Конспірація і безпека є критично важливими елементами всієї структури руху опору. Підготовка особового складу повинна включати навчання методам конспіративної діяльності, захищеного зв'язку, планування евакуації і заміни груп у разі їх викриття.

Координація з органами влади має забезпечуватись визначеними представниками Сил спеціальних операцій, які виступають посередниками між підпільними структурами і ЗСУ, СБУ, місцевими адміністраціями. Державна політика має передбачати залучення емігрантів і патріотично налаштованих громадян до системи спротиву та обмін розвідувальними даними.

Моральна підтримка населення охоплює проведення патріотичних заходів, поширення культурних і національних символів, навчання основам самозахисту, тактичній медицині та домедичній допомозі, а також забезпечення інформаційного супроводу про здобутки сил оборони через підпільні ресурси.

Підготовка територій до спротиву повинна здійснюватися на постійній основі. Доцільним є нормативне закріплення вимог до будівель, інфраструктури та комунікацій, які можуть бути використані для оборони. Необхідно облаштовувати схованки, формувати ландшафтні та інженерні перешкоди для ускладнення просування противника.

Організація руху опору на території противника

Цей напрям є особливо складним через тотальний контроль державної влади агресора, репресивний апарат та обмеження громадянських свобод. Недостатня координація між учасниками операцій може призвести до провалу.

Ключові аспекти спротиву на території противника:

- формування мережі спротиву;
- інформаційна боротьба;
- масові акції протесту;
- диверсійна діяльність;
- міжнародна підтримка;

- робота з місцевим населенням;
- підтримка етнічного і регіонального опору;
- ведення психологічної війни.

Формування мережі передбачає створення автономних малочисельних груп (3–5 осіб), використання шифрованих каналів зв'язку, залучення активістів, ветеранів, інтелігенції.

Інформаційна боротьба включає антипровладну пропаганду, поширення викривальних матеріалів, хакерські атаки на системи державного управління, мобілізацію діаспори, організацію підпільних дискусійних клубів.

Масові акції протесту — це організація стихійних виступів, страйків, флешмобів, залучення робітників до саботажу, використання родинних і кримінальних зв'язків для поширення інформації, участь лідерів громадської думки у протестах.

Диверсії — це цілеспрямоване ураження військових та інфраструктурних об'єктів, зрив проектів влади, ліквідація ключових фігур.

Міжнародна підтримка — встановлення контактів з правозахисниками, імплементація санкцій, інформування про злочини агресора.

Робота з населенням — мобілізація етнічних меншин, молоді, біженців, репресованих; захист їхніх прав та залучення до спротиву.

Підтримка регіонального опору — сприяння автономістським ініціативам, протидія централізації, зміцнення регіональної ідентичності.

Психологічна війна — кампанії деморалізації населення противника через інформацію про втрати, поразки, корупцію в системі влади.

Можливості для розвитку руху опору. Економічна криза в державі-агресорі матиме системні наслідки, що сприятимуть послабленню її економічного та військового потенціалу. Це, своєю чергою, викликатиме зростання соціального невдоволення серед окремих верств населення, що створюватиме сприятливі умови для активізації саботажної діяльності, організації страйків та інших форм протесту. Такі прояви можуть бути використані як додатковий ресурс для залучення нових учасників до руху опору та підвищення ефективності його дій.

Регіональні та міжетнічні конфлікти на території країни-агресора відволікають ресурси та увагу силових структур, змушуючи їх розпорошувати зусилля на внутрішню стабілізацію. На початкових етапах це, ймовірно, призведе до посилення репресивних заходів, однак у довгостроковій перспективі зростання масштабів та географії таких конфліктів сприятиме дестабілізації режиму й надасть додаткові можливості для дій підпільних структур.

Міжнародна ізоляція держави-агресора, яка виступає порушником міжнародного права, чинить негативний вплив як на її економічну систему загалом, так і на свідомість частини прогресивного населення. Ефективність санкційної політики безпосередньо залежить від згуртованості коаліції демократичних держав. Найбільшого ефекту слід очікувати у разі спрямованого впливу на великий бізнес, втрати якого можуть зумовити наростання протестних настроїв спочатку в побутовому середовищі (побутові обговорення, розмови у громадських місцях), а згодом — у трудових колективах і під час масових акцій.

Важливим морально-психологічним фактором виступає успішна оборона держави-жертви агресії. Поширення достовірної інформації про перемоги сил оборони через наявні канали комунікації може стати каталізатором для радикалізації частини населення країни-агресора, яка не підтримує політику війни й окупації. Це, своєю чергою, сприятиме їх залученню до активної участі у русі спротиву.

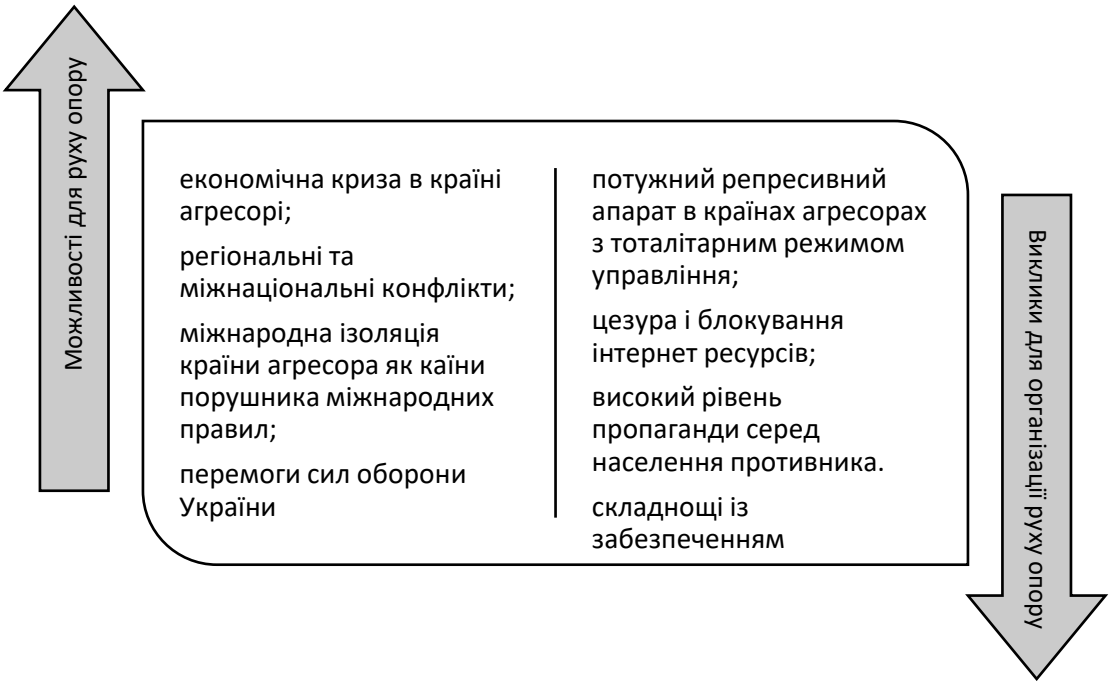


Рисунок. Перспективи та виклики для організації руху опору

Основні виклики для організації руху опору. Наявність потужного репресивного апарату в державах із тоталітарними формами управління є одним із ключових бар'єрів для формування та функціонування організованого спротиву. Проте за умов виникнення численних внутрішніх кризових ситуацій — міжетнічних конфліктів, протестів, соціальних заворушень — сили безпеки агресора будуть змушені розпорошувати ресурси, що відкриває вікно можливостей для підпільної діяльності.

Використання державою-агресором інструментів цензури, блокування інтернет-ресурсів, тотального контролю над інформаційним простором, а також залучення до репресивних і пропагандистських дій парамілітарних структур, організованих злочинних груп, діячів шоу-бізнесу, наукових та медійних інституцій вимагає застосування високотехнологічних засобів протидії. Йдеться, зокрема, про використання штучного інтелекту, новітніх технологій захищеної комунікації та ведення кібервійн.

Поширеність ворожої пропаганди серед населення агресора обумовлює потребу в постійному інформаційному супроводі руху опору, включно з контрпропагандою, розвінчанням фейкових наративів та донесенням об'єктивної інформації про наслідки агресії.

Складнощі із матеріально-технічним забезпеченням руху опору та обмеженість кадрового й ресурсного резерву можуть бути частково подолані шляхом реалізації зазначених вище можливостей, включно із залученням внутрішніх ресурсів і підтримки із зовні.

Організація руху опору — це надзвичайно складна та ризикована діяльність, що потребує ретельної координації дій усіх залучених суб'єктів за умов жорсткого дотримання принципів конспірації. Ключовим елементом у цій системі є орган управління, який має забезпечити планування, підготовку та керівництво діяльністю руху на тимчасово окупованих територіях, а також на території держави-агресора. З огляду на специфіку завдань, створення такого органу є компетенцією Сил спеціальних операцій Збройних Сил України. Повноваження цього органу повинні бути чітко визначені в законодавчих та нормативних актах із відповідним рівнем секретності.

Підготовка територій до можливої окупації, включно з об'єктами критичної інфраструктури незалежно від форми власності, має здійснюватися з урахуванням можливості їх подальшого використання силами руху опору. Досягнення високого рівня готовності у цій

сфері неможливе без тісної взаємодії з органами місцевого самоврядування, державними інституціями, а також підприємствами всіх форм власності.

Економічна діяльність суб'єктів господарювання повинна бути нормативно врегульована з урахуванням імовірності тимчасової втрати контролю над окремими територіями. Зокрема, доцільно передбачити наявність планів евакуації критичних виробництв у безпечні регіони, забезпечити резервні логістичні маршрути для доставки гуманітарної допомоги та вивезення населення. Усі ці заходи мають бути завчасно розроблені, дубльовані та захищені від можливих втручань з боку противника.

Висновки

Організація руху опору проти окупаційної влади охоплює комплекс заходів, спрямованих на забезпечення ефективної протидії агресору та збереження національної ідентичності населення. Попри наявність певної кількості публікацій з цієї тематики, інформація у відкритих джерелах є фрагментарною, що зумовлює потребу у систематизації наявних даних, проведенні глибокого аналізу та формулюванні обґрунтованих висновків.

Необхідно активізувати впровадження напрацьованих результатів у систему військової освіти, зокрема через інтеграцію відповідних тематичних модулів до навчальних планів підготовки офіцерського складу. Це дозволить сформувати у майбутніх командирів необхідні знання та навички для планування і здійснення дій у районах, де передбачається організація руху опору.

Доцільним є проведення комплексного наукового аналізу проблематики організації спротиву з подальшим внесенням змін і доповнень до чинних керівних документів. Актуальність цього напряму зумовлена необхідністю адекватної відповіді на зміну характеру сучасних воєн, зокрема зростанням ролі асиметричних дій, збройного спротиву в тилу противника та використанням гібридних форм впливу.

Організацію та створення мережі руху опору слід розпочинати завчасно — у мирний час, із подальшим нарощуванням активності у період загрози або безпосередньої агресії. Такий підхід забезпечує можливість випереджальних дій, ускладнюючи реалізацію противником оперативно-тактичних завдань на захоплених територіях.

Робота у цьому напрямі повинна здійснюватися на всіх рівнях — як силами оборони, так і органами державної влади та місцевого самоврядування. Її виконання має бути організоване у максимально закритому форматі, з залученням обмеженого кола спеціально визначених осіб, ознайомлених із завданнями виключно в межах власної відповідальності (з дотриманням принципу "need to know").

Організація руху опору та керівництво його діями належить до компетенції Сил спеціальних операцій. Саме в межах Сил спеціальних операцій створюється відповідний орган управління, уповноважений здійснювати планування, підготовку і координацію дій сил спротиву на тимчасово окупованих територіях, а також — за необхідності — на території держави-агресора.

Важливою складовою оборонного планування має стати нормативне врегулювання економічної діяльності підприємств усіх форм власності з урахуванням імовірності окупації окремих територій. Необхідно передбачити механізми оперативного переміщення критично важливих підприємств у безпечні райони в загрозливий період. Логістичні маршрути для постачання гуманітарної допомоги, а також шляхи евакуації населення мають бути продубльовані та захищені від потенційних втручань з боку противника.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Про внесення змін до деяких законів України щодо удосконалення системи підготовки громадян України до військової служби: Закон України від 22.05.2024 № 3724-IX Відомості Верховної Ради (ВВР), 2024, № 31, ст.229 URL: https://zakon.rada.gov.ua/laws/show/3724-20#n28
2. Про внесення змін до деяких законів України щодо уточнення завдань та основ підготовки і ведення національного спротиву: Законі України від 27.01.2022 № 2024-IX. Відомості Верховної Ради України (ВВР), 2023, № 14, ст.35 URL: https://zakon.rada.gov.ua/laws/show/2024-20#Text
3. Про основи національного спротиву: Законі України від 16.07.2021 № 1702-IX Відомості Верховної Ради (ВВР), 2021, № 41, ст.339 URL: https://zakon.rada.gov.ua/laws/show/1702-20#Text
4. Про затвердження змін до Переліку військово-облікових спеціальностей осіб офіцерського складу та Переліку військово-облікових спеціальностей: Наказі МО України від 26.03.2024 № 198. URL: https://zakon.rada.gov.ua/laws/show/z0458-24#Text
5. Кілька фактів про Рух опору та Сили спеціальних операцій ЗСУ. Espreso.tv (укр.). Процитовано 29 липня, 2023. URL: https://espreso.tv/den-sso-kilka-faktiv-pro-rukh-oporu-ta-sili-spetsialnikh-operatsiy-zsu
6. Командувач ССО: Рух опору діє на всіх операційних напрямках. Українська правда (укр.). 10 січня 2023. URL: https://www.pravda.com.ua/news/2023/01/10/7384226/
7. Конопльова, Марина (4 червня 2022). Рух опору ССО виявив та знищив станцію зв'язку окупантів на Харківщині (ВІДЕО). ШоТам (укр). URL: https://shotam.info/rukh-oporu-sso-vyiavyv-ta-znyshchyv-stantsiiu-zv-iazku-okupantiv-na-kharkivshchyni-video/

ССО запустили кампанію про спротив у тилу. Мілітарний (укр.). 30 Серпня, 2024. URL: https://mil.in.ua/uk/news/sso-zapustyly-kampaniyu-pro-sprotyv-u-tylu/

9. ССО: Партизани підірвали в окупованому Мелітополі потяг – DW – 13.10.2023. dw.com (укр.). URL: https://www.dw.com/uk/sso-partizani-pidirvali-v-okupovanomu-melitopoli-potag/a-67090479
10. Як українські партизани чинять опір російській окупації на півдні України. BBC News Україна (укр.). 2024. URL: https://www.bbc.com/ukrainian/features-62345044
11. How the covert Ukrainian resistance movement is operating behind Russian lines. Sky News (англ.). 16 жовтня 2024. URL: https://news.sky.com/story/how-the-covert-ukrainian-resistance-movement-is-operating-behind-russian-lines-13202230

References

1. Zakon Ukrayiny «Pro vnesennya zmin do deyakykh zakoniv Ukrayiny shchodo udoskonalennya systemy pidhotovky hromadyan Ukrayiny do viys'kovoyi sluzhby» № 3724-IX vid 22.05.2024 Vidomosti Verkhovnoyi Rady (VVR), 2024, № 31, st.229 [Law of Ukraine "On Amendments to Certain Laws of Ukraine Regarding Improving the System of Preparing Ukrainian Citizens for Military Service"] Available from : https://zakon.rada.gov.ua/laws/show/3724-20#n28
2. Zakon Ukrayiny «Pro vnesennya zmin do deyakykh zakoniv Ukrayiny shchodo utochnennya zavdan' ta osnov pidhotovky i vedennya natsional'noho sprotyvu» vid 27.01.2022 № 2024-IX. Vidomosti Verkhovnoyi Rady Ukrayiny (VVR), 2023 , № 14, st.35 [Law of Ukraine "On Amendments to Certain Laws of Ukraine Regarding Clarifying the Tasks and Fundamentals

of Preparing and Conducting National Resistance"] Available from : https://zakon.rada.gov.ua/laws/show/2024-20#Text

3. Zakon Ukrayiny «Pro osnovy natsional'noho» vid 16.07.2021 № 1702-IX Vidomosti Verkhovnoyi Rady (VVR), 2021, № 41, [Law of Ukraine "On the Fundamentals of National" dated 16.07.2021 No. 1702-IX Bulletin of the Verkhovna Rada (VVR)] st.339. Available from : https://zakon.rada.gov.ua/laws/show/1702-20#Text
4. Nakazi MO Ukrayiny «Pro zatverdzhennya zmin do Pereliku viys'kovo-oblikovykh spetsial'nostey osib ofitsers'koho skladu ta Pereliku viys'kovo-oblikovykh spetsial'nostey» vid 26.03.2024 № 198 [Order of the Ministry of Defense of Ukraine "On Approval of Amendments to the List of Military-Accounting Specialties of Officers and the List of Military-Accounting Specialties"] Available from : https://zakon.rada.gov.ua/laws/show/z0458-24#Text
5. Kil'ka faktiv pro Rukh oporu ta Syly spetsial'nykh operatsiy ZSU. Espreso.tv (ukr.). Protsytovano 29 lypnya, 2023 [A few facts about the Resistance Movement and the Special Operations Forces of the Armed Forces of Ukraine. Espreso.tv (Ukrainian)]. Available from : https://espreso.tv/den-sso-kilka-faktiv-pro-rukh-oporu-ta-sili-spetsialnikh-operatsiy-zsu
6. Komanduvach SSO: Rukh oporu diye na vsikh operatsiynykh napryamkakh. Ukrayins'ka pravda (ukr.). 10 sichnya 2023.[Commander of the Special Operations Forces: The Resistance Movement operates in all operational areas. Ukrainian Pravda (Ukrainian).]. Available from : https://www.pravda.com.ua/news/2023/01/10/7384226/
7. Konopl'ova, Maryna (4 chervnya 2022). Rukh oporu SSO vyyavyv ta znyshchyv stantsiyu zv"yazku okupantiv na Kharkivshchyni (VIDEO). ShoTam (ukr [Konoplyova, Maryna (June 4, 2022). The Special Operations Forces resistance movement discovered and destroyed the occupiers' communications station in the Kharkiv region]. Available from : https://shotam.info/rukh-oporu-sso-vyiavyv-ta-znyshchyv-stantsiiu-zv-iazku-okupantiv-na-kharkivshchyni-video/
8. SSO zapustyly kampaniyu pro sprotyv u tylu. Militarnyy (ukr.). 30 Serpnya, 2024 . [SSO launched a campaign of resistance in the rear. Military (Ukr).]. Available from : https://mil.in.ua/uk/news/sso-zapustyly-kampaniyu-pro-sprotyv-u-tylu/
9. SSO: Partyzany pidirvaly v okupovanomu Melitopoli potyah – DW – 13.10.2023. dw.com (ukr.). [SSO: Partisans blew up a train in occupied Melitopol – DW – 10/13/2023. dw.com (Ukr)]. Available from : https://www.dw.com/uk/sso-partizani-pidirvali-v-okupovanomu-melitopoli-potag/a-67090479
10. Yak ukrayins'ki partyzany chynyat' opir rosiys'kiy okupatsiyi na pivdni Ukrayiny. BBC News [How Ukrainian partisans resist the Russian occupation in southern Ukraine. BBC News Ukraine (ukr.)]Ukrayina (ukr.). 2024. Available from : https://www.bbc.com/ukrainian/features-62345044
11. How the covert Ukrainian resistance movement is operating behind Russian lines. Sky News (англ.). 16 Oct. 2024. Available from : https://news.sky.com/story/how-the-covert-ukrainian-resistance-movement-is-operating-behind-russian-lines-13202230

Методика впровадження технологій штучного інтелекту в процес рекрутингу в Збройних Силах України

Methodology for Implementing artificial Intelligence technologies in the recruitment process of the Armed Forces of Ukraine

Олександр Сампір [A]
Corresponding author: доктор філософії, начальник науково-дослідного відділу, інституту логістики та підтримки військ (сил), e-mail: sampir1984@ukr.net, ORCID: 0000-0002-3564-1997

Ілона Сампір [A]
старший науковий співробітник кафедри менеджменту персоналу і підготовки військ (сил), e-mail: sampir1986@ukr.net, ORCID: 0000-0003-3194-893X

Анна Федоренко [B]
студентка магістратури, e-mail: fedorenkoanna197@gmail.com, ORCID: 0009-0009-8254-7045

Oleksandr Sampir [A]
Corresponding author: PhD, Head of the Research Department of the Institute of Logistics and Support of Troops (Forces), e-mail: sampir1984@ukr.net, ORCID: 0000-0002-3564-1997

Ilona Sampir [A]
Senior Research Fellow of the Department of Personnel Management and Troop (Forces) Training, e-mail: sampir1986@ukr.net, ORCID: 0000-0003-3194-893X

Anna Fedorenko [B]
master's student, e-mail: fedorenkoanna197@gmail.com, ORCID: 0009-0009-8254-7045

[A] Національний університет оборони України, м. Київ, Україна
[B] Державний університет інформаційно-комунікаційних технологій, м. Київ, Україна

[A] National Defence University of Ukraine, Kyiv, Ukraine
[B] State University of Information and Communication Technologies, Kyiv, Ukraine

Received: April 11, 2025 | Revised: April 20, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.5

Мета роботи: є пошук дієвих способів та інноваційно науково-технічних рішень для підвищення ефективності процесу пошуку та відбору кандидатів на військову службу в ході рекрутингу в Збройних Силах України.
Метод дослідження: метод аналізу та прогнозування на основі машинного навчання із застосуванням алгоритму Random Forest для визначення найкращих кандидатів на військову службу відповідно до заданої посади.
Результати дослідження: розроблено, навчено та протестовано модель машинного навчання, яка виконує пошук та відбір найкращого кандидата на військову службу на основі їхніх характеристик.
Тип статті: науково-практична.

Purpose: is the search for effective methods and innovative scientific and technical solutions to increase the efficiency of the process of searching and selecting candidates for military service during recruitment in the Armed Forces of Ukraine.
Method: a machine learning-based analysis and forecasting method using the Random Forest algorithm to identify the best candidates for military service according to a given position.
Findings: developed, trained, and tested a machine learning model that searches and selects the best candidate for military service based on their characteristics.
Papertype: scientific and practical.

Ключові слова: рекрутинг, пошук та відбір кандидатів, автоматизація процесу прийняття рішень, система, алгоритм, машинне навчання, штучний інтелект, нейромережа, мова програмування Python.

Key words: recruiting, candidate search and selection, decision-making process automation, system, algorithm, machine learning, artificial intelligence, neural network, Python programming language.

Вступ

Сучасний етап розвитку інформаційних технологій відкриває широкі можливості для підвищення ефективності процесів у різних сферах діяльності, зокрема у військовій галузі. Інтеграція високотехнологічних рішень у повсякденну та службову діяльність дозволяє суттєво скоротити часові витрати на виконання рутинних завдань, а також підвищити якість управлінських рішень завдяки більш точному аналізу даних. Особливої актуальності набуває впровадження технологій штучного інтелекту (ШІ) та машинного навчання (МН) у сферу військового рекрутингу, що зумовлено необхідністю оперативного та ефективного добору кадрів в умовах зростання загроз національній безпеці та обмеженості людських і матеріальних ресурсів.

У межах даного дослідження проаналізовано потенціал застосування алгоритмів машинного навчання, зокрема методу Random Forest, з метою автоматизації процесу пошуку та відбору кандидатів на військову службу у Збройних Силах України. Реалізація запропонованого підходу дозволяє забезпечити підвищення об'єктивності ухвалення рішень, покращення точності відбору персоналу та загальне підвищення ефективності функціонування системи кадрового забезпечення в оборонному секторі.

Теоретичні основи дослідження

Упродовж останніх років спостерігається інтенсивне зростання інтересу до застосування технологій ШІ та МН у сфері рекрутингу та кадрового відбору. Особливої актуальності це питання набуває в межах військових організаційних структур, де забезпечення ефективного добору персоналу є одним із пріоритетних завдань в умовах динамічних змін глобального безпекового середовища, а також безпосередньо під час участі у бойових діях.

Дослідження з проблематики застосування алгоритмів машинного навчання у процесах рекрутингу збройних сил ґрунтуються на низці сучасних підходів, серед яких особливе місце займають методи класифікації, зокрема алгоритм Random Forest. У роботі [1] здійснено аналіз сучасних практик використання цифрових інструментів штучного інтелекту в системі підбору персоналу, а також окреслено перспективи подальшого розвитку наукових засад цифровізації рекрутингових процесів в Україні. Підкреслено необхідність глибшого дослідження ефективності зазначених практик, а також їх адаптації до національного контексту.

У роботі [2] розглядається застосування штучних нейронних мереж у процесі управління персоналом, зокрема в контексті пошуку релевантних кандидатів на вакантні посади. Автор пропонує використовувати нейронні мережі для автоматизованого аналізу резюме, ранжування кандидатів за рівнем кваліфікації, а також створення алгоритмів машинного навчання з метою оптимізації перевірки анкетних даних. У дослідженні використано згорткові нейронні мережі та генетичні алгоритми як метод навчання, розроблено підхід до визначення оптимальної структури хромосом.

У публікації [3] досліджуються теоретико-методологічні основи функціонування інтелектуальних систем добору кадрів у корпоративному секторі. Акцентовано, що такі системи мають не замінювати, а якісно доповнювати діяльність фахівців кадрових служб. Проаналізовано особливості структури управлінських рівнів, диференціацію між поняттями "персонал" і "кадри", а також визначено роль інтелектуальної системи добору в забезпеченні ефективного HR-менеджменту.

У роботі [4] розкрито концепцію системи управління персоналом, представлено порівняльний аналіз моделей її побудови, а також проаналізовано особливості їх застосування в організаціях різного типу. Висвітлено вплив цифровізації на трансформацію HR-процесів, зокрема висунуто вимоги до професійних компетентностей персоналу в умовах автоматизації. Узагальнено тенденції у сфері підбору персоналу, зокрема впровадження інноваційних технологій, спрямованих на підвищення ефективності функціонування кадрових служб.

У дослідженні [5] проаналізовано можливості впровадження систем ШІ в управлінській діяльності в контексті підвищення продуктивності та ефективності управлінських рішень. Визначено, що ШІ відкриває нові горизонти у сфері HR, зокрема у процесах рекрутингу, онбордингу, управління талантами, стратегічного планування кар'єри та змін. Особлива увага приділена ролі ШІ в аналітичному супроводі прийняття рішень, що мінімізує вплив суб'єктивних чинників.

У статті [6] обґрунтовано доцільність впровадження цифрових інструментів управління персоналом для забезпечення стійкості організацій у кризових умовах, зокрема в період воєнних дій. Розглянуто потребу адаптації персоналу до роботи в умовах війни, впровадження

мотиваційних заходів з утримання ключових кадрів, а також запобігання їхньому відтоку. Виокремлено ключові компетентності персоналу, що забезпечують ефективність функціонування організації в умовах кризи, а також окреслено проблеми управління персоналом у дистанційному форматі із застосуванням соціально-психологічних підходів.

Таким чином, узагальнення теоретичного та прикладного доробку свідчить про доцільність і перспективність використання технологій ШІ та МН у процесах рекрутингу для потреб Збройних Сил України. Це дозволяє значно підвищити ефективність системи кадрового забезпечення, забезпечити оперативність добору кадрів, зменшити вплив людського фактора та адаптуватися до нових викликів безпекового середовища.

Постановка проблеми

Сучасна безпекова ситуація, зокрема в умовах збройної агресії проти України, вимагає оперативної адаптації системи військового управління до динамічних і багатовимірних викликів. У цьому контексті особливої уваги набуває питання удосконалення системи комплектування Збройних Сил України, оскільки ефективність бойових і управлінських структур значною мірою залежить від якісного відбору особового складу.

Попри наявність інформаційно-аналітичних систем обліку та підтримки прийняття рішень, процес рекрутингу в секторі безпеки та оборони здебільшого залишається трудомістким, недостатньо автоматизованим і суттєво залежним від суб’єктивного фактору. У зв’язку з цим зростає потреба у впровадженні сучасних цифрових технологій, зокрема ШІ та МН, з метою підвищення точності, оперативності та об’єктивності процедур відбору кандидатів на військову службу.

Наукова проблема полягає в тому, що, незважаючи на наявність позитивного міжнародного досвіду використання технологій машинного навчання в сфері управління людськими ресурсами, в Україні наразі відсутні систематизовані підходи до їх впровадження саме в контексті військового рекрутингу. Актуальним є дослідження методологічних основ застосування інструментів МН у межах військової організації, а також оцінка їх ефективності в умовах гібридної війни та високої динаміки бойових дій.

Метою статті є обґрунтування доцільності впровадження машинного навчання, зокрема алгоритму Random Forest, у процесі пошуку та відбору кандидатів на військову службу, а також розробка відповідної моделі для автоматизації рекрутингових процедур. Дослідження спрямоване на виявлення можливостей підвищення ефективності системи комплектування Збройних Сил України шляхом використання інтелектуального аналізу даних, що дозволить забезпечити об’єктивність, швидкість і обґрунтованість прийняття рішень щодо укомплектування підрозділів бойовими кадрами.

Результати

Обґрунтування вибору моделі машинного навчання

У контексті удосконалення процесу рекрутингу в Збройних Силах України доцільним є застосування алгоритмів машинного навчання, зокрема методу опорних векторів (Support Vector Machine, SVM) [7]. Обрання цієї моделі може бути обґрунтоване з кількох ключових позицій.

По-перше, SVM демонструє високу ефективність класифікації навіть у випадках роботи зі складними та неоднорідними даними. У сфері військового рекрутингу, де аналізу підлягають великі масиви інформації про кандидатів із різним рівнем підготовки, досвіду, освіти, особистісних якостей і фізичних характеристик, здатність моделі точно диференціювати релевантних кандидатів є критично важливою.

По-друге, алгоритм забезпечує ефективну роботу з великими обсягами вхідних даних.

У військовій сфері обробка значних масивів інформації — звична практика, і здатність SVM ефективно функціонувати в таких умовах є однією з його суттєвих переваг.

По-третє, модель характеризується гнучкістю в обробці як лінійно, так і нелінійно розподілених даних. Це дозволяє здійснювати аналіз різноманітних типів ознак кандидатів без попереднього перетворення структури даних, що забезпечує ширші можливості моделювання реальних сценаріїв прийняття рішень.

По-четверте, SVM здатна ефективно працювати навіть з обмеженими за обсягом вибірками, що є важливою перевагою під час аналізу спеціалізованих категорій кандидатів, для яких може бракувати достатньої кількості емпіричних даних.

Таким чином, алгоритм SVM має низку характеристик, які роблять його перспективним інструментом для застосування у військовому рекрутингу: він дозволяє ефективно класифікувати дані високої складності, працює з невеликими вибірками, а також підтримує як лінійні, так і нелінійні зв’язки між змінними.

Разом із тим, результати моделювання, проведеного в межах даного дослідження, свідчать про відносно нижчу точність моделі SVM (93,2 %) порівняно з алгоритмом Random Forest (97,3 %), що зумовлює доцільність подальшого використання останнього як більш ефективного інструменту автоматизованого добору кандидатів на військову службу.

```
=== Random Forest Metrics ===
Accuracy: 0.972972972972973
Confusion Matrix:
 [[ 3  0  0  0  0  0  0]
 [ 0  2  0  0  0  0  0]
 [ 0  0  5  0  0  0  0]
 [ 0  0  0  1  0  0  0]
 [ 0  0  0  0  7  0  0]
 [ 0  0  0  0  2 50  0]
 [ 0  0  0  0  0  0  4]]
Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00         3
           1       1.00      1.00      1.00         2
           2       1.00      1.00      1.00         5
           3       1.00      1.00      1.00         1
           4       0.78      1.00      0.88         7
           5       1.00      0.96      0.98        52
           6       1.00      1.00      1.00         4

    accuracy                           0.97        74
   macro avg       0.97      0.99      0.98        74
weighted avg       0.98      0.97      0.97        74
```

Рисунок 1. Класифкаційний звіт моделі Random Forest.

Крім того, аналіз за допомогою матриці плутанини та класифікаційного звіту показав, що Random Forest краще справляється з класифікацією рідкісних класів, що є критично важливим у контексті рекрутингу, де певні категорії кандидатів мають менше представників. Наприклад, для класів 4 та 6 Recall у Random Forest досягав 100%, тоді як у SVM лише 57% і 75% відповідно.

```
=== SVM Metrics ===
Accuracy: 0.9324324324324325
Confusion Matrix:
 [[ 3  0  0  0  0  0  0]
 [ 0  2  0  0  0  0  0]
 [ 0  0  5  0  0  0  0]
 [ 0  0  1  0  0  0  0]
 [ 0  0  0  0  4  3  0]
 [ 0  0  0  0  0 52  0]
 [ 0  0  0  0  0  1  3]]
Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00         3
           1       1.00      1.00      1.00         2
           2       0.83      1.00      0.91         5
           3       0.00      0.00      0.00         1
           4       1.00      0.57      0.73         7
           5       0.93      1.00      0.96        52
           6       1.00      0.75      0.86         4

    accuracy                           0.93        74
   macro avg       0.82      0.76      0.78        74
weighted avg       0.93      0.93      0.92        74
```

Рисунок 2. Класифкаційний звіт моделі SVM.

Таблиця 1 – Порівняльна характеристика моделей Random Forest та SVM

Метрика	Random Forest	SVM
Accuracy	0.97	0.93
Macro avg F1-score	0.98	0.78
Weighted avg F1-score	0.97	0.92
Recall (class 5)	0.96	0.90
Recall (class 4)	1.00	0.57
Recall (class 6)	1.00	0.75

За результатами проведеного порівняльного аналізу моделей машинного навчання встановлено, що алгоритм *Random Forest* демонструє перевагу над *Support Vector Machine* (SVM) за всіма ключовими метриками класифікації. Зокрема, модель *Random Forest* досягла вищого показника загальної точності (97,3 % проти 93,2 %), а також забезпечила кращі результати за показниками повноти (*recall*), точності (*precision*) та F1-міри для більшості класів.

З урахуванням високої точності, стійкості до дисбалансу класів та узгодженості результатів, *Random Forest* обґрунтовано обрано як базову модель для розв'язання задачі класифікації кандидатів на військову службу.

Підготовка даних для навчання моделі передбачає проходження кількох ключових етапів:

1. **Збір даних**: Формується вибірка з релевантною інформацією про потенційних кандидатів. До набору даних можуть входити відомості про рівень освіти, військовий або професійний досвід, фізичні характеристики, психометричні тести, спеціальні

навички тощо.

2. **Очищення даних**: Зібрані дані проходять попередню обробку — усунення дублікатів, заповнення або вилучення пропущених значень, виявлення та усунення помилкових записів.
3. **Кодування категоріальних змінних**: Усі нечислові (категоріальні) ознаки, такі як рівень освіти, тип військової спеціальності тощо, трансформуються в числовий формат. Для цього можуть застосовуватись техніки, зокрема *One-Hot Encoding* або *Label Encoding*.
4. **Масштабування ознак**: Хоча *Random Forest* менш чутливий до масштабування вхідних змінних, нормалізація даних може сприяти уникненню потенційного перекосу при порівнянні ознак з різними діапазонами значень.
5. **Розподіл на вибірки**: Вибірка ділиться на навчальний та тестовий набори. Перший використовується для тренування моделі, другий — для перевірки її узагальнюючої здатності.
6. **Відбір ознак**: Ідентифікація найбільш інформативних ознак, що мають значний вплив на результат моделювання. До таких можуть належати рівень освіти, наявність військової підготовки, попередній бойовий досвід, результати фізичних випробувань тощо.
7. **Підготовка до моделювання**: Дані структуруються у формат, придатний для аналізу алгоритмом *Random Forest* — зазвичай у вигляді матриці ознак з відповідними класами цільової змінної.

Для об’єктивного оцінювання ефективності моделі необхідно застосовувати комплекс показників класифікації, зокрема:

- **Точність (Accuracy)** — частка правильно класифікованих випадків серед загальної кількості;
- **Чутливість (Recall/Sensitivity)** — здатність моделі правильно ідентифікувати позитивні випадки;
- **Специфічність (Specificity)** — здатність правильно визначати негативні випадки;
- **Позитивна/негативна передбачуваність (PPV/NPV)** — вірогідність того, що класифіковані випадки дійсно належать до свого класу.

Крім того, доцільно використовувати **матрицю плутанини (Confusion Matrix)** для кількісної оцінки кількості правильних і неправильних класифікацій за кожним класом, що дозволяє виявити слабкі сторони моделі в контексті конкретних категорій.

Для візуалізації взаємозв’язку між чутливістю та специфічністю рекомендується побудова **ROC-кривої (Receiver Operating Characteristic Curve)** з розрахунком **AUC (Area Under the Curve)** — інтегрального показника якості класифікації.

Крос-валідація є важливим етапом для оцінювання стабільності та надійності моделі. Метод полягає у багаторазовому поділі навчальної вибірки на підмножини з подальшим навчанням на одній частині та тестуванням на іншій, що дозволяє зменшити ймовірність переобучення та підвищити узагальнюючу здатність моделі.

Додатково може бути сформовано **контрольний набір**, що не використовувався на жодному з етапів навчання або валідації, і призначений для перевірки ефективності моделі на нових, невідомих даних. Це дозволяє оцінити її реальну практичну придатність.

Фінальним етапом валідації моделі є її тестування на реальних кейсах військового рекрутингу, що дозволяє перевірити відповідність результатів алгоритму вимогам та критеріям відбору, прийнятим у Збройних Силах України.

Для технічної реалізації запропонованого підходу обрано мову програмування **Python** — універсальний інструмент із широким спектром можливостей, що ідеально підходить для задач машинного навчання [8]. Її переваги:

- простий та зрозумілий синтаксис, який забезпечує легкість освоєння та читання коду;

- розвинена екосистема бібліотек (*Scikit-learn*, *Pandas*, *NumPy*, *Matplotlib*, *Seaborn* тощо), що дозволяє ефективно реалізовувати завдання аналізу даних, моделювання та візуалізації;
- гнучкість інтеграції з іншими мовами програмування та платформами;
- придатність для швидкої розробки прототипів та експериментування з різними підходами.

Попри численні переваги, мова програмування **Python** має низку обмежень, що можуть впливати на ефективність її застосування в реальних завданнях [8].

По-перше, **швидкодія Python поступається** скомпільованим мовам, таким як *C++* або *Java*. Це зумовлено тим, що Python є інтерпретованою мовою, тобто кожен рядок коду виконується поетапно за участі інтерпретатора, що уповільнює загальний час виконання програм.

По-друге, **високе споживання оперативної пам'яті** та особливості механізму збирання сміття можуть ускладнювати використання Python у задачах, що потребують інтенсивної обробки даних. Динамічна типізація змінних і відсутність компіляції під час написання коду часто призводять до збільшення обсягів використаної пам'яті порівняно зі скомпільованими мовами.

По-третє, **гнучкість у зміні типів даних змінних під час виконання програми**, без необхідності їх попереднього оголошення, хоч і спрощує розробку та підвищує зручність використання, проте створює ризики виникнення логічних помилок і непередбачуваної поведінки коду в процесі виконання.

Водночас, **Python є провідною мовою програмування у сфері штучного інтелекту та машинного навчання**, що пояснюється розвиненою екосистемою бібліотек і фреймворків. Такі інструменти, як *NumPy*, *Pandas*, *Scikit-learn*, *TensorFlow* та *PyTorch* забезпечують потужні можливості для аналізу великих обсягів даних, реалізації алгоритмів глибокого навчання та побудови складних моделей.

Крім того, Python вирізняється **високою масштабованістю**, що є критично важливою для реалізації обчислювально складних проєктів. Завдяки підтримці паралельних обчислень і багатоядерної обробки, зокрема за допомогою таких бібліотек, як *Dask*, *Joblib* або *Ray*, Python дає змогу ефективно розподіляти обчислювальні навантаження між ядрами процесора чи окремими вузлами в розподілених системах.

Особливу роль відіграє **візуалізація даних**, що є невід'ємною частиною процесу аналізу та інтерпретації результатів машинного навчання. Для цього використовуються потужні бібліотеки Python — *Matplotlib*, *Seaborn*, *Plotly*, *Altair*, *ggplot* — які забезпечують створення інформативних, інтерактивних графіків, діаграм та теплових карт.

У межах проведеного дослідження було розроблено модель машинного навчання, яка автоматизує процес пошуку та відбору найбільш придатного кандидата для військової служби. Алгоритм реалізовано на мові програмування Python із використанням вищезазначених бібліотек. Схематичне представлення процесу навчання моделі наведено на рисунку 3.

Для побудови моделі машинного навчання вхідні дані були позначені як X (множина вхідних ознак) та Y (цільові мітки). Етап виділення ознак відповідає за попередню обробку вхідних даних та їх перетворення у формат, придатний для подальшого аналізу алгоритмами машинного навчання. Формально, цей процес може бути описаний функцією $h(x)$, яка трансформує ознаки з метою підвищення ефективності навчання.

Модель машинного навчання приймає перетворені ознаки та здійснює прогнозування результатів $\hat{y}$ на основі вхідних даних. У процесі навчання використовується **метрика якості**, яка відіграє ключову роль в оцінюванні точності моделі. Цей компонент порівнює прогнозовані значення $\hat{y}$ з фактичними y, формує зворотний зв'язок і передає його до алгоритму навчання з метою оптимізації ваг моделі $\hat{w}$.

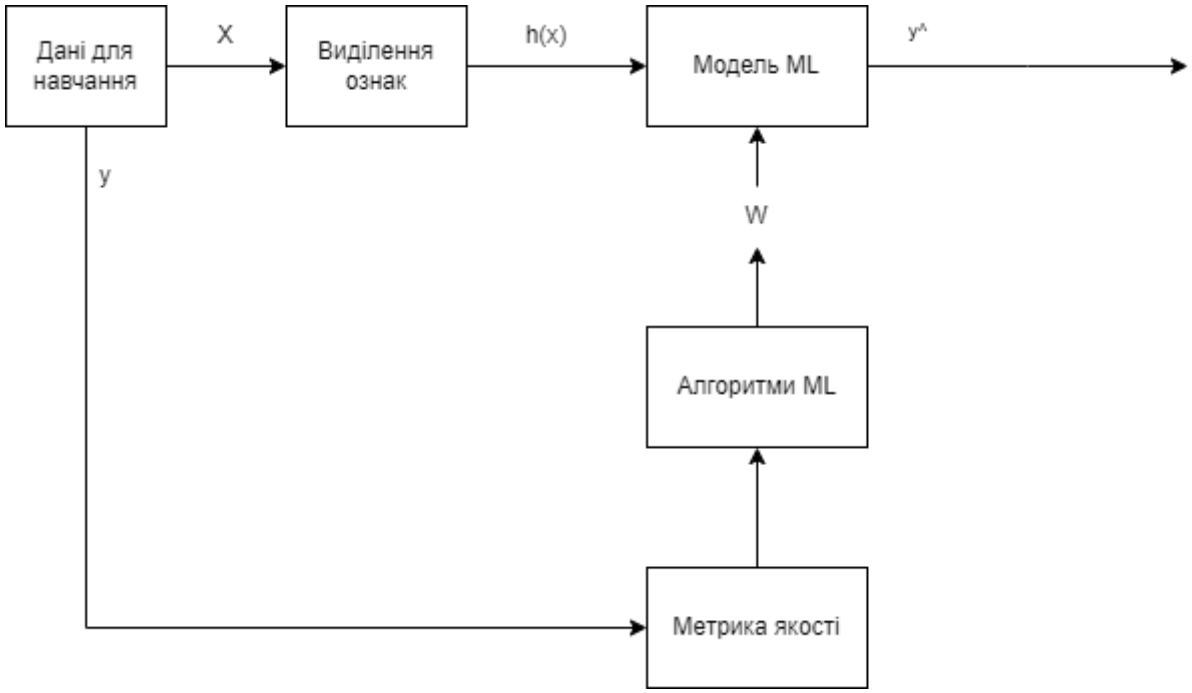


Рисунок 3 – Схема процесу машинного навчання

Типова практика передбачає поділ вибірки на навчальну та тестову у співвідношенні 80:20, де 80% даних використовується для навчання, а 20% — для оцінки ефективності моделі.

Переваги контрольованого навчання полягають у його здатності точно моделювати закономірності та приймати рішення на основі структурованих даних. Такий підхід дає змогу будувати складні моделі, які забезпечують високу точність прогнозів. Наявність навчальних даних із мітками є критично важливою для ефективного засвоєння взаємозв'язків між вхідними ознаками та очікуваними результатами.

Водночас контрольоване навчання має низку обмежень. Зокрема, зміщення (bias) у навчальних даних може спричинити несправедливі або хибні прогнози. Крім того, модель суттєво залежить від якісних позначених даних, отримання яких є трудомістким та ресурсозатратним процесом [9].

Для прикладного впровадження результатів дослідження було розроблено веб-застосунок "Candidate Management System", що автоматизує процес пошуку та відбору кандидатів на основі аналізу їхніх персональних характеристик. Рисунок 4 ілюструє стартову сторінку веб-інтерфейсу зазначеного застосунку.

Розроблений веб-додаток виконує дві основні функціональні задачі:

1. **Додавання нових кандидатів** — забезпечує можливість рекрутерам вводити персоналізовану інформацію про кандидатів, зокрема вік, рівень освіти, громадянство, професійну орієнтацію тощо. Уся введена інформація автоматично зберігається у базі даних для подальшого аналізу та використання в системі прийняття рішень.
2. **Пошук оптимального кандидата** — базуючись на результатах роботи навченої моделі машинного навчання, система виконує аналітичне порівняння параметрів кандидатів із вимогами до конкретної посади. На основі вагових коефіцієнтів (таких як відповідність рівня освіти, стан здоров'я, громадянство тощо), користувач отримує рекомендацію щодо найбільш релевантного кандидата.

Інтерфейс веб-додатку реалізує початкову сторінку навігації, що дає змогу користувачеві обрати один із напрямів роботи в системі — додавання нових даних або виконання пошуку.

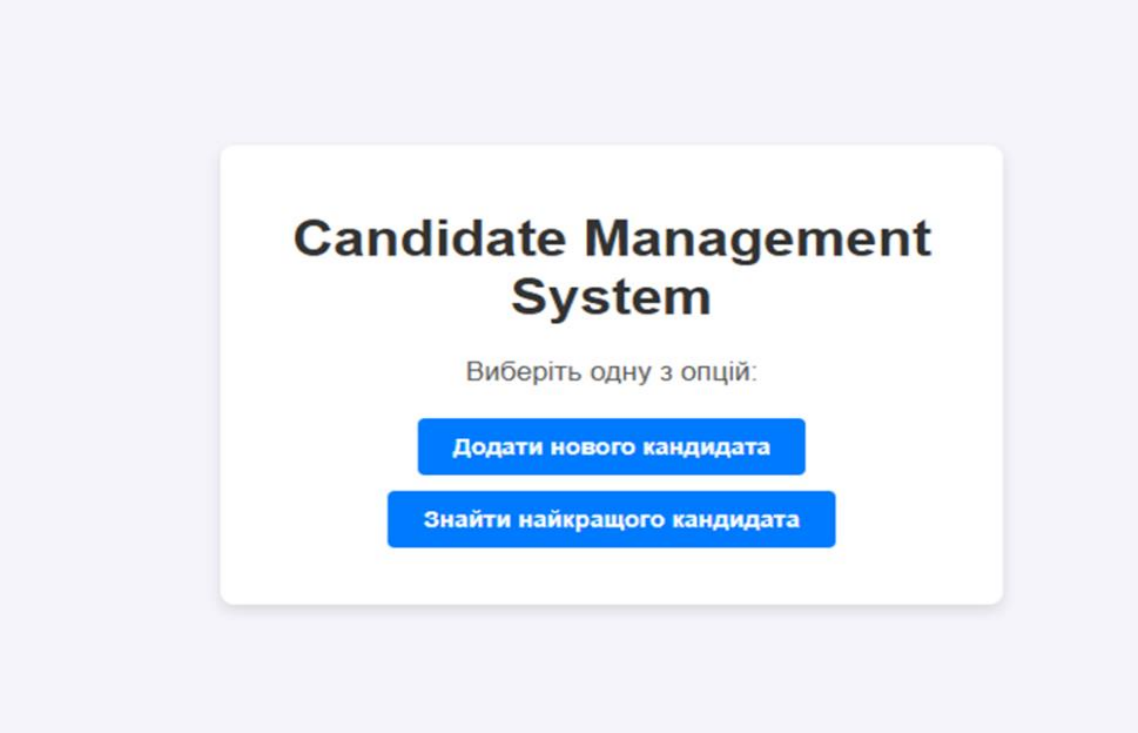


Рисунок 4 – Сторінка для входу в Інтерфейс веб-додатку
“Candidate Management System” для тестування

Система спрямована на підвищення ефективності діяльності рекрутингових центрів та підрозділів з кадрової роботи. Її основною метою є оптимізація та автоматизація процесу прийняття рішень під час комплектування підрозділів Збройних Сил України та інших складових Сил оборони.

Рисунок 5 демонструє форму для введення інформації про нового кандидата у веб-додатку “Candidate Management System”. Дана форма призначена для збору базових персональних характеристик. Її елементи включають:

- **Age (вік)** – числове поле для введення віку кандидата;
- **Service (стаж)** – випадаючий список для зазначення наявності трудового стажу (так/ні);
- **Attraction (судимість)** – випадаючий список для визначення наявності судимості (так/ні);
- **Citizenship (громадянство)** – текстове поле для введення громадянства кандидата;
- **Education (рівень освіти)** – числове поле для вказівки здобутого рівня освіти;
- **Direction of Education (напрям освіти)** – текстове поле для зазначення напряму підготовки (наприклад, “технічний”, “медичний” тощо);
- **Sex (стать)** – випадаючий список для вибору статі (чоловік/жінка);
- **Position (посада)** – текстове поле для введення попередньої займаної посади;
- **Marital Status (сімейний стан)** – випадаючий список для зазначення сімейного статусу (одружений/неодружений);
- **State of Health (стан здоров’я)** – випадаючий список для визначення стану здоров’я (придатний/непридатний).

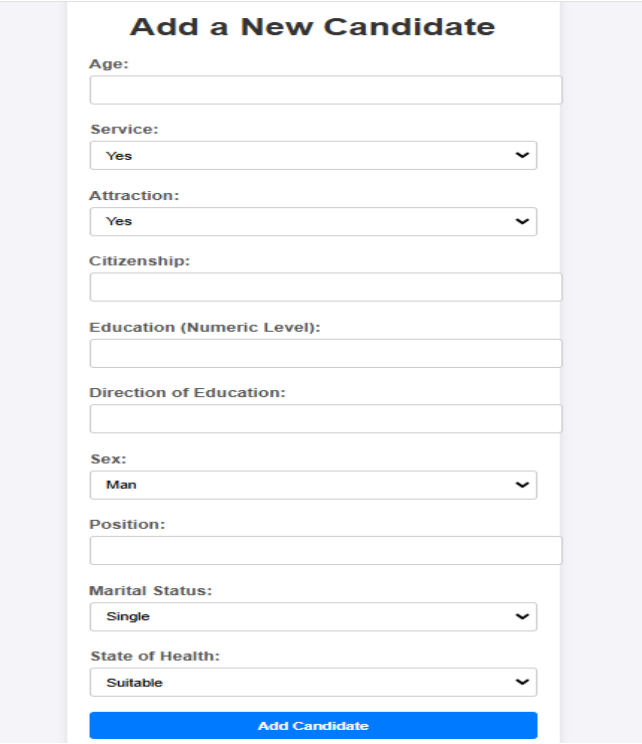


Рисунок 5 – Форма для додавання нового кандидата
у веб-додатку “Candidate Management System”

Кнопка “Add Candidate” після заповнення всіх полів форми і натискання кнопки, інформація зберігається в базі даних або у JSON-файлі для подальшого аналізу.

Ця форма є важливою частиною системи, оскільки дозволяє легко додавати нових кандидатів, структуруючи їхні дані для подальшої роботи алгоритмів відбору.

Сторінка з формою для швидкого пошуку найкращого кандидата показана на рисунку 6.

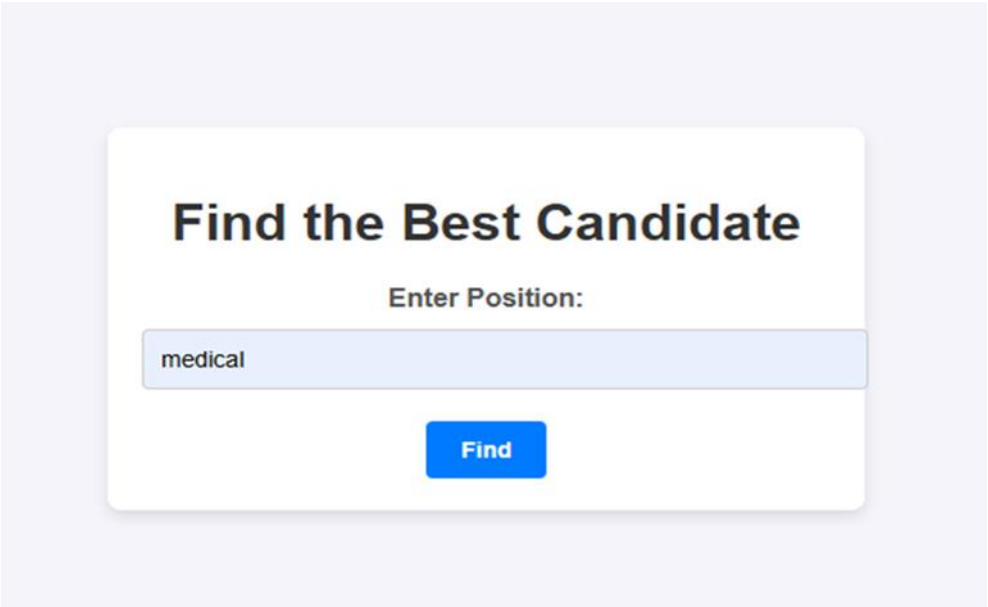


Рисунок 6 – Форма для швидкого пошуку найкращого кандидата

Ця сторінка призначена для рекрутерів, які хочуть швидко знайти найкращого кандидата для заданої посади. Використовуючи алгоритм підбору, система допомагає

прийняти обґрунтоване рішення, автоматизуючи частину процесу відбору.

Такий інтерфейс підходить як для експертів, так і для новачків у рекрутингу.


```
{
  "1": 94,
  "Age": 31,
  "Attraction": "no",
  "AttractionWeight": 1,
  "Citizenship": "Ukrainians",
  "CitizenshipWeight": 1,
  "Directionofeducation": "medical
  "Education": 4,
  "EducationMatch": 1,
  "HealthWeight": 1,
  "Maritalstatus": "married",
  "Position": "doctor",
  "PredictedPosition": "doctor",
  "Probability": 1.0,
  "Service": "no",
  "Sex": "woman",
  "Stateofhealth": "suitable"
}
```


Рисунок 7 – Результат роботи класифікатора у веб-додатку “Candidate Management System”

На рисунку 7 представлено результат функціонування класифікатора у веб-додатку “Candidate Management System” після виконання пошуку найвідповіднішого кандидата відповідно до введеної посади. Виведені системою дані відображають характеристики кандидата, якого класифікатор визначив як найбільш релевантного.

Система “Candidate Management System” використовує **алгоритм Random Forest** для класифікації та прийняття рішень щодо відбору кандидатів.

Опис алгоритму Random Forest

Random Forest — це ансамблевий метод машинного навчання, який базується на побудові множини дерев рішень. Кожне дерево виконує незалежну класифікацію, а кінцевий результат формується шляхом агрегації голосів усіх дерев.

У рамках реалізованої моделі алгоритм було навчено на базі даних кандидатів із урахуванням таких ключових ознак:

- **Громадянство (Citizenship)** — перевага надається громадянам України;
- **Судимість (Attraction)** — пріоритет мають кандидати без судимості;
- **Відповідність освіти (Direction of Education, Education Match)** — враховується, чи відповідає напрям та рівень освіти вимогам до посади;
- **Стан здоров’я (State of Health)** — особи, що визнані придатними за станом здоров’я, отримують додаткову вагу при класифікації;
- **Сімейний стан (Marital Status)** — може враховуватися як додатковий критерій відповідно до кадрової політики;
- **Ймовірність (Probability)** — підсумковий результат роботи алгоритму представлено у вигляді ймовірності відповідності кандидата заданим параметрам посади.

Алгоритм Random Forest аналізує вхідні дані усіх кандидатів, оцінюючи такі параметри, як вік, громадянство, освіта, сімейний стан тощо. На основі цих даних будується ансамбль дерев рішень, кожне з яких здійснює незалежну оцінку кандидатів. Після завершення процесу голосування результати агрегуються, й модель обирає кандидата з найвищим значенням ймовірності відповідності посаді.

У наведеному прикладі (рисунок 7) система ідентифікувала кандидата на посаду **“doctor”** з імовірністю відповідності **1.0 (100%)**.

Алгоритм Random Forest забезпечує **високу точність класифікації (97,3%)** завдяки роботі з великим числом ознак та врахуванню їх вагомості. Метод стійкий до пропущених значень та шумів у даних, що робить його надійним для використання в умовах реального середовища.

Крім того, модель забезпечує можливість інтерпретації результатів: система відображає причини, з яких кандидат був обраний, з урахуванням відповідних вагових коефіцієнтів і розрахованих ймовірностей.

Висновки

У результаті проведеного дослідження обґрунтовано доцільність інтеграції методів машинного навчання, зокрема алгоритмів **Support Vector Machine (SVM)** та **Random Forest**, у процес військового рекрутингу в Збройних Силах України. Аналіз ефективності алгоритму **SVM** засвідчив його високу результативність у класифікації складних та неоднорідних даних, здатність працювати з обмеженими вибірками, а також адаптивність до різнорідних ознак кандидатів.

Водночас алгоритм **Random Forest** продемонстрував високу точність класифікації, стійкість до пропущених значень та інформаційного шуму, а також здатність до інтерпретації прийнятих рішень завдяки використанню вагових коефіцієнтів ознак.

Розроблена система **“Candidate Management System”** забезпечує автоматизацію введення даних про кандидатів, їх обробку та класифікацію відповідно до вимог конкретної військової посади. Реалізація програмного забезпечення мовою Python із застосуванням сучасних бібліотек машинного навчання дозволила створити функціональний прототип цифрового інструменту для підтримки прийняття кадрових рішень у сфері військового управління.

Результати апробації підтвердили ефективність запропонованого підходу: система здатна успішно ідентифікувати найбільш придатного кандидата з урахуванням визначених параметрів та вимог до посади.

Таким чином, отримані результати свідчать про доцільність подальшого розвитку та впровадження технологій машинного навчання в систему рекрутингу Збройних Сил України. У перспективі доцільно зосередити зусилля на:

- розширенні набору ознак для підвищення точності класифікації;
- адаптації моделей до умов реального функціонування військових частин;
- масштабуванні системи для інтеграції в кадрові процеси структурних підрозділів Сил оборони України.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Кравчук, О. І., Варіс, І. О., & Пєркова, М. В. (2023). Сучасні практики використання штучного інтелекту для цифровізації рекрутингу. Проблеми сучасних трансформацій. Серія: економіка та управління, (8). https://doi.org/10.54929/2786-5738-2023-8-04-06.
2. Sineglazov, V. M. (2019). Intelligent System of Personnel Management. Освіта України, (3). URL : https://er.nau.edu.ua/items/980b1893-41c8-496b-8ad3-47f5a2694bb1.

3. Shved, V. (2022). Теоретико-методологічні засади інтелектуальної системи кадрового менеджменту. Причорноморські економічні студії, (74), 151–156. https://doi.org/10.32843/BSES.74-22.
4. Kholod, S., Pavlova, V., Spitsyna, A., Maistrenko, Y., Anufrieva, O., & Lukianykhin, V. (2021). Transformation of the personnel management system in the conditions of digitalization of hr processes. Studies of applied economics, 39(6). https://doi.org/10.25115/eea.v39i6.5015.
5. Черненко, Н. (2022). Штучний інтелект в управлінні персоналом. Таврійський науковий вісник. Серія: Економіка, (12), 76–83. https://doi.org/10.32851/2708-0366/2022.12.11.
6. Замлинський, В., Скрипник, Н., & Федака, В. (2025). Управління персоналом в умовах воєнного стану: інтеграція цифрових технологій. Herald of Khmelnytskyi National University. Economic Sciences, 338(1), 555-563. https://doi.org/10.31891/2307-5740-2025-338-82.
7. Сампір І., Сампір О., &Горбачова Я. (2024). Впровадження технології штучного інтелекту в процес рекрутингу в Збройних Силах України. CollectionofScientificPapers «ΛΌГОΣ», (March 29, 2024; March29, 2024; Cambridge, UnitedKingdom), 132–136. https://doi.org/10.36074/logos-01.03.2024.028.
8. Пилипенко, В. (2024). Дослідження точності методів машинного навчання при прогнозуванні успішності студентів. Herald of Khmelnytskyi National University. Technical Sciences, 335(3(1), 349-356. https://doi.org/10.31891/2307-5732-2024-335-3-47.
9. Karl T. 6 reasons why is python used for machine learning. New Horizons. URL: https://www.newhorizons.com/resources/blog/why-is-python-used-for-machine-learning.

References

1. Kravchuk O. I., Varis, I. O., & Perkova, M. V. (2023). Modern practices of using artificial intelligence for digitalization of recruiting. Problems of modern transformations. Series: economics and management, (8). https://doi.org/10.54929/2786-5738-2023-8-04-06.
2. Sineglazov, V. M. (2019). Intelligent System of Personnel Management. Освіта України, (3). Retrieved from : https://er.nau.edu.ua/items/980b1893-41c8-496b-8ad3-47f5a2694bb1.
3. Shved, V. (2022). Theoretical and methodological principles of the intellectual system of personnel management. Black Sea Economic Studies, (74), 151–156. https://doi.org/10.32843/BSES.74-22.
4. Kholod, S., Pavlova, V., Spitsyna, A., Maistrenko, Y., Anufrieva, O., & Lukianykhin, V. (2021). Transformation of the Personnel Management System in the Conditions of Digitalization of HR Processes. Studies of Applied Economics, 39(6). https://doi.org/10.25115/eea.v39i6.5015.
5. Chernenko, N. (2022). Artificial Intelligence in Personnel Management. Tavria Scientific Bulletin. Series: Economics, (12), 76–83. https://doi.org/10.32851/2708-0366/2022.12.11.
6. Zamlynsky, V., Skrypnyk, N., & Fedaka, V. (2025). Personnel management in martial arts conditions: integration of digital technologies. Herald of Khmelnytskyi National University. Economic Sciences, 338(1), 555-563. https://doi.org/10.31891/2307-5740-2025-338-82.
7. Sampir I., Sampir O., & Gorbacheva Y. (2024). Implementation of artificial intelligence technology in the recruitment process in the Armed Forces of Ukraine. Collection of Scientific Papers «ΛΌГОΣ», (March 29, 2024; March29, 2024; Cambridge, United Kingdom), 132–136. https://doi.org/10.36074/logos-01.03.2024.028.
8. Karl T. 6 reasons why is python used for machine learning. New Horizons. URL: https://www.newhorizons.com/resources/blog/why-is-python-used-for-machine-learning
9. Pylypenko, V. (2024). Research on the accuracy of machine learning methods in predicting student success. Herald of Khmelnytskyi National University. Technical Sciences, 335(3(1), 349-356. https://doi.org/10.31891/2307-5732-2024-335-3-47.

Адаптація логістики пально-мастильних матеріалів в умовах сучасної війни: досвід та перспективи для України

Adaptation of fuel and lubricant logistics in modern warfare: experience and prospects for Ukraine

Андрій Венцюк [A]
Corresponding author: викладач кафедри забезпечення військ (сил), e-mail: andrejvencuk@gmail.com, ORCID: 0000-0003-1460-1619

Олексій Заручинський [A]
старший викладач кафедри забезпечення військ (сил), e-mail: 02121983alx@gmail.com, ORCID: 0009-0002-6047-2555

Надія Бурдейна [A]
кандидат економічних наук, доцент кафедри кадрової, мобілізаційної та організаційно-штатної роботи, e-mail: nadine-burd@rambler.ru, ORCID: 0000-0002-3070-1866

Олександр Федченко [A]
старший викладач кафедри забезпечення військ (сил), e-mail: fedchtenco_alekc_@ukr.net

Andriy Ventsyuk [A]
Corresponding author: lecturer at the Department of Provision of Troops (Forces), e-mail: andrejvencuk@gmail.com, ORCID: 0000-0003-1460-1619

Oleksii Zaruchynskyi [A]
Senior Lecturer of the Department of Provision of Troops (Forces), e-mail: 02121983alx@gmail.com, ORCID: 0009-0002-6047-2555

Nadiya Burdeyna [A]
PhD in Economics, Associate Professor of Department of Personnel, Mobilization and Organizational and Staff Work, e-mail: nadine-burd@rambler.ru, ORCID: 0000-0002-3070-1866

Oleksandr Fedchenco [A]
Senior Lecturer of the Department of Provision of Troops (Forces), e-mail: fedchtenco_alekc_@ukr.net

[A] Військова академія, м. Одеса, Україна

[A] Military Academy, Odessa, Ukraine

Received: April 11, 2025 | Revised: April 21, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.6

Мета роботи: полягає у розробці рекомендацій щодо підвищення ефективності постачання пально-мастильних матеріалів, мінімізації логістичних ризиків і впровадження інноваційних рішень.

Метод дослідження: Аналіз та синтез.

Результати дослідження: встановлено, що ефективна логістика ПММ залежить від децентралізації системи постачання, використання мобільних заправних комплексів, впровадження цифрових систем моніторингу та прогнозування потреб. Запропоновано адаптивну модель логістики для ЗСУ, що забезпечує підвищення стійкості та зменшення часу доставки пального.

Теоретична цінність дослідження: робота розширює існуючі теорії військової логістики шляхом інтеграції інноваційних технологій і пропонує нові підходи до управління запасами ПММ в умовах динамічних бойових дій.

Практична цінність дослідження: запропоновані рішення можуть бути використані військовими логістичними структурами України для оптимізації постачання та підвищення ефективності виконання бойових завдань.

Цінність дослідження: стаття пропонує унікальну адаптивну модель логістики ПММ для умов сучасної війни, що враховує національні та міжнародні особливості, із застосуванням цифрових і автономних рішень.

Обмеження дослідження: дослідження обмежене доступністю актуальних військових нормативів. Подальші роботи можуть бути зосереджені на впровадженні штучного інтелекту для прогнозування потреб у ПММ та дослідженні альтернативних джерел енергії.

Тип статті: теоретико-емпіричний.

Purpose: is to develop recommendations for enhancing supply efficiency, minimizing logistical risks, and implementing innovative solutions.

Method: analysis and synthesis.

Research results: the study revealed that effective POL logistics depends on supply system decentralization, the use of mobile refueling units, and the implementation of digital monitoring and demand forecasting systems. An adaptive logistics model for the Ukrainian military was proposed to enhance resilience and reduce fuel delivery times.

Theoretical implications: the work expands existing military logistics theories by integrating innovative technologies and proposes new approaches to POL inventory management in dynamic combat conditions.

Practical implications: the proposed solutions can be applied by Ukrainian military logistics units to optimize supply chains and improve combat mission effectiveness.

Originality / Value: this article introduces a unique adaptive POL logistics model tailored to modern warfare, considering national and international specifics with the application of digital and autonomous solutions.

Research limitations / Future research: the study is limited by the availability of current military regulations. Future research may focus on implementing artificial intelligence for demand forecasting and exploring alternative energy sources.

Type of article: theoretical-empirical.

Ключові слова: логістика, війна, пально-мастильні матеріали, норми витрат пального, стандарти.

Key words: logistics, war, fuel and lubricants, fuel consumption norms, standards.

Вступ

Сучасна війна характеризується високою динамікою бойових дій, широким застосуванням мобільних формувань та необхідністю безперебійного функціонування військової

інфраструктури. У таких умовах логістика пально-мастильних матеріалів (ПММ) постає як один із ключових чинників, що визначає рівень бойової готовності військ. Ефективне управління логістичними процесами постачання ПММ набуває стратегічного значення та вимагає адаптації до змін операційного середовища.

Забезпечення підрозділів Збройних Сил України паливними ресурсами потребує впровадження адаптивних підходів, які враховують досвід ведення сучасних бойових дій, аналіз норм витрат пального, а також необхідність переходу до сучасних стандартів логістичного забезпечення. Особливу увагу слід приділити розробці гнучких і технологічно обґрунтованих механізмів постачання, що базуються на прогнозуванні потреб, раціональному розподілі ресурсів та використанні інноваційних рішень.

Перспективи логістичного забезпечення паливом у воєнний час визначаються спроможністю логістичних систем до швидкої адаптації, мінімізації втрат і скорочення часу доставки ресурсів до місць призначення. Зміна підходів до організації постачання ПММ передбачає активне впровадження сучасних засобів моніторингу, автоматизації процесів та використання альтернативних джерел енергії з метою підвищення автономності бойових підрозділів. Усе це зумовлює актуальність наукового аналізу проблематики логістики ПММ як одного з ключових компонентів підтримання обороноздатності України в умовах новітніх викликів і загроз.

Теоретичні основи дослідження

Проведене дослідження сприяє подальшому розвитку теорії військової логістики, зокрема в аспекті забезпечення ПММ в умовах сучасного збройного конфлікту. У межах роботи було розширено теоретичні засади адаптації логістичних систем за рахунок інтеграції цифрових технологій моніторингу, прогнозування потреб із застосуванням елементів штучного інтелекту, а також упровадження альтернативних джерел енергії для підвищення автономності бойових підрозділів.

Запропоновані підходи не заперечують чинних теоретичних моделей, однак передбачають їхнє суттєве доповнення з урахуванням викликів, характерних для повномасштабної війни на території України. Наголошується на необхідності підвищення гнучкості логістичних систем і переходу від централізованих схем постачання до багатоканальних, мобільних та децентралізованих моделей, що здатні забезпечити стабільність функціонування навіть за умов вогневого впливу противника або порушення тилових комунікацій.

Теоретично обґрунтовано доцільність впровадження адаптивних логістичних структур, здатних швидко реагувати на зміну оперативної обстановки, забезпечуючи стійкість системи матеріально-технічного забезпечення. Зазначені підходи відповідають сучасним тенденціям ведення бойових дій і становлять основу для подальшого розвитку методології планування й управління логістичними процесами в системі національної оборони.

Постановка проблеми

Актуальність дослідження зумовлена необхідністю адаптації систем логістичного забезпечення ПММ до умов сучасної війни, яка характеризується високою динамікою змін бойової обстановки, маневреністю військових дій та зростанням вимог до оперативності, стійкості та надійності постачання. Існуючі логістичні моделі виявляють обмежену ефективність у нових умовах і потребують модернізації з метою мінімізації ризиків втрат ресурсів, оптимізації норм витрати пального, а також впровадження сучасних технологічних підходів і стандартів забезпечення військових частин паливом в умовах ведення бойових дій.

Методологія дослідження

У процесі дослідження було застосовано комплекс взаємопов'язаних загальнонаукових і спеціальних методів, що забезпечили всебічне вивчення проблематики логістики паливно-мастильних матеріалів (ПММ) в умовах сучасної війни:

Індукція — використана для узагальнення результатів анкетувань, емпіричних спостережень та аналітичних досліджень, що дозволило сформувати цілісне уявлення про поточний стан системи забезпечення ПММ у Збройних Силах України (ЗСУ).

Дедукція — застосована для інтерпретації теоретичних положень щодо управління матеріальними ресурсами в умовах бойових дій, а також перевірки їх відповідності емпіричним даним, отриманим у ході дослідження.

Порівняльний метод — реалізований шляхом зіставлення вітчизняних стандартів забезпечення ПММ із підходами, що використовуються в збройних силах США, НАТО та Ізраїлю, з метою ідентифікації ефективних практик та оцінки можливостей їх адаптації до українського контексту.

Аналіз причинно-наслідкових зв'язків — застосований для дослідження впливу централізованих та децентралізованих логістичних моделей на оперативність та надійність забезпечення військ ПММ, а також для визначення наслідків обмеженої мобільності паливних резервів для загальної боєздатності підрозділів.

Систематизація — забезпечила упорядкування та узагальнення емпіричних даних щодо норм споживання ПММ, ефективності використання мобільних заправних комплексів, застосування цифрових систем моніторингу запасів та інструментів прогнозування потреб.

Результати

Логістичне забезпечення військових частин у контексті повномасштабної збройної агресії Російської Федерації проти України є визначальним чинником підтримання їх боєздатності та оперативної спроможності. У таких умовах забезпечення ПММ вимагає не лише дотримання чинних норм витрати пального, а й розробки адаптивних логістичних рішень, спроможних ефективно функціонувати в умовах постійної загрози, динамічних змін бойової обстановки та порушеної інфраструктури.

Адаптація логістичних процесів має враховувати особливості інтенсивності бойових дій, характер операцій та специфіку місцевості. У воєнний період особливої ваги набуває безперервне поповнення запасів ПММ, що забезпечує сталість виконання бойових завдань і знижує ризики втрати мобільності підрозділів.

Як зазначає М. М. Сендецький та інші дослідники, сучасні підходи до логістичного забезпечення в умовах збройного конфлікту передбачають застосування гнучких логістичних моделей, які поєднують централізоване управління ресурсами з елементами децентралізації. У Збройних Силах України впроваджуються саме такі моделі постачання, що дозволяють швидко адаптуватися до змін потреб військових частин (Сендецький та ін., 2024).

Інноваційні рішення включають використання мобільних заправних комплексів, автоматизованих систем моніторингу залишків ПММ та цифрових платформ для управління логістичними ланцюгами. Застосування таких рішень сприяє скороченню часу доставки пального, оптимізації маршрутів і підвищенню загальної ефективності використання ресурсів.

Прогнозування потреб у ПММ в умовах активних бойових дій вимагає інтеграції комплексних аналітичних підходів, які поєднують бойовий досвід, оперативні дані щодо характеру операцій, типів задіяної техніки та метеоумов. Сучасні методики базуються на використанні математичних моделей, систем підтримки прийняття рішень і технологій штучного інтелекту для визначення оптимальних обсягів та термінів постачання. Такий підхід забезпечує формування як поточних, так і стратегічних запасів, необхідних для ведення

затяжних бойових дій.

Таким чином, ефективне забезпечення військових частин ПММ у сучасній війні ґрунтується на поєднанні теоретичних положень логістики, сучасних моделей постачання та новітніх технологій прогнозування, що дозволяє своєчасно реагувати на виклики війни та гарантувати безперервність логістичних процесів (Іванський та ін., 2020).

Адаптація логістики ПММ у поточних умовах потребує не лише ґрунтовного теоретичного обґрунтування, а й ретельного аналізу практичного досвіду як національного, так і міжнародного рівнів. Дослідження досвіду постачання військ у ході різних збройних конфліктів дозволяє ідентифікувати ефективні логістичні моделі, оцінити специфіку забезпечення в екстремальних умовах і визначити потенційні напрями вдосконалення системи забезпечення Збройних Сил України.

Міжнародний досвід логістичного забезпечення, зокрема під час воєнних конфліктів, підкреслює важливість гнучкості логістичних систем, впровадження сучасних стандартів і застосування передових технологій. Збройні Сили США та країн НАТО активно застосовують багаторівневі моделі логістики, які поєднують централізоване управління з децентралізованими механізмами доставки безпосередньо до бойових підрозділів. Це дозволяє своєчасно реагувати на зміни обстановки, забезпечуючи дотримання нормативів витрат і підтримання безперервності операцій.

Особливої уваги заслуговує досвід НАТО щодо застосування автоматизованих систем моніторингу запасів, які забезпечують контроль споживання ПММ у режимі реального часу та підвищують точність прогнозування потреб. Водночас, Ізраїль, зважаючи на специфіку загроз національній безпеці, активно розвиває мобільні заправні комплекси й безпілотні системи доставки пального в складні для доступу райони. Такі рішення суттєво знижують логістичні втрати та забезпечують оперативне реагування на запити з передових позицій (Bartl, Bader).

Повномасштабна збройна агресія російської федерації проти України, що розпочалася у 2022 році, стала безпрецедентним викликом для національної системи логістичного забезпечення, зокрема у сфері постачання паливно-мастильних матеріалів (ПММ). На початкових етапах активної фази бойових дій було виявлено низку системних проблем: нестача мобільних засобів доставки, порушення логістичних ланцюгів унаслідок руйнування інфраструктури, а також відсутність належної адаптації нормативів витрати пального до умов високої інтенсивності операцій.

Водночас, наявний досвід забезпечення, напрацьований у ході проведення Антитерористичної операції (АТО) та операції Об’єднаних сил (ООС), а також активна кооперація з країнами-членами НАТО, сприяли трансформації системи логістики ПММ. Зокрема, було впроваджено сучасні стандарти постачання, розвинуто національні мобільні логістичні спроможності та покращено механізми реагування на динамічну обстановку на фронті.

Одним із ключових елементів адаптації стало створення розосереджених складів з резервними запасами ПММ, що дозволило знизити ризики їх знищення внаслідок авіаційних ударів або ракетних обстрілів. Також були запроваджені гнучкі схеми постачання, які передбачають оперативну зміну маршрутів залежно від поточних загроз і тактичної ситуації. Практика воєнного часу підтвердила ефективність використання мобільних заправних комплексів, які забезпечують підвищену автономність підрозділів та зменшують їхню залежність від стаціонарних об’єктів тилового забезпечення (Добровольський, Романченко, 2022).

Серед результативних логістичних рішень слід виокремити впровадження автоматизованих систем обліку та контролю споживання пального, що забезпечили зменшення випадків нераціонального використання ресурсів та сприяли дотриманню встановлених нормативів. Водночас, розгортання мобільних паливних станцій на базі колісних платформ дало змогу здійснювати оперативне заправлення передових підрозділів навіть у випадках блокування основних транспортних артерій. Практика бойових дій засвідчила

необхідність врахування кліматичних і рельєфних особливостей районів проведення операцій, що істотно впливає на ефективність логістичного забезпечення.

Однак досвід також виявив низку неефективних рішень. Зокрема, надмірна централізація управління логістичними процесами на початкових етапах вторгнення призвела до затримок у постачанні ПММ окремим військовим частинам. Додаткові ускладнення виникли через недостатню гнучкість логістичних структур у реагуванні на зміну бойової обстановки. Мали місце випадки втрат ПММ внаслідок недостатнього захисту складів і відсутності ефективної системи оповіщення про загрози. Указані фактори підкреслюють нагальну потребу в подальшому вдосконаленні логістичних механізмів, орієнтованих на підвищення стійкості та ефективності забезпечення в умовах війни.

Загальний аналіз вітчизняного та міжнародного досвіду свідчить про критичну важливість поєднання гнучких організаційних підходів, технологічної модернізації та стратегічного планування в системі логістики ПММ. Комплексна адаптація цих компонентів виступає запорукою підтримання боєздатності військових частин, стійкості логістичних систем і стабільності виконання бойових завдань у складних умовах збройного конфлікту (Ляшенко, Задерейко, 2024).

Важливою складовою ефективного забезпечення є нормативно обґрунтоване планування витрат ПММ. Норми витрати визначають обсяги необхідного ресурсу для виконання конкретних бойових завдань в умовах різного характеру операцій. Особливої актуальності набуває порівняльний аналіз чинних нормативів Збройних Сил України з аналогічними положеннями, прийнятими у збройних силах країн-членів НАТО. У державах Альянсу, зокрема в США, стандарти витрати пального формуються на основі систематичних досліджень експлуатаційних характеристик техніки, характеру місій, географічних та кліматичних умов. При цьому значну увагу приділено адаптивності таких нормативів до змін бойового середовища.

До 2022 року в Україні діяли традиційні норми, закріплені, зокрема, в наказі Міністерства транспорту України від 10 лютого 1998 року № 43 “Про затвердження норм витрат палива і мастильних матеріалів на автомобільному транспорті”, а також у наказі Міністерства транспорту та зв’язку України від 3 березня 2008 року № 244 “Про затвердження норм витрат паливно-мастильних матеріалів для спеціального рухомого складу”. Проте в умовах повномасштабної війни ці нормативи виявилися недостатньо гнучкими для забезпечення потреб маневрових бойових дій.

У відповідь на ці виклики Збройні Сили України почали впроваджувати практику оперативного коригування обсягів споживання ПММ, орієнтовану на поточну оперативну обстановку, характер виконуваних завдань і реальні потреби військових частин (Сівак та ін., 2021). У сучасних умовах нормативи витрат пального визначаються окремими документами Міністерства оборони України, більшість з яких мають обмежений доступ або використовуються виключно у службовому порядку з міркувань безпеки.

Таким чином, забезпечення Збройних Сил України паливно-мастильними матеріалами в умовах повномасштабної війни є динамічним процесом, що вимагає постійної адаптації нормативно-правової бази, впровадження інноваційних технологічних рішень і врахування як національного, так і міжнародного досвіду у сфері військової логістики.

Бойові умови та типи залученої військової техніки мають безпосередній вплив на обсяги споживання ПММ. У контексті збройної агресії російської федерації проти України з 2022 року спостерігається суттєве зростання витрат пального під час проведення маневрених операцій, оборонних боїв із частими змінами позицій, а також при забезпеченні глибоких рейдових дій. Особливо інтенсивне споживання ПММ фіксується під час використання важкої бронетехніки, артилерійських систем і засобів авіаційної підтримки, які потребують значних запасів пального для збереження боєготовності.

Забезпечення в умовах урбанізованого театру бойових дій, характерного для окремих операцій Збройних Сил України, передбачає врахування специфічних факторів. Зокрема, це інтенсивне використання двигунів у режимі холостого ходу, часті перегрупування та проведення евакуаційних заходів. Додатковими чинниками, що впливають на витрати ПММ, є погодні умови, рельєф місцевості та стан транспортної інфраструктури. Згідно з практичним досвідом, складні погодні умови, зокрема сильні морози або інтенсивні опади, можуть призводити до підвищення споживання пального на 10–20 %, що обов'язково має враховуватись при логістичному плануванні (Сендецький та ін., 2024).

Удосконалення системи логістичного забезпечення ПММ у Збройних Силах України здійснюється з орієнтацією на впровадження міжнародних стандартів, зокрема розроблених у рамках НАТО та провідних міждержавних оборонних альянсів. Ці стандарти передбачають застосування адаптивних норм витрат пального, запровадження автоматизованих систем моніторингу споживання, а також оптимізацію логістичних ланцюгів із метою скорочення часу доставки ресурсів до військових частин.

Процес адаптації міжнародних стандартів здійснюється з урахуванням специфіки бойових дій на різних театрах воєнних дій, географічних особливостей і технічного стану національної інфраструктури. Наприклад, використання підходів НАТО до прогнозування потреб у ПММ сприяло впровадженню сучасних інформаційно-аналітичних систем управління логістикою, які забезпечують моніторинг у режимі реального часу. Це, у свою чергу, підвищує ефективність управління запасами та дозволяє оперативно коригувати логістичні плани відповідно до динаміки бойових дій.

Разом з тим, повна імплементація міжнародних стандартів стикається з низкою викликів. До ключових з них належать: необхідність модернізації парку військової техніки, значна частина якого морально та фізично застаріла й характеризується підвищеним споживанням пального, а також наявність логістичних вузьких місць, зумовлених масштабним знищенням інфраструктури. Водночас отриманий під час війни досвід засвідчив доцільність і перспективність розширення практики застосування мобільних паливних комплексів, розвитку цифрових платформ та поглиблення співпраці з міжнародними партнерами з метою подальшої адаптації логістичних процесів до умов ведення сучасної війни.

Комплексний аналіз норм витрати пального, з урахуванням бойових факторів та особливостей застосування військової техніки, у поєднанні з інтеграцією міжнародних стандартів, виступає ключовим чинником підвищення стійкості логістичних систем Збройних Сил України. Його реалізація дозволяє мінімізувати ризики нестачі ресурсів, забезпечити оперативну гнучкість постачання та сприяти ефективному виконанню бойових завдань (Department of Defense (DoD), Defense Logistics Agency (DLA). *Military Standard: Quality Assurance for Petroleum Products, Lubricants, and Related Products (MIL-STD – 3004C)*).

У країнах НАТО для оцінювання мобільності військової техніки та прогнозування витрат ПММ широко застосовується *NATO Reference Mobility Model* (NRMM). Ця модель дозволяє оперативним штабам прогнозувати тактичну мобільність техніки на полі бою, а також оптимізувати логістичні операції, включно з розрахунком споживання пального. Незважаючи на варіативність норм залежно від типу техніки та умов експлуатації, NRMM забезпечує уніфікований підхід до оцінки логістичних параметрів.

Адаптація NRMM та інших міжнародних стандартів до реалій українського війська є стратегічно важливим кроком для підвищення ефективності логістичного забезпечення. Їх запровадження дає змогу не лише оптимізувати витрати ПММ, але й покращити планування операцій, а також забезпечити відповідність сучасним вимогам ведення бойових дій (MTU Center for Dependable Transportation. *ET–148 Final Report to NATO*).

Поряд із технологічними та організаційними компонентами, фінансово-економічний аспект логістики ПММ є ключовим чинником, що безпосередньо впливає на стійкість системи

забезпечення та ефективність її функціонування у воєнний час. Раціональне управління фінансовими ресурсами, спрямованими на транспортування, зберігання й розподіл пального, набуває особливого значення в умовах обмежених бюджетних можливостей та високих операційних витрат.

Оцінка вартості логістичних операцій у період активних бойових дій потребує комплексного підходу, що включає не лише прямі витрати на закупівлю ПММ, а й супутні витрати, зокрема на транспортування, утримання матеріально-технічної бази, безпеку перевезень та збереження запасів у зонах бойових дій. Урахування високого рівня ризиків, пов'язаних із руйнуванням транспортної інфраструктури, необхідністю обходу небезпечних ділянок та використання спеціалізованих транспортних засобів, зумовлює суттєве зростання логістичних витрат. Їх оптимізація передбачає впровадження сучасних цифрових систем моніторингу, які забезпечують контроль споживання пального в режимі реального часу, прогнозування потреб та мінімізацію перевитрат. Важливою складовою цієї системи є багатоканальна модель постачання, що дозволяє знизити фінансові ризики у разі порушення основних маршрутів забезпечення (Тесніков, Фурсова, 2022).

Ефективне скорочення витрат на транспортування та зберігання пального можливе за рахунок впровадження інноваційних рішень, зокрема використання модульних мобільних резервуарів, які дозволяють оперативно розгортати пункти зберігання поблизу лінії фронту, скорочуючи логістичне плече. Інтеграція альтернативних джерел енергії, таких як біопаливо або мобільні сонячні генераторні установки, дозволяє зменшити залежність від традиційного постачання ПММ, водночас знижуючи операційні витрати. Важливим напрямом удосконалення є підготовка спеціалістів з військової логістики з акцентом на економічні аспекти планування, що забезпечує більш ефективний розподіл ресурсів, підвищує гнучкість логістичних схем та сприяє загальній фінансовій стійкості у довготривалих кампаніях (Воробйов, 2022).

У сучасних умовах ведення війни традиційні методи логістичного забезпечення ПММ виявили низку системних обмежень, що потребують запровадження новітніх технологічних рішень. Динаміка бойових дій, широка географія театрів військових операцій та високий рівень загроз для логістичних маршрутів зумовлюють необхідність трансформації логістичних процесів із акцентом на цифровізацію, прогнозну аналітику та використання альтернативних енергоносіїв.

Серед ключових інноваційних рішень — впровадження цифрових систем управління запасами та моніторингу транспорту, які забезпечують оперативне відстеження наявності ПММ, місцезнаходження техніки та коригування маршрутів залежно від бойової обстановки. Інтегровані інформаційні платформи та супутниковий моніторинг підвищують точність прогнозування потреб у ПММ, мінімізуючи ризики перебоїв у постачанні, що особливо важливо в умовах децентралізованих бойових дій.

Використання штучного інтелекту (ШІ) та аналітики великих даних у процесі логістичного планування відкриває нові можливості для ефективного управління забезпеченням. Алгоритми машинного навчання дозволяють моделювати потреби в ПММ з урахуванням інтенсивності бойових дій, типів техніки, метеорологічних умов і історичних даних, що сприяє зменшенню перевитрат та уникненню надмірного накопичення запасів.

Окрему увагу заслуговують заходи щодо інтеграції альтернативних джерел енергії. Досвід окремих підрозділів Збройних Сил України свідчить про успішне використання мобільних сонячних електростанцій для живлення обладнання та заряджання безпілотних літальних апаратів, що дозволяє скоротити потребу у транспортуванні ПММ на передову. Застосування біопального для тилових операцій також розглядається як перспективний напрям з огляду на зниження енергозалежності та екологічне навантаження (Торічний, Райко, 2023).

Попередній аналіз свідчить, що ефективність системи забезпечення ПММ визначається

її здатністю до оперативного реагування на зміни бойової обстановки. З метою підвищення гнучкості та стійкості логістичної системи доцільно реалізувати такі напрями:

– **Розробка гнучких логістичних моделей.** Адаптивні логістичні схеми мають передбачати різні сценарії бойових дій — від оборонних до наступальних. Важливими компонентами є впровадження мобільних пунктів заправки, автоматизованих вузлів розподілу та гібридних транспортних засобів. Цифрові платформи забезпечуватимуть оперативне коригування маршрутів, а стандартизовані протоколи — ефективне перепрофілювання логістичних мереж.

– **Підвищення кваліфікації фахівців.** Підготовка спеціалістів з військової логістики має орієнтуватися на інтеграцію теоретичних знань і практичних навичок в умовах, максимально наближених до реальних бойових сценаріїв. Особливу увагу слід приділяти навчанню роботі з цифровими системами, алгоритмами прогнозування та управління ризиками. Міжнародне співробітництво дозволить розширити обмін досвідом і забезпечити участь у спільних навчаннях.

– **Формування резервних систем постачання.** З огляду на уразливість критичної інфраструктури доцільним є створення децентралізованих складів із мобільними запасами поза зонами ризику. Перспективним напрямом є застосування дронів та наземних безпілотних транспортних засобів для доставки ПММ у важкодоступні райони. Альтернативні енергетичні комплекси можуть забезпечити автономність тилових баз та мобільних груп (Ляшенко, Задерейко, 2024).

Комплексне удосконалення логістики ПММ у Збройних Силах України має ґрунтуватися на поєднанні гнучких організаційних підходів, впровадженні інноваційних технологій та підвищенні фахової підготовки персоналу. Такий підхід дозволить не лише забезпечити стійкість системи постачання, але й суттєво підвищити ефективність виконання бойових завдань в умовах сучасної війни.

Обговорення

У результаті проведеного дослідження встановлено, що ефективна логістика ПММ у Збройних Силах України в умовах сучасної війни вимагає інтеграції гнучкості, технологічної модернізації та стратегічного планування. Ці висновки узгоджуються з існуючими теоріями військової логістики та результатами попередніх досліджень, які підкреслюють важливість адаптивних логістичних моделей і впровадження інноваційних технологій для забезпечення військ. Порівняння з міжнародним досвідом, зокрема практиками США, НАТО та Ізраїлю, продемонструвало, що використання автоматизованих систем моніторингу запасів, мобільних заправних комплексів і альтернативних джерел енергії суттєво підвищує ефективність постачання та знижує логістичні ризики. Це відповідає теоретичним положенням про необхідність інтеграції цифрових рішень для забезпечення безперервності бойових операцій у динамічних умовах.

Однак дослідження також виявило ряд відмінностей між українськими реаліями та міжнародними стандартами, особливо в частині гнучкості логістичних схем і швидкості реагування на загрози. Незважаючи на активне впровадження Україною передових підходів, зберігаються проблеми, пов’язані з модернізацією техніки, недостатньою децентралізацією постачання на початкових етапах конфлікту та обмеженим використанням штучного інтелекту у прогнозуванні потреб. Ці розбіжності пояснюються як специфікою бойових дій на території України, так і наявними інфраструктурними обмеженнями. Отримані результати наголошують на необхідності подальшої адаптації міжнародного досвіду до національних умов та вдосконалення системи підготовки фахівців із військової логістики для забезпечення стійкості й ефективності постачання ПММ у тривалих конфліктах.

Висновки

У результаті проведеного дослідження встановлено, що ефективність логістики ПММ у Збройних Силах України в умовах сучасної війни залежить від гнучкості логістичних схем, цифровізації процесів та впровадження інноваційних технологій прогнозування потреб. Аналіз міжнародного досвіду і національної практики підкреслив важливість децентралізації постачання, створення резервних систем та використання альтернативних джерел енергії. Попри досягнення, залишаються проблеми, пов'язані із захистом інфраструктури, перевитратами ресурсів і затримками в постачанні, що вимагає удосконалення системи управління та підготовки персоналу.

Подальші дослідження слід зосередити на розробці адаптивних логістичних моделей, впровадженні штучного інтелекту для точного прогнозування потреб у ПММ та оптимізації фінансових витрат. Перспективними напрямами є розширення використання альтернативних джерел енергії, вдосконалення навчальних програм для фахівців, а також оцінка впливу логістичних інновацій на боєздатність військ. Це сприятиме підвищенню стійкості та ефективності логістики Збройних Сил України в умовах воєнних викликів.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Сендецький М. М., Сащук С. І., Махнюк О. В., Комаров В. О. (2024). Дослідження особливостей економії паливно-мастильних матеріалів під час транспортування у силах оборони України. Приладобудування: стан і перспективи. XXIII Міжнародна науково-технічна конференція Київ, Україна: збірник матеріалів конференції. Київ: КПІ ім. Ігоря Сікорського, 305–309.
2. Іванський В. М., Баранов А. М., Баранов Ю. М. (2020). Проблеми логістичного забезпечення Збройних Сил України. Інформаційні технології: наука, техніка, технологія, освіта, здоров'я, 5, 104.
3. Bartl P., Bader J. Standardising lubricants and fuels for NATO applications. URL: https://www.fuelsandlubes.com/fli-article/standardising-lubricants-and-fuels-for-nato-applications/ (дата звернення: 20.02.2025).
4. Добровольський А., Романченко В. (2022). Аналіз чинників, що впливають на показники ефективності логістичного забезпечення щодо постачання та транспортування матеріально-технічних засобів в умовах ведення бойових дій. Збірник наукових праць Національної академії державної прикордонної служби України. Сер.: військові та технічні науки, 4, 340–352.
5. Ляшенко В. і Задерейко О. (2024). Аналіз чинників, що впливають на показники живучості системи управління логістичним забезпеченням військ (сил) в операціях (бойових діях) та визначення шляхів їх нейтралізації. Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки, 20 (2), 55–59. https://doi.org/10.37701/dndivsovt.20.2024.07.
6. Сівак В., Мацько О., Марченко Д. (2021). Аналіз негативних чинників, що впливають на показники живучості системи логістичного забезпечення в умовах ведення бойових дій, та визначення шляхів їх нейтралізації. Збірник наукових праць Національної

академії державної прикордонної служби України. Сер.: військові та технічні науки, 1, 272–287. https://doi.org/10.32453/3.v84i1.815.

7. Про затвердження Норм витрат палива і мастильних матеріалів на автомобільному транспорті: Наказ Міністерства транспорту України від 10.02.1998, № 43. URL: https://zakon.rada.gov.ua/rada/show/v0043361–98#Text (дата звернення: 19.02.2025).
8. Про затвердження норм витрат паливно-мастильних матеріалів для спеціального рухомого складу: Наказ Міністерства транспорту та зв'язку України від 03.03.2008, № 244. URL: https://zakon.rada.gov.ua/rada/show/v0244650–08#Text (дата звернення: 19.02.2025).
9. Department of Defense (DoD), Defense Logistics Agency (DLA). Military Standard: Quality Assurance for Petroleum Products, Lubricants, and Related Products (MIL-STD – 3004C). URL: https://www.dla.mil/Portals/104/Documents/Energy/Quality%20and%20Technical%20Support/E_MilSTD3004_1603.pdf (дата звернення: 17.02.2025).
10. MTU Center for Dependable Transportation. *ET – 148 Final Report to NATO.* Michigan Technological University. 231 p. URL: https://www.mtu.edu/cdt/downloadable-materials/et–148-final-report-to-nato.pdf
11. Тесніков О., Фурсова В. (2022). Фактори впливу на функціонування системи логістичного забезпечення збройних сил України в умовах війни. Економіка та суспільство, 42. https://doi.org/10.32782/2524–0072/2022–42–17.
12. Воробйов О., Власов І., Тягай С., Бамбуляк М. (2022). Обґрунтування шляхів використання сучасних інформаційних технологій для обліку матеріальних засобів по службі пального збройних сил України за досвідом передових країн світу. Сучасні інформаційні технології у сфері безпеки та оборони. Київ, Україна, 43 (1), 53–58. https://doi.org/10.33099/2311–7249/2022–43–1–53–58.
13. Торічний В. О., Райко В. В. (2023). Технічне забезпечення як складова логістичного забезпечення сил безпеки україни: компаративістський аналіз (Україна-НАТО). Наукові інновації та передові технології, 10 (24), 211–220. https://doi.org/10.52058/2786–5274–2023–10(24)–211–220.

References

1. Sendeckyi, M. M., Sashchuk, S. I., Makhniuk, O. V., & Komarov, V. O. (2024). Research on the features of fuel and lubricant savings during transportation in the Defense Forces of Ukraine. Instrument Engineering: State and Prospects. XXIII International Scientific and Technical Conference, Kyiv, Ukraine: Conference Proceedings. Kyiv: Igor Sikorsky KPI, 305–309.
2. Ivanskyi, V. M., Baranov, A. M., & Baranov, Yu. M. (2020). Problems of logistical support of the Armed Forces of Ukraine. *Information Technologies: Science, Engineering, Technology, Education, Health*, 5, 104.
3. Bartl, P., & Bader, J. Standardising lubricants and fuels for NATO applications. Available from: https://www.fuelsandlubes.com/fli-article/standardising-lubricants-and-fuels-for-nato-applications/ (Accessed: 20.02.2025).
4. Dobrovolskyi, A., & Romanchenko, V. (2022). Analysis of factors influencing the efficiency indicators of logistical support for the supply and transportation of material and technical resources under combat conditions. *Collection of Scientific Papers of the National Academy of the State Border Guard Service of Ukraine. Series: Military and Technical Sciences*, 4, 340–352.
5. Lyashenko, V., & Zadereyko, O. (2024). Analysis of factors affecting the survivability indicators of the logistics management system in military operations and ways to neutralize them. *Collection of Scientific Papers of the State Research Institute for Testing and Certification of Weapons and Military Equipmen*t, 20 (2), 55–59. https://doi.org/10.37701/dndivsovt.20.2024.07.

6. Sivak, V., Matsko, O., & Marchenko, D. (2021). Analysis of negative factors affecting the survivability indicators of the logistics support system under combat conditions and ways to neutralize them. *Collection of Scientific Papers of the National Academy of the State Border Guard Service of Ukraine. Series: Military and Technical Sciences*, 1, 272–287. https://doi.org/10.32453/3.v84i1.815.
7. Ministry of Transport of Ukraine. (1998). On Approval of Fuel and Lubricant Consumption Standards in Road Transport: Order No. 43, dated 10.02.1998. Available from: https://zakon.rada.gov.ua/rada/show/v0043361–98#Text (Accessed: 19.02.2025).
8. Ministry of Transport and Communications of Ukraine. (2008). On Approval of Fuel and Lubricant Consumption Standards for Special Rolling Stock: Order No. 244, dated 03.03.2008. Available from: https://zakon.rada.gov.ua/rada/show/v0244650–08#Text (Accessed: 19.02.2025).
9. Department of Defense (DoD), Defense Logistics Agency (DLA). Military Standard: Quality Assurance for Petroleum Products, Lubricants, and Related Products (MIL-STD – 3004C). Available from: https://www.dla.mil/Portals/104/Documents/Energy/Quality%20and%20Technical%20Support/E_MilSTD3004_1603.pdf (Accessed: 17.02.2025).
10. MTU Center for Dependable Transportation. (n. d.). ET – 148 Final Report to NATO. Michigan Technological University, 231 p. Available from: https://www.mtu.edu/cdt/downloadable-materials/et–148-final-report-to-nato.pdf
11. Tesnikov, O., & Fursova, V. (2022). Factors influencing the functioning of the logistics support system of the Armed Forces of Ukraine during wartime. *Economy and Society*, 42. https://doi.org/10.32782/2524–0072/2022–42–17.
12. Vorobyov, O., Vlasov, I., Tyagay, S., & Bambulyak, M. (2022). Justification of ways to use modern information technologies for accounting material resources in the fuel service of the Armed Forces of Ukraine based on the experience of leading countries. *Modern Information Technologies in the Field of Security and Defense*, Kyiv, Ukraine, 43 (1), 53–58. https://doi.org/10.33099/2311–7249/2022–43–1–53–58.
13. Torichnyi, V. O., & Raiko, V. V. (2023). Technical support as a component of the logistics support of Ukraine's security forces: A comparative analysis (Ukraine-NATO). *Scientific Innovations and Advanced Technologies,* 10 (24), 211–220. https://doi.org/10.52058/2786–5274–2023–10(24)–211–220.

Нормативне регулювання супроводження експлуатації інформаційних систем військового призначення: проблеми та шляхи вдосконалення

Regulatory framework for the military information systems support and operation: problems and ways of improvement

Андрій Дядечко
Corresponding author: доктор філософії, начальник науково-дослідного відділу проблем супроводження експлуатації інформаційних систем, e-mail: andrewvvs@gmail.com, ORCID: 0000-0003-0191-8326

Галина Руденська
старший науковий співробітник науково-дослідного відділу проблем супроводження експлуатації інформаційних систем, e-mail: rudenska85@ukr.net, ORCID: 0000-0002-4719-3765

Національний університет оборони України, м. Київ, Україна

Andrii Diadechko
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

Galyna Rudenska
Senior Researcher of Research Department on Information Systems Support and Operation Issues, e-mail: rudenska85@ukr.net, ORCID: 0000-0002-4719-3765

National Defense University of Ukraine, Kyiv, Ukraine

Received: April 11, 2025 | Revised: April 23, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.7

Мета роботи: є аналіз проблем нормативного регулювання супроводження експлуатації інформаційних систем військового призначення та обґрунтування необхідності створення узагальненого військового стандарту, який би забезпечив ефективну організацію та управління цими процесами.

Метод дослідження: методи системного аналізу, порівняльного аналізу нормативно-правових документів, а також експертні оцінки ефективності чинного регулювання.

Результати дослідження: визначено ключові проблеми нормативного регулювання супроводження експлуатації інформаційних систем військового призначення, серед яких: фрагментарність нормативної бази, невідповідність сучасним технологічним викликам, відсутність єдиних стандартів безпеки та управління життєвим циклом інформаційних систем. Обґрунтовано необхідність розробки військового стандарту, який би встановлював єдині вимоги до супроводження експлуатації таких систем.

Теоретична цінність дослідження: стаття доповнює наукову базу щодо нормативного забезпечення супроводження експлуатації інформаційних систем військового призначення, пропонуючи системний підхід до їхнього регулювання. Розроблені концептуальні підходи можуть бути використані для формування методологічних основ військових стандартів у цій сфері.

Практична цінність дослідження: результати дослідження можуть бути використані при розробці та вдосконаленні нормативних документів, які регламентують супроводження експлуатації інформаційних систем в оборонному секторі. Запропоновані рішення сприятимуть підвищенню ефективності та безпеки функціонування інформаційних систем військового призначення.

Цінність дослідження: наукова новизна дослідження полягає у комплексному аналізі проблем нормативного забезпечення супроводження експлуатації інформаційних систем військового призначення та обґрунтуванні необхідності створення військового стандарту. Вперше пропонується системний підхід до розробки єдиного нормативного документа, що забезпечить уніфіковане та ефективне управління процесами супроводження експлуатації інформаційних систем в оборонному секторі.

Тип статті: теоретичний з практичними рекомендаціями.

Purpose: is to analyze regulatory challenges in maintaining and operating military information systems and justify the need for a unified military standard to ensure effective organization and management.

Method: system analysis, comparative analysis of regulatory documents, and expert assessments of current regulation effectiveness.

Research results: Key regulatory challenges in maintaining and operating military information systems have been identified, including fragmented regulations, misalignment with modern technological challenges, and the lack of unified security and lifecycle management standards. The need for a military standard establishing uniform requirements for these processes is substantiated.

Theoretical implications: The article contributes to the scientific foundation of regulatory support for maintaining and operating military information systems by proposing a systematic approach to their regulation. The developed conceptual approaches can be used to establish the methodological basis for military standards in this field.

Practical implications: The research findings can be used in the development and improvement of regulatory documents governing the maintenance and operation of information systems in the defense sector. The proposed solutions will enhance the efficiency and security of military information systems.

Originality / Value: The scientific novelty of the study lies in the comprehensive analysis of regulatory challenges in maintaining and operating military information systems and the justification for the creation of a military standard. For the first time, a systematic approach is proposed for developing a unified regulatory document that will ensure standardized and effective management of information system maintenance processes in the defense sector.

Type of article: theoretical with practical recommendations.

Ключові слова: інформаційні системи, супроводження експлуатації, нормативне регулювання, військовий стандарт.

Key words: information systems, operation support, normative regulation, military standard.

Вступ

Супроводження експлуатації інформаційних систем (далі – ІС) військового призначення є невід'ємною складовою їх життєвого циклу, що забезпечує стабільне функціонування, належний рівень інформаційної безпеки, а також своєчасну адаптацію до змін оперативно-тактичних умов. Ефективне управління процесами супроводження потребує наявності чіткої нормативно-правової бази, яка встановлювала б уніфіковані вимоги до організації, моніторингу, модернізації, технічної підтримки та інформаційного захисту таких систем.

Попри наявність окремих нормативних документів, що регламентують специфічні аспекти супроводження ІС, наразі відсутній єдиний інтегрований військовий стандарт, який би системно охоплював усі етапи та компоненти цього процесу. Існуюче нормативне забезпечення має фрагментарний характер, не повною мірою враховує сучасні технологічні виклики, зокрема зростаючу складність архітектури ІС, динамічність бойового середовища та загрозу кібернетичних атак, а також не забезпечує узгодженості дій між усіма суб'єктами супроводу.

Відсутність інтегрованого підходу ускладнює координацію між підрозділами, відповідальними за технічне обслуговування, оновлення програмного забезпечення, контроль безпеки та експлуатаційну підтримку. Це, своєю чергою, може призводити до зниження ефективності функціонування ІС, зростання операційних ризиків, зниження готовності систем до роботи в умовах бойових дій.

Метою цієї статті є ідентифікація ключових проблем нормативного забезпечення супроводження експлуатації ІС військового призначення та обґрунтування доцільності розробки уніфікованого військового стандарту, який би забезпечував систематизацію, стандартизацію та ефективне регламентування процесів супроводження з урахуванням специфіки сучасного гібридного та інформаційного протиборства.

Теоретичні основи дослідження

Аналіз чинних нормативних документів [1–39] засвідчив, що нормативне регулювання супроводження експлуатації ІС військового призначення охоплює сукупність стандартів, інструкцій, регламентів і методичних рекомендацій, які визначають вимоги до функціонування, безпеки, модернізації та технічної підтримки таких систем. Основною метою відповідного регулювання є забезпечення стабільної експлуатації ІС, підвищення ефективності їх застосування у військових операціях, а також мінімізація ризиків, пов'язаних з їх використанням в умовах бойових дій.

Нормативні акти, що регламентують супроводження ІС, умовно поділяються на чотири основні категорії:

міжнародні стандарти з управління життєвим циклом ІС;

стандарти з інформаційної безпеки;

стандарти НАТО;

національні нормативні документи (ДСТУ, керівні документи Міністерства оборони України тощо).

Попри наявність зазначених документів, у сфері супроводження експлуатації ІС військового призначення досі відсутній єдиний комплексний нормативний акт, який би системно регламентував усі аспекти супроводження протягом життєвого циклу ІС.

Досвід країн-членів НАТО демонструє ефективність функціонування військових ІС на основі чітких стандартів. Зокрема:

- **AAP-20** *NATO Programme Management Framework (NATO Life Cycle Model)* визначає етапи життєвого циклу військових систем, включаючи експлуатацію, супроводження,

оцінювання технічного стану, обґрунтування модернізації або виведення з експлуатації;

- **STANAG 4728** *System Life Cycle Management* формулює рамкові положення щодо управління життєвим циклом ІС, забезпечуючи їх надійність, адаптивність та відповідність вимогам НАТО;
- **AAP-48** *NATO System Life Cycle Processes* описує процеси, необхідні для підтримання працездатності ІС, включаючи технічне обслуговування, оновлення та модернізацію, а також процедури внесення змін з метою відповідності новим вимогам і технологіям.

У більшості країн-членів Альянсу запроваджено уніфіковані стандарти супроводження, що забезпечують взаємосумісність, узгодженість процесів і оперативну готовність ІС в оборонному секторі.

Аналіз наукової літератури свідчить про розробку окремих підходів до нормативного забезпечення супроводження експлуатації ІС військового призначення. Зокрема:

у [40] досліджено адміністративно-правові засади використання та розвитку інформаційних технологій в умовах воєнного стану, підкреслено важливість адаптації нормативної бази до нових викликів інформаційного простору;

у [41] розглянуто моделі та процеси життєвого циклу ІС управління оборонними ресурсами, з акцентом на виборі оптимальної моделі для ефективного супроводження;

у [42] проаналізовано підходи до розробки спеціалізованого програмного забезпечення для ІС військового призначення з урахуванням вимог до їх нормативної сумісності та функціональної специфіки;

у [43] висвітлено організаційні аспекти інформаційно-аналітичної підтримки проектів розроблення, впровадження та супроводження ІС, з акцентом на необхідності нормативного регламентування процесів управління життєвим циклом;

у [44] представлено сучасні методи організації технологічної підтримки інформаційної інфраструктури Міністерства оборони України, де наголошено на ролі кібербезпеки й інформаційного захисту у виконанні оборонних завдань.

Запропоновані в цих наукових працях концепції можуть бути використані як методологічна основа для розроблення уніфікованого військового стандарту супроводження експлуатації ІС, що сприятиме підвищенню надійності, стійкості та оперативної ефективності систем у Збройних Силах України.

Постановка проблеми

В умовах стрімкого розвитку цифрових технологій, ускладнення кіберзагроз і зростання вимог до оперативного управління оборонними ресурсами, питання ефективного нормативного регулювання процесів супроводження експлуатації ІС військового призначення набуває особливої актуальності.

Аналіз чинної нормативної бази у сфері супроводження ІС дозволяє виокремити низку системних проблем, які суттєво ускладнюють організацію цього процесу:

- **фрагментарність нормативного забезпечення**, що проявляється у відсутності єдиного комплексного документа, який би охоплював усі аспекти супроводження ІС протягом їх життєвого циклу; наявні нормативні акти регламентують лише окремі елементи, не забезпечуючи цілісного підходу;
- **невідповідність сучасним технологічним викликам** – чинні нормативні документи не враховують специфіку використання новітніх технологій, зокрема хмарних обчислень, штучного інтелекту, аналітики великих даних (Big Data) та комплексних систем кіберзахисту;
- **недостатня гармонізація національних стандартів з міжнародними** – існує розрив між національними нормативами та положеннями ключових документів НАТО, таких як

AAP-20, AAP-48, STANAG 4728, що ускладнює сумісну діяльність у рамках багатонаціональних оборонних програм;

- **відсутність уніфікованих вимог до технічного обслуговування, оновлення та модернізації ІС** – чинні нормативи не містять чітко визначених процедур супроводження програмного забезпечення, управління життєвим циклом ІС, а також реагування на технічні збої й несправності;
- **недостатня увага до аспектів кібербезпеки у процесі супроводження** – відсутні комплексні нормативні вимоги щодо оцінки кіберризиків, управління вразливостями, впровадження заходів інформаційного захисту та оперативного реагування на кіберінциденти в процесі експлуатації ІС.

З огляду на вищезазначене, виникає об'єктивна необхідність розроблення єдиного військового стандарту, який би нормативно врегулював ключові аспекти супроводження експлуатації ІС військового призначення з урахуванням міжнародного досвіду та сучасних технологічних викликів.

У процесі аналізу існуючих нормативно-правових актів встановлено, що на сьогодні супроводження експлуатації ІС регламентується значною кількістю розрізнених документів, які охоплюють лише окремі етапи або функціональні напрямки. Відсутність систематизованого підходу до реалізації супровідних заходів ускладнює організацію та управління відповідними процесами, що негативно впливає на загальну ефективність експлуатації ІС.

Таким чином, актуальним є:

узагальнення нормативних положень щодо організації та виконання заходів супроводження;

систематизація відповідних процесів супроводу;

інтеграція вимог чинних нормативних актів в єдиний комплексний документ, який регламентуватиме повний спектр заходів супроводження експлуатації ІС військового призначення.

Розробка такого документа дозволить створити уніфіковану нормативну основу для забезпечення ефективного, безпечного та технологічно адаптивного функціонування інформаційних систем у Збройних Силах України.

Методологія дослідження

У статті розглядаються нормативно-правові та організаційно-методичні аспекти супроводження експлуатації ІС військового призначення в Україні. Здійснено аналіз чинних національних нормативних актів, які регламентують відповідні процеси, а також міжнародних стандартів та стандартів НАТО, що можуть бути використані як основа для удосконалення нормативного регулювання у вітчизняній оборонній сфері.

Для проведення дослідження використано такі джерела інформації:

- нормативно-правові акти України, які регламентують супроводження експлуатації ІС;
- міжнародні стандарти *ISO/IEC/IEEE* та стандарти НАТО, що визначають підходи до управління життєвим циклом військових ІС;
- наукові публікації, аналітичні матеріали та експертні огляди, присвячені питанням нормативного забезпечення супроводження ІС;
- результати експертного аналізу сучасних тенденцій і кращих практик у сфері військової інформатизації.

Методологічну основу дослідження становлять такі підходи:

- **системний аналіз**, що застосовується для виявлення ключових недоліків у чинному нормативному регулюванні супроводження експлуатації ІС;
- **порівняльний аналіз**, який дозволяє зіставити національні підходи з міжнародними та стандартами НАТО з метою виявлення прогалин і визначення напрямів удосконалення

нормативної бази;

- **контент-аналіз нормативних документів**, спрямований на оцінку відповідності чинного регулювання сучасним технологічним викликам;
- **метод прогнозування**, який використовується для обґрунтування доцільності розроблення уніфікованого військового стандарту супроводження експлуатації ІС та оцінки його потенційного впливу на ефективність функціонування ІС у сфері оборони.

Дослідження сфокусоване виключно на етапі експлуатації ІС, без розгляду інших фаз життєвого циклу, таких як проєктування, розробка чи виведення з експлуатації. Крім того, аналіз обмежено відкритими офіційними нормативними документами та публічними науковими джерелами, без використання конфіденційної або засекреченої інформації з оборонного сектору.

Результати

Відсутність єдиного нормативного документа, який комплексно регламентує процес супроводження експлуатації ІС військового призначення, ускладнює забезпечення їхньої безперервної, надійної та ефективної роботи в умовах сучасних загроз і технологічних викликів. Існуючі в Україні нормативно-правові акти та технічні стандарти охоплюють лише окремі аспекти цього процесу, що призводить до фрагментації підходів і створює додаткові труднощі у практичному впровадженні заходів експлуатаційної підтримки.

З метою обґрунтування оптимального підходу до нормативного регулювання супроводження експлуатації ІС здійснено аналіз чинної нормативної бази України, міжнародних стандартів управління життєвим циклом ІС, а також відповідних документів НАТО і провідних країн-партнерів. Дослідження охоплювало ключові положення, що стосуються організації експлуатаційної підтримки, управління конфігурацією, технічного обслуговування, забезпечення інформаційної безпеки та удосконалення функціональних характеристик систем у процесі їхньої експлуатації.

На основі результатів аналізу визначено доцільний порядок супроводження експлуатації ІС військового призначення, що включає основні заходи, відповідальних виконавців та нормативно-правову базу, яка забезпечує правове та організаційне підґрунтя (див. таблицю).

Крім того, з урахуванням передового міжнародного досвіду та специфіки функціонування ІС в оборонному секторі, у статті запропоновано структуру військового стандарту, який може бути покладений в основу створення єдиного нормативного документа з питань супроводження експлуатації ІС військового призначення.

Таблиця 1 – Порядок супроводження експлуатації інформаційних систем

№ п/п	Етап супроводження	Основні заходи	Відповідальні суб'єкти	Нормативна основа
1.	Планування супроводження експлуатації ІС	- Формування плану супроводження; - Категоризація ІС за рівнем критичності; - Розробка регламентів та інструкцій.	Органи управління, розпорядники ІС	ЗУ "Про захист інформації в ІКС", ДСТУ ISO/IEC/IEEE 12207:2018, ДСТУ ISO/IEC/IEEE 15288:2016, ДСТУ В 15.003:2021, AAP-48, ДСТУ ISO/IEC 27005, ADatP-4774, ADatP-4778, ДСТУ ISO/IEC/IEEE 27001:2023, ДСТУ ISO/IEC 20000, MC 0458/4

№ п/п	Етап супроводження	Основні заходи	Відповідальні суб'єкти	Нормативна основа
2.	Організація технічного супроводження	- Моніторинг та діагностика стану ІС; - Регламентні роботи та технічне обслуговування; - Виявлення та усунення несправностей; - Резервне копіювання та відновлення.	Органи управління, розпорядники ІС, служби технічної підтримки підрозділів ІКС	ДСТУ ISO/IEC 27035, ДСТУ ISO/IEC 27002, ДСТУ ISO/IEC 20000, ДСТУ ISO/IEC 14764, STANAG 4728, ДСТУ В 15.003:2021, ДСТУ ISO/IEC/IEEE 12207:2018, ДСТУ ISO/IEC 27031, ДСТУ EN ISO 22301, ДСТУ ISO/IEC/IEEE 27001, Наказ МОУ № 240/нм від 17.04.24
3.	Управління оновленнями та модернізація ІС	- Політика керування оновленням; - Адаптація ІС до нових вимог.	Органи управління, розпорядники ІС, розробники ІС, підрядники	ДСТУ ISO/IEC 14764, ДСТУ ISO/IEC 20000, NIST SP 800-128, ДСТУ В 15.003:2021, ДСТУ ISO/IEC/IEEE 12207:2018, ДСТУ ISO/IEC/IEEE 15288:2016, AAP-48, COBIT 2019
4.	Кібербезпека під час супроводження експлуатації ІС	- Управління доступом та автентифікація; - Управління вразливостями та реагування на інциденти; - Контроль безпеки каналів передачі даних; - Організація безперервного підвищення рівня безпеки	Органи управління, розпорядники ІС, підрозділи кібербезпеки, служби захисту інформації	ЗУ "Про захист інформації в ІКС", ПКМУ № 518 від 19.06.2019, ДСТУ ISO/IEC/IEEE 27001:2023, ДСТУ ISO/IEC 27002, NIST SP 800-53, NIST SP 800-61, NIST SP 800-77, NIST SP 800-184, ДСТУ ISO/IEC 27035, ДСТУ ISO/IEC 15408, ДСТУ ISO/IEC 27033, ДСТУ ISO/IEC 29128, ДСТУ ISO/IEC 27005, ДСТУ ISO/IEC 27032
5.	Інформаційно-аналітичне забезпечення супроводження експлуатації ІС	- Збирання та обробка експлуатаційних даних; - Аналіз ефективності роботи ІС та її компонентів; - Формування рекомендацій щодо вдосконалення супроводження експлуатації; - Ведення бази даних щодо історії технічного обслуговування та інцидентів; - Використання методів прогнозування для оптимізації процесів супроводження.	Органи управління, розпорядники ІС, служби технічної підтримки підрозділів ІКС, аналітичні підрозділи	ЗУ "Про захист інформації в ІКС", ЗУ "Про інформацію", ДСТУ ISO/IEC 27004, NIST SP 800-137, AAP-20

№ п/п	Етап супроводження	Основні заходи	Відповідальні суб'єкти	Нормативна основа
6.	Контроль та аудит процесів супроводження експлуатації ІС	- Регулярний моніторинг стану ІС; - Періодичні аудити та перевірки; - Аналіз вразливостей та ризиків; - Удосконалення процесів супроводження.	Органи управління, розпорядники ІС, підрозділи кібербезпеки, внутрішні аудитори та інспекційні органи	ДСТУ ISO/IEC 27001, ДСТУ ISO/IEC 27002, ДСТУ ISO/IEC 27007, ДСТУ ISO/IEC 27008, ДСТУ ISO/IEC 20000, COBIT 2019, NIST SP 800-53
7.	Фінансово-економічне забезпечення супроводження експлуатації ІС	- Планування витрат; - Контроль бюджетування.	Органи управління, розпорядники ІС, фінансово-економічні підрозділи	Закон України "Про публічні закупівлі", ПКМУ № 339 від 27.05.2015, ПКМУ № 262 від 08.03.2024, ПКМУ № 544 від 23.08.2016, ДСТУ ISO/IEC 38500

На основі визначеного порядку супроводження експлуатації інформаційних систем (ІС) військового призначення запропоновано структуру військового стандарту, що забезпечить комплексне нормативне регулювання відповідних процесів. Такий стандарт має на меті уніфікацію вимог, процедур і відповідальності на всіх етапах експлуатаційної підтримки ІС з урахуванням сучасних технологічних викликів та міжнародного досвіду.

Проєкт структури військового стандарту ВСТ 600.XXX.XXX:20XX

1. Загальні положення

1.1. Призначення стандарту

1.2. Сфера застосування

1.3. Нормативні посилання

1.4. Терміни, визначення та скорочення

2. Загальні вимоги до супроводження експлуатації ІС

2.1. Принципи супроводження

2.2. Класифікація ІС за рівнем критичності та її вплив на супроводження

2.3. Види супроводження (профілактичне, коригувальне, адаптаційне, удосконалювальне)

2.4. Взаємодія між розробником, експлуатуючою організацією та користувачами

3. Організація процесів супроводження експлуатації ІС

3.1. Планування та організація супроводження

3.2. Вимоги до технічного супроводу

3.3. Контроль працездатності та управління інцидентами

3.4. Взаємодія з користувачами та функціонування служби підтримки

4. Технічна підтримка та обслуговування ІС

4.1. Моніторинг і діагностика стану ІС

.2. Проведення регламентних робіт та технічного обслуговування

4.3. Виявлення, аналіз та усунення відмов

4.4. Оцінка продуктивності ІС і виявлення "вузьких місць"

4.5. Забезпечення безперервного функціонування та аварійного відновлення

5. Кібербезпека в процесі супроводження ІС

5.1. Вимоги до захисту інформації

5.2. Політики доступу, автентифікації та управління привілеями

5.3. Управління вразливостями та реагування на кіберінциденти

5.4. Захист каналів передачі даних

5.5. Резервне копіювання та відновлення даних

6. Оновлення та модернізація ІС під час експлуатації

6.1. Класифікація оновлень (функціональні, безпекові, технічні)

6.2. Політика управління оновленнями та порядок попереднього тестування

6.3. Забезпечення зворотної сумісності

6.4. Документування змін

7. Інформаційно-аналітичне забезпечення супроводження

7.1. Системи збору та аналізу даних про функціонування ІС

7.2. Прогнозування відмов і оцінка ризиків

7.3. Використання автоматизованих систем управління супроводженням

7.4. Застосування технологій штучного інтелекту для підтримки прийняття рішень

8. Підготовка персоналу та навчання

8.1. Програми підготовки користувачів

8.2. Підвищення кваліфікації технічного персоналу

8.3. Навчання реагуванню на інциденти

8.4. Оцінювання результативності підготовки

9. Контроль та аудит процесів супроводження

9.1. Критерії оцінювання ефективності супроводження

9.2. Порядок проведення внутрішнього аудиту

9.3. Забезпечення якості процесів супроводження

9.4. Документування та звітування за результатами аудиту

10. Фінансово-економічне забезпечення супроводження

10.1. Планування витрат на супроводження

10.2. Оптимізація витрат і оцінка економічної ефективності

10.3. Контроль бюджетного використання ресурсів

10.4. Альтернативні моделі фінансування (аутсорсинг, державно-приватне партнерство)

Запропонована структура охоплює всі ключові компоненти процесу супроводження експлуатації ІС військового призначення, створюючи підґрунтя для уніфікації підходів, підвищення ефективності, забезпечення надійності та кіберстійкості систем в умовах гібридних загроз та швидких технологічних змін.

Висновки

Таким чином, у ході проведеного дослідження здійснено комплексний аналіз нормативно-правового забезпечення супроводження експлуатації інформаційних систем військового призначення. Виявлено ключові проблеми, зокрема — відсутність єдиного нормативного документа, який би регламентував відповідні процеси та забезпечував уніфікацію підходів до їх реалізації.

На підставі аналізу міжнародного досвіду, зокрема стандартів НАТО та ISO, ідентифіковано основні напрями вдосконалення нормативної бази у сфері супроводження експлуатації ІС. У цьому контексті обґрунтовано доцільність розроблення військового стандарту, що охоплює всі ключові аспекти супроводження, включаючи технічне обслуговування, забезпечення інформаційної безпеки, управління оновленнями, кадрову підготовку та логістичну підтримку.

У межах дослідження розроблено проект структури зазначеного військового стандарту, що включає основні розділи та положення, спрямовані на нормативне регламентування процесів супроводження експлуатації ІС. Запропонована структура забезпечує системний і комплексний підхід до організації відповідної діяльності та сприяє підвищенню ефективності управління інформаційними системами військового призначення.

Отримані результати можуть бути використані в процесі розроблення нормативно-правових актів, що регламентують супроводження експлуатації інформаційних систем у Міністерстві оборони України та інших структурах сектору безпеки і оборони.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Про захист інформації в інформаційно-комунікаційних системах: Закон України № 80/94-ВР від 05.07.1994 (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/80/94-вр. (Дата звернення: 10.03.2025).
2. Про інформацію: Закон України № 2657-XII від 02.10.1992 (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/2657-12. (Дата звернення 10.03.2025).
3. Про публічні закупівлі: Закон України № 922-VIII від 25.12.2015 (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/922-19. (Дата звернення 11.03.2025).
4. Про затвердження вимог до кіберзахисту об’єктів критичної інфраструктури: Постанова Каб. Міністрів України № 518 від 19.06.2019 (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/518-2019. (Дата звернення 25.03.2025).
5. Про затвердження Порядку фінансового забезпечення потреб національної оборони держави, мобілізаційної підготовки, заходів з мобілізації та Збройних Сил за рахунок благодійних пожертв фізичних та юридичних осіб: Постанова Каб. Міністрів України № 339 від 27.05.2015. URL: https://zakon.rada.gov.ua/laws/show/339-2015. (Дата звернення 14.03.2025).
6. Деякі питання забезпечення розвитку інновацій та технологій для потреб оборони: Постанова Каб. Міністрів України № 262 від 08.03.2024. URL: https://zakon.rada.gov.ua/laws/show/262-2024. (Дата звернення 18.03.2025).
7. Про затвердження Порядку використання коштів, передбачених у державному бюджеті для виконання державних цільових програм реформування та розвитку оборонно-промислового комплексу, розроблення, освоєння і впровадження нових технологій, нарощування наявних виробничих потужностей для виготовлення продукції оборонного призначення: Постанова Каб. Міністрів України № 544 від 23.08.2016 (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/544-2016. (Дата звернення 18.03.2025).
8. Про затвердження Порядку організації в системі Міністерства оборони України технічної підтримки інформаційних (автоматизованих), інформаційно-комунікаційних, електронних комунікаційних систем, систем спеціального зв'язку та користувачів таких систем: Наказ Міністерства оборони України № 240/нм від 17.04.2024. URL: https://zakon.rada.gov.ua/rada/show/v0240322-24. (Дата звернення 19.03.2025).
9. ISACA. COBIT 2019 Framework: Governance and Management Objectives. ISACA, 2018. 252 с.
10. ДСТУ ISO/IEC/IEEE 12207:2018. Інженерія систем і програмних засобів. Процеси життєвого циклу програмних засобів. Дійсний з 15.08.2018. ДП «УкрНДНЦ», 2018.
11. ДСТУ ISO/IEC/IEEE 15288:2016. Інженерія систем і програмного забезпечення. Процеси життєвого циклу систем. Дійсний з 01.01.2018. ДП «УкрНДНЦ», 2016.

12. ДСТУ ISO/IEC/IEEE 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги. Дійсий з 22.08.2023. ДП «УкрНДНЦ», 2023.
13. ДСТУ ISO/IEC 27002:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки. Дійсний з 22.08.2023. ДП «УкрНДНЦ», 2023.
14. ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання. Дійсний з 01.10.2018. ДП «УкрНДНЦ», 2018.
15. ДСТУ ISO/IEC 27005:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки. Дійсний з 22.08.2023. ДП «УкрНДНЦ», 2023.
16. ДСТУ ISO/IEC 27007:2018. Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою. Дійсний з 01.01.2019. ДП «УкрНДНЦ», 2018.
17. ДСТУ ISO/IEC TS 27008:2019. Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки. Дійсний з 01.11.2019. ДП «УкрНДНЦ», 2019.
18. ДСТУ ISO/IEC 27031:2015. Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу. Чинний з 01.01.2016. ДП «УкрНДНЦ», 2015.
19. ДСТУ ISO/IEC 27032:2024 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки. Дійсний з 01.02.2025. ДП «УкрНДНЦ», 2024.
20. Серія стандартів ДСТУ ISO/IEC 27033. Інформаційні технології. Методи захисту. Захист мережі. Частини 1 – 6. ДП «УкрНДНЦ».
21. Серія стандартів ДСТУ ISO/IEC 27035. Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частини 1 – 3. ДП «УкрНДНЦ».
22. Серія стандартів ДСТУ ISO/IEC 20000. Інформаційні технології. Керування послугами. Частини 1 – 12. ДП «УкрНДНЦ».
23. ДСТУ ISO/IEC 14764:2014. Інженерія програмного забезпечення. Процеси життєвого циклу програмного забезпечення. Технічне обслуговування. Дійсний з 01.01.2016. ДП «УкрНДНЦ», 2014.
24. ДСТУ EN ISO 22301:2021. Безпека та стабільність. Системи управління неперервністю бізнесу. Вимоги. Чинний з 01.09.2022. ДП «УкрНДНЦ», 2021.
25. Серія стандартів ДСТУ ISO/IEC 15408. Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частини 1 – 5. ДП «УкрНДНЦ».
26. ДСТУ ISO/IEC 29128-1:2024 Інформаційна безпека, кібербезпека та захист конфіденційності. Перевірка криптографічних протоколів. Частина 1. Структура. Дійсний з 01.02.2025. ДП «УкрНДНЦ», 2024.
27. ДСТУ ISO/IEC 38500:2016 Інформаційні технології. Управління ІТ в організації. Дійсний з 01.10.2017. ДП «УкрНДНЦ», 2016.
28. ДСТУ В 15.003:2021. Система розроблення і поставлення на виробництво озброєння та військової техніки. Процеси життєвого циклу озброєння та військової техніки. Дійсний з 01.09.2022. ДП «УкрНДНЦ», 2021.
29. AAP-20. NATO Programme Management Framework (NATO Life Cycle Model). Ed. C, v. 1. NSO, Brussels, 1110 Belgium, 2015, 78 p.
30. AAP-48. NATO System Life Cycle Processes. Ed. C, v. 1. NSO, Brussels, 1110 Belgium, 2022, 202 p.
31. STANAG 4728. System Life Cycle Management. Ed. 2. NSO, Brussels, 1110 Belgium, 2022, 5 p.
32. ADatP-4774. Confidentiality metadata. Label Syntax. Ed. A, Ver. 1. NATO, Allied Data Processing Publication, 2017, 108 p.

33. ADatP-4778. Metadata Binding Mechanism. Ed. A, Ver. 1. NATO, Allied Data Processing Publication, 2018, 72 p.
34. MC 0458/4. NATO Education, Training, Exercises and Evaluation Policy. NATO, 2023, 48 p.
35. NIST SP 800-37 Rev. 2. Risk Management Framework (RMF) For Information System and Organizations. A System Life Cycle Approach for Security and Privacy. National Institute of Standards and Technology, U.S., Gaithersburg, 2018, 183 p.
36. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information System and Organizations. National Institute of Standards and Technology, U.S., Gaithersburg, 2020, 492 p.
37. NIST SP 800-83 Rev. 1. Guide to Malware Incident Prevention and Handling for Desktops and Laptops. National Institute of Standards and Technology, U.S., Gaithersburg, 2013, 47 p.
38. NIST SP 800-128. Guide for Security – Focused Configuration Management of Information System. National Institute of Standards and Technology, U.S., Gaithersburg, 2019, 99 p.
39. NIST SP 800-160 V. 1, Rev. 1. Engineering Trustworthy Secure System. National Institute of Standards and Technology, U.S., Gaithersburg, 2022, 195 p.
40. Серебро М.В. Особливості адміністративно-правового регулювання використання та розвитку інформаційних технологій в умовах воєнного стану. Київський часопис права, № 3, 2024, с. 177-183. https://doi.org/10.32782/klj/2024.3.26.
41. Руденська Г.В. Моделі та процеси життєвого циклу інформаційної системи управління оборонними ресурсами. Збірник наукових праць ЦВСД, № 1(68), Київ, НУОУ, 2020, с. 59-65. https://doi.org/10.33099/2304-2745/2020-0/59-65.
42. Рибидайло А., Галаган В., Васюхно С., Мулявка А., Руденська Г. Порядок організації створення спеціального програмного забезпечення для інформаційних систем військового призначення. Збірник наукових праць ЦВСД, № 1(77), Київ, НУОУ, 2023, с. 69-78. https://doi.org/10.33099/2304-2745/2023-1-77/69-78.
43. Бондарчук С., Васюхно С., Галаган В., Гріненко О. Пропозиції щодо організації інформаційно-аналітичної підтримки ведення проєктів інформатизації. Збірник наукових праць ЦВСД, № 3(73), Київ, НУОУ, 2021, с. 67-72. https://doi.org/10.33099/2304-2745/2021-3-73/68-73.
44. Андрій Дядечко, Іван Даценко, Олександр Головченко. Концептуальні аспекти технологічної підтримки інформаційної інфраструктури Міністерства оборони України. Сучасні інформаційні технології у сфері безпеки та оборони, № 51(3), Київ, НУОУ, 2024, с. 96-107. https://doi.org/10.33099/2311-7249/2024-51-3-96-107.

References

1. On the Protection of Information in Information and Communication Systems: Law of Ukraine No. 80/94-BP dated 05.07.1994 (as amended). Available from : https://zakon.rada.gov.ua/laws/show/80/94-вр. (Date of access: 10.03.2025).
2. For information: Law of Ukraine No. 2657-XII of 02.10.1992 (as amended). Available from : https://zakon.rada.gov.ua/laws/show/2657-12. (Date of access 10.03.2025).
3. On public procurement: Law of Ukraine No. 922-VIII of 25.12.2015 (as amended). Available from : https://zakon.rada.gov.ua/laws/show/922-19. (Date of access 11.03.2025).
4. On approval of requirements for cyber protection of critical infrastructure facilities: Resolution of the Cabinet of Ministers of Ukraine No. 518 of 19.06.2019 (as amended). Available from : https://zakon.rada.gov.ua/laws/show/518-2019. (Date of access 25.03.2025).
5. On approval of the Procedure for financial support of the needs of the national defense of the state, mobilization training, mobilization measures and the Armed Forces at the expense of charitable donations from individuals and legal entities: Resolution of the Cabinet of Ministers of Ukraine No. 339 of 27.05.2015. Available from : https://zakon.rada.gov.ua/laws/show/339-2015. (Date of application 14.03.2025).

6. Some issues of ensuring the development of innovations and technologies for defense needs: Resolution of the Cabinet of Ministers of Ukraine No. 262 of 08.03.2024. Available from : https://zakon.rada.gov.ua/laws/show/262-2024. (Date of access 18.03.2025).
7. On approval of the Procedure for the use of funds provided for in the state budget for the implementation of state target programs for the reform and development of the defense-industrial complex, the development, mastering and implementation of new technologies, and the expansion of existing production capacities for the manufacture of defense products: Resolution of the Cabinet of Ministers of Ukraine No. 544 of 23.08.2016 (as amended). Available from : https://zakon.rada.gov.ua/laws/show/544-2016. (Date of application 18.03.2025).
8. On approval of the Procedure for organizing technical support of information (automated), information and communication, electronic communication systems, special communication systems and users of such systems in the system of the Ministry of Defense of Ukraine: Order of the Ministry of Defense of Ukraine No. 240/nm dated 17.04.2024. Available from : https://zakon.rada.gov.ua/rada/show/v0240322-24. (Date of application 19.03.2025).
9. ISACA. COBIT 2019 Framework: Governance and Management Objectives. ISACA, 2018. 252 p.
10. DSTU ISO/IEC/IEEE 12207:2018. Systems and software engineering. Software life cycle processes. Valid from 15.08.2018. "UkrNDNC", 2018.
11. DSTU ISO/IEC/IEEE 15288:2016. Systems and Software Engineering. Systems Life Cycle Processes. Valid from 01.01.2018. "UkrNDNC", 2016.
12. DSTU ISO/IEC/IEEE 27001:2023. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. Valid from 22.08.2023. "UkrNDNC", 2023.
13. DSTU ISO/IEC 27002:2023. Information security, cybersecurity and privacy protection. Information security controls. Valid from 22.08.023. "UkrNDNC", 2023.
14. DSTU ISO/IEC 27004:2018 Information technologies. Protection methods. Information security management systems. Monitoring, measurement, analysis and evaluation. Valid from 01.10.2018. "UkrNDNC", 2018.
15. DSTU ISO/IEC 27005:2023. Information security, cybersecurity and privacy protection. Information security risk management guidance. Valid from 22.08.2023. "UkrNDNC", 2023.
16. DSTU ISO/IEC 27007:2018. Information technologies. Protection methods. Guidance on auditing information security management systems. Valid from 01.01.2019. "UkrNDNC", 2018.
17. DSTU ISO/IEC TS 27008:2019. Information technologies. Protection methods. Guidance on assessing information security protection. Valid from 01.11.2019. "UkrNDNC", 2019.
18. DSTU ISO/IEC 27031:2015. Information technologies. Protection methods. Guidelines for the readiness of information and communication technologies for business continuity. Valid from 01.01.2016. "UkrNDNC", 2015.
19. DSTU ISO/IEC 27032:2024 Information technology. Protection methods. Guidelines for cybersecurity. Valid from 01.02.2025. "UkrNDNC", 2024.
20. Series of standards DSTU ISO/IEC 27033. Information technologies. Protection methods. Network protection. Parts 1 – 6. "UkrNDNC".
21. Series of standards DSTU ISO/IEC 27035. Information technologies. Protection methods. Information security incident management. Parts 1 – 3. "UkrNDNC".
22. DSTU ISO/IEC 20000 series of standards. Information technology. Service management. Parts 1 – 12. "UkrNDNC".
23. DSTU ISO/IEC 14764:2014. Software engineering. Software life cycle processes. Maintenance. Valid from 01.01.2016. "UkrNDNC", 2014.
24. DSTU EN ISO 22301:2021. Security and stability. Business continuity management systems. Requirements. Effective from 01.09.2022. "UkrNDNC", 2021.

25. DSTU ISO/IEC 15408 series of standards. Information technologies. Cybersecurity and privacy protection. IT security assessment criteria. Parts 1 – 5. "UkrNDNC".
26. DSTU ISO/IEC 29128-1:2024 Information security, cybersecurity and privacy protection. Verification of cryptographic protocols. Part 1. Structure. Valid from 01.02.2025. "UkrNDNC", 2024.
27. DSTU ISO/IEC 38500:2016 Information technology. IT management in the organization. Valid from 01.10.2017. "UkrNDNC", 2016.
28. DSTU V 15.003:2021. System for the development and commissioning of weapons and military equipment. Life cycle processes of weapons and military equipment. Effective from 01.09.2022. "UkrNDNC", 2021.
29. AAP-20. NATO Programme Management Framework (NATO Life Cycle Model). Ed. C, v. 1. NSO, Brussels, 1110 Belgium, 2015, 78 p.
30. AAP-48. NATO System Life Cycle Processes. Ed. C, v. 1. NSO, Brussels, 1110 Belgium, 2022, 202 p.
31. STANAG 4728. System Life Cycle Management. Ed. 2. NSO, Brussels, 1110 Belgium, 2022, 5 p.
32. ADatP-4774. Confidentiality metadata. Label Syntax. Ed. A, Ver. 1. NATO, Allied Data Processing Publication, 2017, 108 p.
33. ADatP-4778. Metadata Binding Mechanism. Ed. A, Ver. 1. NATO, Allied Data Processing Publication, 2018, 72 p.
34. MC 0458/4. NATO Education, Training, Exercises and Evaluation Policy. NATO, 2023, 48 p.
35. NIST SP 800-37 Rev. 2. Risk Management Framework (RMF) For Information System and Organizations. A System Life Cycle Approach for Security and Privacy. National Institute of Standards and Technology, U.S., Gaithersburg, 2018, 183 p.
36. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information System and Organizations. National Institute of Standards and Technology, U.S., Gaithersburg, 2020, 492 p.
37. NIST SP 800-83 Rev. 1. Guide to Malware Incident Prevention and Handling for Desktops and Laptops. National Institute of Standards and Technology, U.S., Gaithersburg, 2013, 47 p.
38. NIST SP 800-128. Guide for Security – Focused Configuration Management of Information System. National Institute of Standards and Technology, U.S., Gaithersburg, 2019, 99 p.
39. NIST SP 800-160 V. 1, Rev. 1. Engineering Trustworthy Secure System. National Institute of Standards and Technology, U.S., Gaithersburg, 2022, 195 p.
40. Serebro M.V. Peculiarities of administrative and legal regulation of the use and development of information technologies under martial law. Kyiv Law Journal, No. 3, 2024, pp. 177-183. https://doi.org/10.32782/klj/2024.3.26.
41. Rudenska G.V. Models and processes of the life cycle of the information system for managing defense resources. Collection of scientific papers of the Central Scientific and Technical University of Ukraine, No. 1(68), Kyiv, NUOU, 2020, pp. 59-65. https://doi.org/10.33099/2304-2745/2020-0/59-65.
42. Rybydaylo A., Galahan V., Vasyukhno S., Mulyavka A., Rudenska G. The procedure for organizing the creation of special software for military information systems. Collection of scientific works of the Central Scientific and Technological Center, No. 1(77), Kyiv, NUOU, 2023, pp. 69-78. https://doi.org/10.33099/2304-2745/2023-1-77/69-78.
43. Bondarchuk S., Vasyukhno S., Galahan V., Grinenko O. Proposals for the organization of information and analytical support for conducting informatization projects. Collection of scientific works of the Central Scientific and Technological Center, No. 3(73), Kyiv, NUOU, 2021, pp. 67-72. https://doi.org/10.33099/2304-2745/2021-3-73/68-73.
44. Andrii Diadechko, Ivan Datsenko, Oleksandr Holovchenko. Conceptual aspects of technological support of the information infrastructure of the Ministry of Defense of Ukraine. Modern information technologies in the sphere of security and defense, No. 51(3), Kyiv, NUOU, 2024, pp. 96-107. https://doi.org/10.33099/2311-7249/2024-51-3-96-107.

Визначення системи показників та критерію оцінювання проходження військової служби за контрактом збройних сил з урахуванням рівня навченості

Definition of a System of Indicators and Assessment Criteria for Military Service Under a Contract in the Armed Forces Taking Into Account the Level of Education

Денис Іванін [A]
Corresponding author: ад'юнкт кафедри менеджменту персоналу і підготовки військ (сил), e-mail: srazin36@gmail.com, ORCID: 0009-0006-4287-2933

Андрій Стрепетов [A]
ад'юнкт кафедри менеджменту персоналу і підготовки військ (сил), e-mail: a.strepetov@gmail.com, ORCID: 0009-0006-1146-6561

Сергій Рудой [A]
ад'юнкт кафедри менеджменту персоналу і підготовки військ (сил), e-mail: srufous@gmail.com, ORCID: 0009-0007-6538-2299

Denis Ivanin [A]
Corresponding author: PhD student of the department of personnel management and training of troops (forces), e-mail: srazin36@gmail.com, ORCID: 0009-0006-4287-2933

Andrii Strepetov [A]
PhD student of the Department of Personnel Management and Training of Troops (Forces), e-mail: a.strepetov@gmail.com, ORCID: 0009-0006-1146-6561

Serhii Rudoi [A]
PhD student of the Department of Personnel Management and Training of Troops (Forces), e-mail: srufous@gmail.com, ORCID: 0009-0007-6538-2299

[A] Національний університет оборони України, м. Київ, Україна

[A] National Defense University of Ukraine, Kyiv, Ukraine

Received: April 13, 2025 | Revised: April 23, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.8

Мета роботи: вирішення актуального завдання щодо визначення показників і критерію оцінювання порядку проходження військової служби за контрактом Збройних Сил України.
Метод дослідження: аналіз, синтез, математичне моделювання.
Результати дослідження: У статті викладено показники та критерій оцінювання порядку проходження військової служби за контрактом Збройних Сил України.
Теоретична цінність дослідження: результати проведеного дослідження можуть бути використані в розробці методики оцінювання порядку проходження військової служби за контрактом збройних сил, а також у ході подальших досліджень з даного напряму в наукових установах.
Тип статті: науково-теоретична.

Purpose: is to solve the current problem of determining indicators and criteria for evaluating the procedure for completing military service under a contract in the Armed Forces of Ukraine.
Method: analysis, synthesis, and mathematical modeling.
Research results: The article presents indicators and criteria for evaluating the procedure for completing military service under a contract in the Armed Forces of Ukraine.
Theoretical implications: The results of the study can be used in developing a methodology for assessing the procedure for completing military service under a contract in the armed forces, as well as in the course of further research in this area in scientific institutions.
Type of article: scientific and theoretical article.

Ключові слова: збройні сили, військова служба, оцінювання, показники, критерій.

Key words: armed forces, military service, evaluation, indicators, criterion.

Вступ

Втрати людського потенціалу внаслідок збройної агресії російської федерації, низький рівень народжуваності, високий рівень смертності (приблизно третина громадян України помирає у віці до 65 років), а також зростання масштабів еміграції у пошуках кращих умов життя суттєво ускладнюють забезпечення достатньої чисельності кадрового та мобілізаційного резерву як у поточному періоді, так і в довгостроковій перспективі [1].

Зазначені негативні демографічні та соціальні тенденції суттєво впливають на здатність держави гарантувати потреби Збройних Сил України (далі – ЗС України) та інших складових сил оборони у людських ресурсах як під час широкомасштабної збройної агресії, так і в умовах післявоєнного відновлення. Вони також становлять виклик у контексті реалізації заходів оборонної реформи, спрямованої на посилення спроможностей сил оборони України,

підвищення їхньої боєготовності, забезпечення здатності виконувати завдання за призначенням, а також брати участь у спільних операціях (бойових діях) разом із підрозділами держав-членів НАТО.

Теоретичні основи дослідження

Аналіз наявних досліджень і публікацій у відповідній сфері свідчить про те, що більшість із них зосереджені на моделюванні проходження військової служби за посадами, водночас залишаючи поза увагою специфіку проходження служби за військовим званням. Такий підхід не повною мірою відображає концептуальні засади, визначені у стратегічних і доктринальних документах Міністерства оборони України та ЗС України, а також не відповідає принципам проходження військової служби, прийнятим у державах — членах НАТО [2, 3].

Зокрема, в одному з попередніх досліджень [4] авторами було запропоновано математичну модель у вигляді системи диференціальних рівнянь для опису процесу проходження військової служби за посадами. У праці [5] розглянуто підходи до визначення показників оцінювання ефективності системи кадрового менеджменту у військовій сфері, однак без урахування динаміки розвитку військовослужбовця за військовим званням.

Постановка проблеми

В умовах повномасштабної збройної агресії російської федерації проти України, а також на тлі існуючих і потенційних внутрішніх ризиків, триває активне удосконалення військової кадрової політики у ЗС України. Одним із її ключових завдань є формування ефективної моделі проходження військової служби, що передбачає модернізацію організаційно-штатної структури та функціональних засад кадрового управління.

У межах зазначеної трансформації пріоритет надається підвищенню вимог до військово-професійних якостей військовослужбовців усіх категорій. Це, у свою чергу, вимагає невідкладного реформування системи кадрового забезпечення з урахуванням потреб оборонного сектору в умовах воєнного стану та перспектив післявоєнного розвитку.

У зв’язку з цим актуалізується завдання пошуку та впровадження найбільш раціональних форм і методів організації проходження військової служби за контрактом у ЗС України [2].

Результати

Проходження військової служби за контрактом у ЗС України має бути спрямоване на розвиток професійних компетентностей військовослужбовців, подальше впровадження професіоналізації та формування спроможностей до ефективного управління підпорядкованими підрозділами, забезпечення виконання завдань за призначенням, організації підготовки особового складу, участі у процедурах прийняття рішень і виконанні штабних функцій в органах військового управління всіх рівнів. Крім того, це включає участь в управлінні військами (силами) у складі командних груп на займаних посадах, підтримання справності та готовності озброєння і військової техніки до бойового застосування, забезпечення військової дисципліни та правопорядку у підрозділах, а також збереження життя і здоров’я особового складу [1].

Для досягнення зазначених цілей особливу увагу необхідно приділяти підготовці, кар’єрному зростанню (присвоєнню військових звань, призначенню на посади тощо) та формуванню ефективної системи мотивації.

Військова служба за контрактом у ЗС України є невід’ємно пов’язаною з багаторівневою системою підготовки, що забезпечує послідовну професіоналізацію військовослужбовців, їх готовність до виконання функціональних обов’язків на посадах різного рівня. Зазначене відповідає загальним підходам і вимогам до підготовки військовослужбовців, прийнятим у

збройних силах держав–членів НАТО, зокрема визначеним у *Non-Commissioned Officer Professional Military Education Reference Curriculum*.

Поряд із питаннями належного укомплектування Збройних Сил України кваліфікованим і досвідченим персоналом, актуалізується проблема довгострокового утримання військових професіоналів на службі, ефективного управління їх кар'єрною траєкторією та раціонального кадрового використання. Важливим є також надання належних повноважень, забезпечення відповідного соціального захисту, створення й підтримання комплексу матеріальних і нематеріальних мотиваційних чинників проходження військової служби за контрактом.

Одним із ключових завдань дослідження у межах науки про військові операції є декомпозиція системи, яка реалізується за допомогою методу системного аналізу. Застосування цього підходу дозволяє обґрунтовано визначити сукупність показників, що характеризують ефективність проходження військової служби за контрактом у ЗС України [6].

У процесі визначення ієрархії показників проходження військової служби за контрактом застосовано метод системного аналізу з урахуванням принципу, згідно з яким математична модель не повинна включати надмірну кількість другорядних параметрів. Це дозволяє уникнути ускладнення моделі через незначні або маловпливові фактори [5].

Проходження військової служби за контрактом у ЗС України є комплексною та багатовимірною категорією. Для забезпечення раціонального оцінювання необхідно формалізувати відповідну функціональну залежність, яка ґрунтується на найбільш значущих показниках із різною спрямованістю та інтенсивністю впливу, що, у свою чергу, забезпечує комплексність та точність оцінювання.

Утримання військовослужбовців на службі, а також їх професійний розвиток безпосередньо залежать від ефективності функціонування елементів системи проходження військової служби за контрактом — починаючи з моменту підписання контракту і протягом усього терміну перебування у Збройних Силах України.

До ключових показників успішного проходження військової служби за контрактом доцільно віднести ті, що відображають вплив внутрішніх факторів і результати діяльності органів військового управління з персоналу, спрямованих на розвиток і збереження людського капіталу. Основними складовими проходження служби виступають: кар'єрне зростання, підготовка та мотивація [7].

Узагальнений показник ефективності проходження військової служби має відображати інтегральний результат взаємодії вказаних складових, що дає змогу здійснювати об'єктивне оцінювання цього процесу [5].

У якості узагальненого показника доцільно обрати безрозмірну величину — **рівень проходження військової служби** $W_{\text{К}}(t)$, яка характеризує успішність проходження військової служби за контрактом у Збройних Силах України на дискретний момент часу t. Цьому показнику привласнюються описані вище характеристики.

Узагальнений показник — рівень проходження військової служби в ЗС України (далі — *рівень проходження служби*) $W_{\text{К}}(t)$ — залежить від таких чинників, як рівень кар'єрного зростання, рівень підготовки та рівень мотивації. З огляду на ймовірнісну природу досліджуваних процесів, значення показника приймається в межах від 0 до 1, що можна записати у вигляді [7]:

$$0 < W_{\text{К}}(t) \leq 1, \tag{1}$$

Цільова функція рівня проходження військової служби визначається наступним чином [8]:

$$W_{\text{К}}(t) = f_{\text{К}}\{Q_{\text{З}}(t); Q_{\text{П}}(t); Q_{\text{М}}(t)\}, \tag{2}$$

де $Q_{З}(t)$ – показник “рівень кар’єрного зростання” на дискретний момент часу;
$Q_{П}(t)$ – показники “рівень оволодіння певною військово-обліковою спеціальністю” на дискретний момент часу;
$Q_{М}(t)$ – показники “рівень мотивації”, на дискретний момент часу.

Кожен із зазначених показників є агрегованим, тобто формується на основі сукупності показників нижчого рівня ієрархії, які розкривають їх зміст та визначають відповідний рівень у безрозмірному форматі.

Кар’єрне зростання реалізується шляхом просування по службі, укладання контракту тощо. Фізичний зміст показника $Q_{З}(t)$ може бути представлений як функціональна залежність такого вигляду:

$$Q_{З}(t) = f_{З}\{P_{ПЗ}(t); P_{УК}(t)\}, \quad (3)$$

де $P_{ПЗ}(t)$ – показник “рівень ймовірності просування по службі” на дискретний момент t;
$P_{УК}(t)$ – показник “рівень ймовірності укладання контракту” на дискретний момент t.

Показник $P_{ПЗ}(t)$формується на основі ймовірностей нижчого порядку, таких як:
ймовірність направлення на підготовку (перепідготовку);
ймовірність присвоєння чергового військового звання;
ймовірність переміщення на посаду з меншим обсягом обов’язків.

Ці ймовірності визначаються на основі перехідних ймовірностей у межах графа переходів станів об’єктів системи комплектування ЗС України військовослужбовцями за контрактом (рис. 1), із застосуванням математичної моделі марковських процесів без поповнення станів для неоднорідного марковського ланцюга з дискретним часом [5].

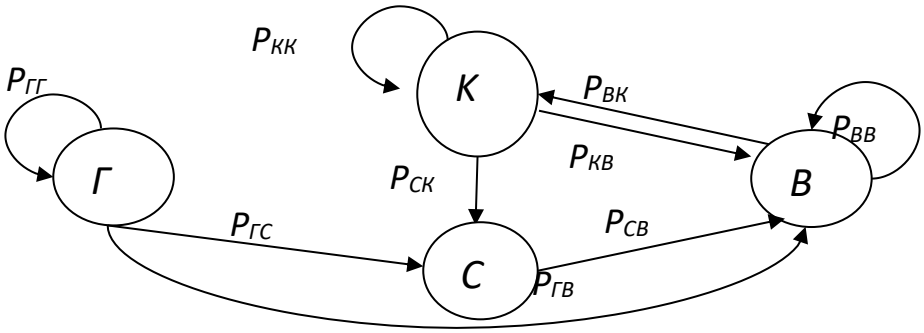


Рисунок 1 – Граф переходу станів об’єктів системи комплектування збройних сил військовослужбовцями військової служби за контрактом

Перехідні ймовірності марківського ланцюгу між станами будуть залежати від: особистих якостей військовослужбовця; медичного обстеження; професійно-психологічного відбору; спеціальної перевірки; направлення військовослужбовця на навчання; фізичної підготовки; лідерських якостей.

Враховуючи категорії військовослужбовців сержантського та старшинського складу ЗС України, слід поділити на (рис. 1) наступні стани [3]:

(Г) – перебуває в початковому стані (виконує обов’язки за певним ВОС);

(С) – направлений на підготовку (перепідготовку) з метою присвоєння чергового військового звання та призначення на відповідну посаду;

(В) – призначення на відповідну посаду;

(К) – переміщений на нижчу посаду.

Показник “рівень ймовірності укладання контракту” $P_{\text{УК}}(t)$ залежить від ймовірностей показників нижчих за ієрархію “рівень ймовірності довготривалого контракту, що забезпечує кар’єрне зростання”, “рівень ймовірності укладання контракту терміном до 5 років”, “рівень ймовірності укладання контракту терміном від 5 до 10 років” та “рівень ймовірності відмови продовжувати контракт”, що визначається перехідними ймовірностями до графу переходів станів об’єктів системи комплектування ЗС військовослужбовцями військової служби за контрактом (рис. 2) з використанням математичної моделі марковських процесів без поповнення станів неоднорідного марковського ланцюга з дискретним часом [3].

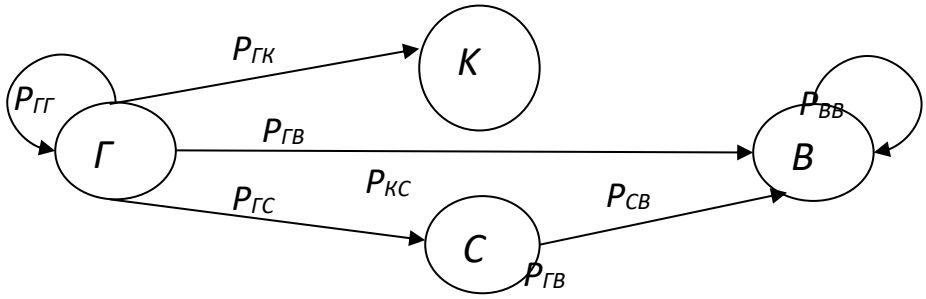


Рисунок 2 – Граф переходу станів об’єктів системи комплектування збройних сил військовослужбовцями військової служби за контрактом

Перехідні ймовірності марківського ланцюгу між станами буде залежати від термінів укладання контракту визначених законодавством та підзаконними актами.

Враховуючи визначені терміни укладання контрактів в ЗС України, слід поділити на наступні стани (рис. 2) [3]:

(Г) – рівень ймовірності укладання контракту терміном до 5 років;

(С) – рівень ймовірності укладання контракту терміном від 5 до 10 років;

(В) – рівень ймовірності довготривалого контракту, що забезпечує *max* кар’єрне зростання;

(К) – рівень ймовірності відмови продовжувати контракт.

Рівень оволодіння певною військово-обліковою спеціальністю залежить від рівня успішності навчання підчас підготовки, (перепідготовки) на курсах лідерства визначених обов’язковими для просування по службі, набутого досвіду за час проходження служби:

$$Q_{\text{П}}(t) = f_{\text{П}}\{P_{\text{У}}(t); P_{\text{Д}}(t)\}, \quad (4)$$

де $P_{\text{У}}(t)$ – показник “рівень успішності навчання” на дискретний момент часу;
$P_{\text{Д}}(t)$ – показник “рівень набутого досвіду” на дискретний момент часу.

Фізичний зміст показника “рівень мотивації” $Q_{\text{М}}(t)$ характеризується матеріальною та нематеріальної мотиваціями. Тоді функціональна залежність матиме наступний вигляд [9]:

$$Q_{\text{М}}(t) = f_{\text{М}}\{P_{\text{М}}(t); P_{\text{Н}}(t)\}, \quad (5)$$

де $P_{\text{М}}(t)$ – показник “рівень матеріальної мотивації” на дискретний момент часу;
$P_{\text{Н}}(t)$ – показник “рівень нематеріальної мотивації” на дискретний момент часу.

Узагальнена система показників, яка пропонується використовувати для оцінювання рівня проходження військової служби за контрактом осіб сержантського і старшинського складу ЗС України наведена на рис. 3.

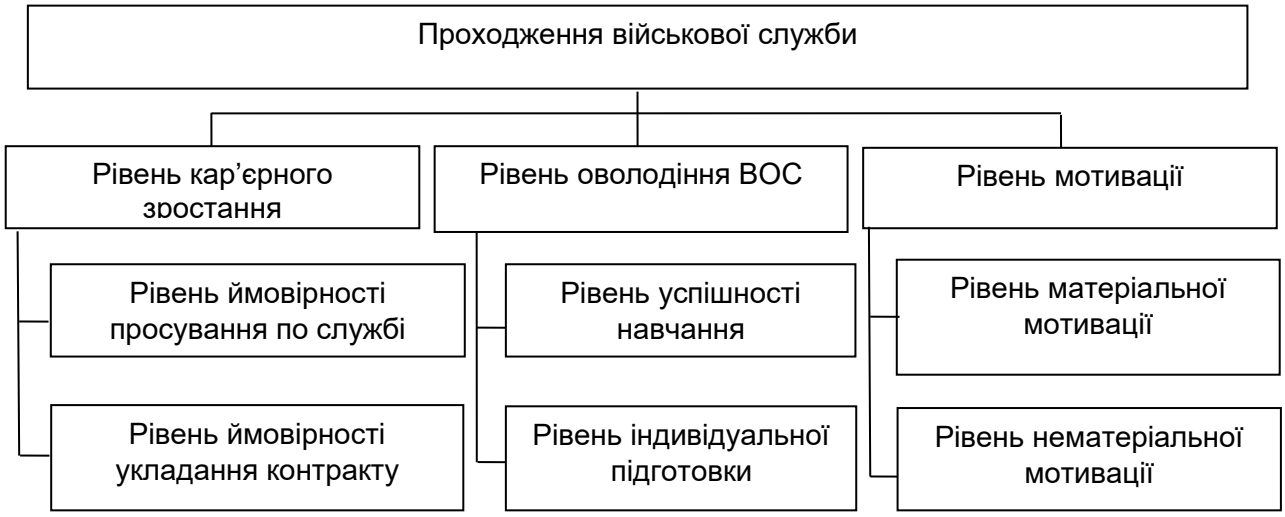


Рисунок 3 – Система показників оцінювання рівня проходження військової служби за контрактом у ЗС України

Для визначення критерію рівня проходження військової служби за контрактом ЗС України $W_K(t)$ пропонується використати універсальну шкалу Харінгтона, у відповідності до якої, кожній якісній оцінці відповідає кількісна величина у межах успішного проходження військової служби або неуспішного проходження військової служби [9].

Для переведення отриманої кількісної оцінки $W_K(t)$ в якісну, пропонується використати шкалу яка наведена у табл. 1.

Таблиця 1 – Шкала переведення кількісних оцінок $W_K(t)$ в якісні

Кількістна оцінка		Відповідність критерію	Якісна оцінка
Min	max		
0,8	1	0,8≤	Успішне проходження
0,37	0,8	≥ 0,37 - 0,8 <	Опосередковане проходження
0	0,37	< 0,37	Неуспішне проходження

Таким чином критерієм рівня проходження військової служби за контрактом у ЗС України $W_K(t)$, який буде характеризувати успішність проходження, будемо рахувати величину $W_K(t) \geq 0{,}8$, яка відповідає оцінці УСПІШНЕ ПРОХОДЖЕННЯ.

Висновки

У статті, на підставі проведеного системного аналізу процесу проходження військової служби за контрактом у Збройних Силах України з урахуванням змін у системі кадрового менеджменту та чинників, що впливають на проходження служби за військовими званнями, було подальше розвинено підхід до формування нової сукупності оцінювальних показників. Вперше обґрунтовано комплексну систему показників, яка, на відміну від наявних, враховує рівень кар'єрного зростання, рівень оволодіння військово-обліковою спеціальністю та рівень мотивації, і базується на синергетичному ефекті, що виникає в результаті їх взаємодії.

Отримані результати можуть бути використані під час розроблення методики оцінювання проходження військової служби за контрактом у Збройних Силах України, а також у межах подальших досліджень у цьому науковому напрямі.

Перспективним напрямом подальших наукових досліджень є обґрунтування практичних рекомендацій щодо удосконалення порядку проходження військової служби за військовими званнями.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Стратегія залучення, розвитку та утримання людського капіталу в силах оборони України на період до 2027 року: за станом на 02 вер. 2024 р. / Міністерство оборони України. – Офіц. вид. – К.: МОУ. вид-во, 2024. – 49 с. (Нормативний документ Міністерства оборони України. Концепція).
2. Концепція військової кадрової політики Міністерства оборони України на період до 2028 року: за станом на 27 жов. 2023 р./ Міністерство оборони України. – Офіц. вид. – К.: МОУ. вид-во, 2023. – 61 с. (Нормативний документ Міністерства оборони України. Концепція).
3. Положення про підготовку і проведення призову громадян України на строкову військову службу та прийняття призовників на військову службу за контрактом: за станом на 20 січ. 2021 р./ Кабінет Міністрів України. – Офіц. вид. – К.: Каб. Мін. вид-во, 2021. – 14 с.
4. Математичні основи кадрового менеджменту у військовій сфері / [Романченко І. С., Гусак Ю. А., Сиротенко А. М., Шуляк П. І., Данилюк С. Л., Бобрун О. В., Пасічник В. М.] ; під ред. І. С. Романченко. – [1-е вид.]. – К. : ЦНДІ ЗС України, 2019. – 243 с.
5. Основи теорії досліджень ефективності системи кадрового менеджменту у військовій сфері / [Безуглий В.М., Вінокуров Д.В., Георгадзе О. А, та ін] ; під ред. Г.М. Тіхонов. – [1-е вид.]. – К. : НУОУ, 2024. – 136 с.
6. Загорка О. М., Мосов С. П., Стужук П. І. Елементи дослідження систем військового призначення / Загорка О. М. – Київ: НУОУ, 2005. – 100 с.
7. Управління персоналом у Збройних Силах України / [Тіхонов Г. М., Боднар О. В., Думенко М. П., і др.] : під. ред. Ю. А. Гусак. – [1-ше вид.]. – К. : НУОУ, 2022. – 132 с.
8. Сааті Т. Л. Принятие решений при зависимостях и обратных связях : Аналитические сети. 2008. 360с.
9. Матвієнко В. Я. Прогностика / Матвієнко В. Я. – Київ: Припринти, 2000. – 520 с.
10. Харрингтон Д. Управление качеством в американских корпорациях / науч. ред. Л.А. Конарева ; пер. с англ. Москва : Экономика, 1990. 272 с.

References

1. Strategy for attracting, developing and retaining human capital in the Defense Forces of Ukraine for the period until 2027: as of Spt. 02. 2024 / Ministry of Defense of Ukraine. – Officer. kind. – Kyiv: MOU. edition, 2024. 49 p. (Normative document of the Ministry of Defense of Ukraine. Concept).

2. Concept of the military personnel policy of the Ministry of Defense of Ukraine for the period until 2028: as of Oct. 27. 2023 / Ministry of Defense of Ukraine. – Officer. kind. – Kyiv: MOU. edition, 2023. 61 p. (Normative document of the Ministry of Defense of Ukraine. Concept).
3. Regulations on the preparation and conduct of conscription of citizens of Ukraine for military service and the acceptance of conscripts for military service under a contract: as of Jan. 20. 2021 / Cabinet of Ministers of Ukraine. – Officer. kind. – Kyiv: CMU. edition, 2021. 14p.
4. Mathematical foundations of personnel management in the military sphere / [Romanchenko I. S., Husak Yu. A., Syrotenko A. M. and others]: sub. ed. Romanchenko I. S. – [1st ed.]. – Kyiv: CSRI, 2019. 243 p.
5. Mathematical foundations of personnel management in the military sphere / [Bezyhlyi V. M., Husak Yu. A., Syrotenko A. M. and others]: sub. ed. Tikhonov G. – [1st ed.]. – Kyiv: NDUU, 2024. 136p.
8. Zagorka O., Mosov S., Stuzhuk P. Elements of research of military purpose systems / Zagorka O. M. – Kyiv: NDUU, 2005. – 100 p.
7. Personnel management in the Armed Forces of Ukraine / [Tikhonov G.M., Bodnar O.V., Dumenko M.P., and others]: sub. ed. Yu. A. Husak. – [1st ed.]. – Kyiv: NDUU, 2022. 132 p.
8. Thomas L. Saaty. Decision Making with Dependence and Feedback: The Analytic Network Process / Thomas L. Saaty. – Pittsburgh: RWS Publications, 1996.
9. Matvienko V. Ya. Prognostics / Matvienko V. Ya. – Kyiv: Priprints, 2000. – 520 c..
10. Harrington D. Quality management in American corporations / Harrington D. Economy, 1990. – 272 s.

Дотичність ризиків та загроз реалізації (військової) кадрової політики України та держави Ізраїль щодо (військової) підготовки громадян

The Relativeness of Risks and Threats to Implementation of the (Military) Personnel Policy of Ukraine and the State of Israel Citizens in Terms of (Military) Training

Андрій Бєлік
старший офіцер відділу планування спроможностей управління планування спроможностей, e-mail: tieua@ukr.net, ORCID: 0009-0003-4648-5795

Andrii Byelik
Senior Officer of the Capability Planning Department, e-mail: tieua@ukr.net, ORCID: 0009-0003-4648-5795

Головне управління оборонного планування Генерального штабу Збройних Сил України, м. Київ, Україна

Main Defense Planning Directorate of the General Staff of the Armed Forces of Ukraine, Kyiv, Ukraine

Received: April 11, 2025 | Revised: April 23, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.9

Мета роботи: здійснення ґрунтовного аналізу чинної нормативно-правової бази у сфері військової підготовки громадян України, а також визначення ключових викликів, ризиків і загроз, що ускладнюють впровадження ефективної кадрової політики у військовій сфері загалом та формування результативної системи військової підготовки громадян України зокрема. На основі отриманих результатів дослідження передбачається обґрунтувати шляхи подолання виявлених проблем та надати науково обґрунтовані рекомендації щодо розвитку ефективної та стійкої системи військової підготовки громадян України.

Метод дослідження: абстрагування, порівняння та кількісно-якісний аналіз, синтез.

Результати дослідження: Результати проведеного дослідження сприяють поглибленню наукового розуміння підходів до формування та впровадження військової кадрової політики. Вони дозволяють зацікавленим сторонам підвищити рівень обізнаності щодо предметної області дослідження, ідентифікувати наявні проблеми та проблемні ситуації, виявити слабкі місця чинної нормативно-правової бази, а також окреслити прогалини у відповідних необхідних спроможностях. Отримані результати можуть бути використані для підвищення ефективності та результативності управлінського впливу суб'єктів управління на функціонування об'єкта і предмета дослідження, що розглядається у цій статті.

Теоретична цінність дослідження: полягає у здійсненні порівняльного аналізу кадрової політики у військовій сфері України та Ізраїлю, що дозволяє виявити спільні та відмінні риси їх змістового наповнення й механізмів реалізації, а також окреслити ризики, пов'язані з їх впровадженням. Урахування соціокультурних чинників та актуальних безпекових реалій сучасності доповнює наявні теоретичні підходи до військової підготовки, сприяє переосмисленню безпекового середовища та наближенню процесів ухвалення рішень у сфері розвитку людського капіталу до науково обґрунтованих методів.

Практична цінність дослідження: полягає в можливості практичного використання отриманих результатів для розроблення рекомендацій щодо підвищення ефективності системи військової підготовки громадян України. Зокрема, це може бути досягнуто шляхом адаптації успішних практик Держави Ізраїль з урахуванням національного контексту та потреб сектору безпеки і оборони. Результати дослідження можуть бути використані як науково-обґрунтована основа для формування державної політики у сфері військової підготовки, спрямованої на зміцнення обороноздатності держави.

Тип статті: теоретична.

Purpose: is to conduct a comprehensive analysis of the current regulatory and legal framework governing military training of Ukrainian citizens, as well as to identify key challenges, risks, and threats that hinder the implementation of an effective personnel policy in the military sphere in general, and the development of an efficient system of military training for Ukrainian citizens in particular. Based on the results of the analysis, the study seeks to outline ways to resolve the identified issues and to provide scientifically grounded recommendations for the development of an effective and resilient system of military training for Ukrainian citizens.

Method: abstraction, comparison and quantitative-qualitative analysis, synthesis.

Findings: The results of the study conducted contribute to a deeper scientific understanding of approaches to the development and implementation of military personnel policy. They enable stakeholders to increase their awareness of the research subject, identify existing problems and critical issues, reveal weaknesses in the current regulatory framework, and highlight capability gaps in relevant areas. The findings can be used to enhance the effectiveness and efficiency of managerial influence exerted by governing entities on the functioning of the object and subject under investigation in this article.

Theoretical implications: The theoretical value of this study lies in the comparative analysis of military personnel policy in Ukraine and Israel, which makes it possible to identify their common features and differences, as well as to highlight the risks associated with their implementation. By taking into account socio-cultural factors and the current security realities, the research complements existing theories of military training, contributes to a reassessment of the security environment, and brings decision-making processes in the field of human capital development closer to scientifically grounded methods.

Practical implications: lies in the potential application of its findings for developing practical recommendations aimed at enhancing the effectiveness of the military training system for Ukrainian citizens. This may be achieved, in particular, through the adaptation of successful practices from the State of Israel, taking into account the national context and the specific needs of the security and defense sector. The study's results may serve as a scientifically grounded foundation for shaping state policy in the field of military training, aimed at strengthening the country's defense capabilities.

Type of article: theoretical.

Ключові слова: Україна-Ізраїль, аналіз ризиків, військова кадрова політика, людський капітал, міжнародна співпраця, принципи соціальної безпеки, загальновійськова підготовка.

Key words: Ukraine-Israel, risk analysis, military conflict, military personnel policy, human capital, international cooperation, social security principles, general military training.

Вступ

В умовах необхідності трансформації форм і способів застосування Збройних Сил та інших складових сил оборони [1], особливої актуальності набуває проблема ефективності освітньо-підготовчої діяльності інституцій та громадян України, а також розвитку ефективної, результативної, гнучкої, прозорої системи (військової) підготовки громадян України, що може забезпечуватись підсистемним комплексом у складі моделей, програм тощо.

Теоретичні основи дослідження

Питання військової підготовки військовослужбовців вивчали такі науковці, як М. Банько, В. Безуглий, О. Георгадзе, В. Гриньков, І. Грязнов, Д. Винокуров, А. Деркач, А. Зельницький, Є. Камалов, В. Клачко, С. Козін, В. Кортенко, С. Кубіцький, А. Лігоцький, Ю. Приходько, І. Радванський, В. Райко, Л. Рудкевич, А. Руднєвська, І. Руснак, Ю. Сердюк, А. Сіцінський, Г. Тіхонов, Т. Ткаченко, В. Телелим, В. Харабара, О. Хміляр та інші.

Проблемами формування готовності майбутніх офіцерів до професійної діяльності переймалися: А. Балендр, С. Кубіцький, І. Платонов, А. Сіцінський, О. Старчук, В. Уліч та інші.

Постановка проблеми

Орієнтуючись на визначений Конституцією України вектор розвитку Сил оборони, необхідно постійно забезпечувати трансформацію форм, методів і змістовного наповнення підготовки військ (сил). Цей процес має перебувати в полі постійної уваги профільних інституцій і бути спрямованим на формування та розвиток необхідних, передусім критичних, спроможностей [2]. У цьому контексті важливого значення набуває системна адаптація існуючих підходів до сучасних вимог, а також впровадження найбільш ефективних моделей військової підготовки громадян України.

Зважаючи на те, що на сьогодні механізми функціонування базової військової служби та окремі елементи системи військової підготовки перебувають на етапі формування, у даній статті здійснено спробу ідентифікації актуальних ризиків реалізації кадрової політики у сфері оборони. Їх врахування дозволяє сформулювати обґрунтовані пропозиції щодо впровадження ефективних моделей інституалізованої військової підготовки громадян України (далі – МІВіПГ) у загальну систему військової підготовки громадян України (далі – СВПГУ).

Метою статті є аналіз чинної структури нормативно-правової бази, що регламентує процес військової підготовки громадян України, з подальшим визначенням ключових викликів, ризиків і загроз, які супроводжують запровадження ефективної військової кадрової політики загалом, а також функціонування СВПГУ зокрема. На основі результатів аналізу запропоновано можливі шляхи розв’язання виявлених проблемних аспектів та сформульовано практичні рекомендації щодо розвитку високорезультативної системи військової підготовки громадян України.

Методологія дослідження

Дослідження ґрунтується на системному підході до аналізу чинної структури нормативно-правового забезпечення процесу військової підготовки громадян України. У процесі наукового дослідження застосовано такі методи:

- **системний аналіз** — з метою виявлення та класифікації структурних елементів системи військової підготовки громадян України;
- **порівняльний аналіз** — для оцінювання відповідності чинних механізмів військової підготовки громадян України сучасним вимогам оборонної політики;
- **метод аналогій** — для адаптації позитивного досвіду Держави Ізраїль у контексті вдосконалення національної системи військової підготовки.

Комплексне застосування зазначених методів забезпечило всебічне та об’єктивне уявлення про поточний стан системи військової підготовки громадян України, дало змогу ідентифікувати її ключові проблеми, а також окреслити перспективні напрями її подальшої трансформації.

Результати

Виконання плану пріоритетних дій Уряду на 2023 рік [3] зумовило затвердження Концепції військової кадрової політики в системі Міністерства оборони України на період до 2028 року [4]. Ця концепція, як система поглядів, визначає головну мету військової кадрової політики – створення умов для гарантованого та якісного комплектування Збройних Сил України підготовленим і вмотивованим особовим складом, здатним виконувати завдання за призначенням, та його ефективне використання.

Підґрунтям поточної кадрової політики стало підписання Указу Президента України [5], яким Кабінету Міністрів України було доручено (серед іншого) запровадження моделі інтенсивної системи військової підготовки як альтернативної форми проходження строкової служби.

У 2024 році Міністром оборони України було затверджено “Політику залучення, розвитку та утримання людського капіталу в силах оборони” (далі – Політика), спрямовану на створення комплексної системи, що охоплює формування оборонної свідомості, реформу соціальної сфери та ветеранської політики, а також якісні зміни грошового забезпечення та оновлення системи охорони здоров’я. Пункт 2.4.5 Політики визначає інтенсивну військову підготовку громадян призовного віку, наголошуючи на необхідності розроблення та впровадження принципово нової системи організації та проведення інтенсивної військової підготовки цивільної молоді.

Передбачається, що підготовка включатиме базову загальновійськову підготовку та фахову підготовку для отримання військово-облікової спеціальності, зокрема шляхом інтеграції до навчальних планів закладів вищої освіти всіх форм власності як окремої навчальної дисципліни. Загальний термін інтенсивної військової підготовки не перевищуватиме п’яти місяців, передбачатиметься можливість проходження відповідної підготовки для осіб, старших 25 років. У подальшому підтримання рівня та набуття нових фахових компетенцій відбуватиметься під час обов’язкових періодичних навчальних зборів.

Законом України від 11.04.2024 № 3633-IX “Про внесення змін до деяких законодавчих актів України щодо окремих питань проходження військової служби, мобілізації та військового обліку” [6] внесено зміни до низки нормативно-правових актів, зокрема до Закону України “Про військовий обов’язок і військову службу” [7], де було сформульовано нове поняття “базова військова служба”.

Враховуючи, що запланована розробка моделей інтенсивної системи військової підготовки громадян України досі не реалізована, а актуальність питання зростає, з метою вивчення наявної інформації, систематизації даних та надання висновків, на початковому етапі розробки моделей інтенсивної військової підготовки і професійної орієнтації (МІВіПО) у СВПГУ пропонується залучити показники Держави Ізраїль з відкритих джерел для порівняльного аналізу кадрової політики. Ізраїль де-факто перебуває у стані нелінійної війни та має успішний практичний досвід військової підготовки громадян.

Попри відмінності генезису та історичного розвитку суспільно-економічних формацій України та Ізраїлю, існують схожості, які в умовах кратної переваги потенціалів реальних противників цих держав, зумовлені не лише пошуком сталих зовнішніх політико-економічних зв’язків із провідними економіками світу для посилення обороноздатності, а й необхідністю досягнення балансу інтересів основних об'єктів національної безпеки: громадянина, суспільства та держави.

Військова кадрова політика в Україні та Ізраїлі має особливості, зумовлені різними геополітичними, соціальними та економічними контекстами. Однак, існують спільні ризики, що можуть бути релевантними для обох держав, а також специфічні ризики для кожної з них. На нашу думку, для подальшого якісного формування та реалізації військової кадрової політики України, варто врахувати деякі аспекти досвіду Ізраїлю. У Державі Ізраїль допризовна військова підготовка є важливою складовою системи національної безпеки та включає такі ключові аспекти:

1. Обов'язковий призов: усі громадяни (за незначними винятками) проходять військову службу після досягнення 18 років. Чоловіки служать три роки, жінки – два.
2. Підготовка у школах: в Ізраїлі військова підготовка починається у закладах середньої освіти. Учні отримують базові знання про військову справу, тактику, безпеку та національну ідентичність.
3. Програма "Махаль" [8]: програма для іноземних добровольців, що дозволяє молодим людям з-за кордону проходити військову службу в ізраїльських збройних силах.
4. Військова підготовка в молодіжних організаціях: існують різні молодіжні програми, що фокусуються на розвитку лідерських якостей, фізичної підготовки та патріотизму.
5. Курси та табори: організація літніх таборів та курсів, що спеціалізуються на військовій підготовці, де молодь може отримати навички, необхідні під час служби.
6. Підготовка до призову: перед призовом молоді люди проходять медичні огляди та тестування для визначення їхніх здібностей та найбільш підходящих ролей у війську.
7. Система підготовки резервістів: після закінчення регулярної служби громадяни стають резервістами та продовжують проходити навчання та тренування на регулярній основі.

Ця система підготовки сприяє формуванню патріотичних цінностей та готовності до захисту держави серед молоді.

В Ізраїлі значні зусилля та ресурси спрямовуються на модель підготовки в школах, яка включає такі ключові елементи:

1. Військово-патріотичне виховання: курси та лекції, на яких учні поглиблено вивчають історію Ізраїлю, основи національної безпеки та роль армії в суспільстві; патріотичні заходи, присвячені пам'яті полеглих героїв, національні свята та військові паради.
2. Фізична підготовка: програми фізичної підготовки, що включають види спорту із специфічною спрямованістю, такі як рукопашний бій, біг із перешкодами тощо; елементи тактичних ігор, що входять до програми занять з фізкультури, сприяють розвитку командної єдності.
3. Військово-спеціальні знання: учні можуть отримувати базові знання й уміння з основ військової справи, такі як перша медична допомога, орієнтування на місцевості, симуляційні навчання зі стрільби, а також застосування різних видів військового обладнання; залучення військовослужбовців ЦАХАЛ до проведення навчальних занять, що дозволяє учням шкіл отримувати знання через безпосередню комунікацію.
4. Лідерські якості та командна робота: організація групових проєктів, що вимагають спільної роботи, сприяє розвитку лідерських навичок і вміння працювати в команді; проведення змагань між класами та школами, що допомагають учням відточувати навички та вдосконалювати взаємодію.
5. Соціальна відповідальність: заохочення участі учнів у волонтерських заходах, пов'язаних із соціальною відповідальністю, таких як допомога ветеранам або участь у громадських проєктах.
6. Психологічна підготовка: вивчення технік, які допомагають молоді знімати стрес, розвивати психологічну стійкість і навички прийняття рішень у складних ситуаціях.

Синергія цих елементів підготовки у школах Ізраїлю сприяє всебічному розвитку молоді, формуючи підготовлених та відповідальних громадян, готових до служби та захисту держави.

Обмеженість обсягом статті не дозволяє всебічно охопити тонкощі та взаємозв'язки багатоаспектної кадрової політики щодо підготовки громадян, а також представити всі можливі погляди на дотичність ризиків реалізації кадрової політики у контексті обох держав. Проте, спробуємо виокремити ключові ризики та загрози.

А. Спільні ризики та загрози формуванню та реалізації військової кадрової політики України та Держави Ізраїль:

А.1. Недостатня адаптація до сучасних викликів.

Сучасний світ характеризується суперечливими станами: емерджентною складністю, епістемологічною невизначеністю, інформаційним перевантаженням [9], що супроводжуються іронією метамодерну. В умовах абстрактних категорій та споконвічних конфліктів діалектики розвитку, людина потребує стійких орієнтирів.

У зв'язку з "відтоком мізків", іншими турбулентними процесами та негативними явищами системного характеру, може відбуватися поступова когнітивна рефлексія щодо кумулятивності знань та некумулятивності етики.

Для успішної адаптації до сучасних викликів та забезпечення конкурентоспроможності необхідно ґрунтуватися на єдиній мові концептуальних основ, запропонованих класичними філософами Заходу (зокрема, Георгом Вільгельмом Фрідріхом Гегелем у "Феноменології духу") [10], що може слугувати базою для глибинної трансформації кадрової політики через інтеграційну єдність із традицією західної методології.

Крім того, нормативно-правова база може не встигати за змінами безпекового середовища, що призводить до неефективного планування та розвитку спроможностей складових сектору безпеки та оборони.

А.2. Нестача кваліфікованих кадрів.

Ізраїль має усталені військові традиції та норми права, проте це не убезпечує від проблем оптимізації чисельності та підготовки військових і суміжних спеціальностей у відповідності до нових технологічних викликів та загроз. В Україні, у зв'язку з багаторазовим продовженням строку дії воєнного стану [11], скасуванням у поточному році строкової служби [5], але за відсутності усталених норм та механізмів запровадження моделей військової підготовки громадян, виникають проблеми з реалізацією військового обов'язку (підготовкою, прийняттям, призовом, проходженням служби громадянами, дотриманням правил військового обліку) [7] та утриманням кваліфікованих кадрів.

А.3. Вплив внутрішньополітичних факторів.

Вимушена політична стабільність, зокрема у сенсі можливостей унормування незмінності вищого військово-політичного керівництва під час дії правового режиму воєнного стану, дозволяє зберігати сталість та поступовість стратегічного вектору розвитку, але може призводити до недостатньої відкритості до важливих та термінових реформ. Несприятлива політична кон'юнктура може призводити до призначення на ключові позиції некомпетентних осіб та інших провалів у критичних спроможностях [2].

А.4. Недостатня міжвідомча координація.

Керівні документи не завжди забезпечують оперативність та належну координацію між різними військовими та цивільними підприємствами, установами і організаціями, що може призводити до дублювання повноважень/функцій та перевитрат ресурсів.

А.5. Висока залежність від мобілізаційного ресурсу.

Залежність від мобілізації призовників, військовозобов'язаних та резервістів є ризиком для ефективності військової підготовки та системи комплектування, у разі недостатності рівня підготовки, накопичення військово-навчених людських ресурсів для комплектування посад,

передбачених штатами воєнного часу, а також недодержання інших принципів і змісту мобілізаційної підготовки [12, стаття 3].

А.6. Інформаційні ризики України та Ізраїлю у контексті кадрової (військової) політики:

Інформаційні ризики у контексті кадрової (військової) політики обох держав можна розглядати з кількох ключових аспектів:

- вибіркове використання історичних явищ і подій як політичного ресурсу для легітимації та укорінення гіпертрофованих форм авторитаризму;
- ворожа дезінформація та пропаганда, за умови недостатньої скоординованості та результативності власного інформаційного впливу, може негативно позначатися на рівнях морально-психологічної підготовки, міжнародної підтримки і навіть поляризації суспільств [13];
- невідповідність у системах збору та аналізу інформації може призводити до невиправданих кадрових рішень, як-то недооцінка або переоцінка потенціалів і спроможностей певних інституцій та спеціалістів;
- зростання питомої ваги соціальних медіа, що разом зі збільшенням кількості каналів і квазіекспертних думок, здатне викривляти та примітивізувати проблематику, а також розпорошувати увагу і ускладнювати можливість консолідації навколо термінового та важливого;
- застосування штучного інтелекту та когнітивних технологій у деструктивних цілях;
- кібернапади на державні (військові) об’єкти можуть призводити до витоку таємної та чутливої інформації, а також ушкодження і втрати ресурсів;
- безпідставна приватизація чи засекречування суспільно необхідної інформації, яка має бути загальнодоступною та слугувати суспільним інтересам і державі;
- надмірна цифровізація, що призводить до приросту таких явищ як “цифровий аутизм”, “цифрове слабоумство” тощо.

З метою протистояння ризикам та загрозам у сфері інформації (як першооснови існування людини, суспільства та держави), органи державної влади спільно із регуляторами у сфері медіа, за сприяння соціогуманітаріїв наукових кіл, фахівців сил спеціальних операцій, за підтримки громадянського суспільства мають невпинно виробляти та запроваджувати високорезультативну політику щодо формування національної “думкоформи безпеки” та вдосконалювати шляхи протидії неприйнятним ідеологіям.

Спільні ризики реалізації військової кадрової політики України та Ізраїлю вказують на необхідність її постійного моніторингу та адаптації, а також на важливість міжвідомчої взаємодії для оперативного врахування сучасних викликів і загроз у сфері безпеки та оборони.

Б. Істотні відмінності щодо викликів, ризиків та загроз формуванню та реалізації військової кадрової політики України та Держави Ізраїль:

Б.1. Фінансування та ресурси.

За показником ВВП, економіка Ізраїлю більша ніж економіка України (509,9 млрд. дол. США проти 178,8 млрд. дол. США відповідно) [14], і Ізраїль витрачає більший відсоток державного бюджету на сектор безпеки та оборони. У перерахунку на душу населення це демонструє значно більший потенціал спроможностей економіки Ізраїлю у порівнянні з Україною, зокрема щодо забезпечення сучасними технологіями у процесі військової підготовки.

Дані з офіційних джерел щодо макроекономічних показників України свідчать про наступне:

- значна частина бюджетної системи формується за рахунок зовнішньої допомоги;
- зростання державного та гарантованого державою боргу, який станом на 30.06.2024 становив 6 168 млрд. грн. [15];

- прогнозовані показники дефіциту державного бюджету у 2024 році на рівні 20,7% ВВП [16];
- прискорення темпів промислової інфляції, що сягнули 33,3% у річному вимірі [17];
- призупинення приросту строкових гривневих депозитів населення [17];
- від'ємне сальдо торговельного балансу, що характеризується значним розривом між експортом та імпортом на рівні історичного максимуму [18].

Зазначені макроекономічні тенденції свідчать про потенційні ризики, пов'язані з фінансуванням програм підготовки громадян. Навіть у разі прямого копіювання ізраїльських моделей, необхідно передбачати значні видатки на адаптацію технологій та інфраструктури. На початковому етапі це може призвести до збільшення навантаження на державний бюджет, погіршення макрофінансових показників, підвищення соціальної напруженості та інших негативних наслідків, зокрема у військовій сфері.

Б.2. Мотивація та соціальна адаптація

Важливим аспектом є мотивація та соціальна адаптація громадян, які залучаються до програм підготовки. На відміну від Ізраїлю, де існує розвинена система соціальної підтримки ветеранів, в Україні, незважаючи на наявність законодавчої бази щодо статусу ветеранів війни та гарантій їх соціального захисту, існують певні виклики. Специфічні соціально-економічні умови, брак усталених традицій шанування захисників та захисниць України, а також неоднозначне ставлення суспільства до соціальних інститутів [19] можуть призводити до проблем з мотивацією та труднощів адаптації ветеранів у таких сферах:

- Реабілітація та реадаптація.
- Соціальні гарантії.
- Житлове забезпечення.
- Соціальна підтримка сімей.
- Професійна підготовка (перепідготовка) та зайнятість [20].

Недостатня прозорість та ефективність механізмів підтримки ветеранів та інших категорій громадян може мати деструктивні наслідки, підриваючи довіру до державних інституцій та знижуючи мотивацію до участі в оборонних програмах.

Б.3. Принципи соціальної безпеки: порівняльний аналіз

Принципи соціальної безпеки, що лежать в основі ізраїльської моделі, можуть бути сформульовані наступним чином [21]:

Б.3.1. **Армія оборони Ізраїлю (ЦАХАЛ):** Обов'язкова служба у регулярному війську та резерві сприяє підтримці високого рівня громадянської єдності.

Б.3.2. **Національний резерв:** Усі громадяни, придатні до військової служби, зобов'язані служити у складі національного резерву.

Б.3.3. **Досягнення та збереження свободи дій:** Свобода є пріоритетною умовою для успішного розв'язання проблем і досягнення цілей, забезпечуючи необхідну гнучкість у використанні інструментів сили.

Б.3.4. **Опора на власні сили:** Цей принцип сприяє усвідомленню меж відповідальності та забезпечує свободу дій.

Б.3.5. **Загальний військовий обов'язок:** Рівність, партнерство та солідарність верств населення у служінні, цінування та вдячність тим, хто служить, а також активна участь більшості громадян у забезпеченні потреб війська є ключовими факторами успіху ізраїльської моделі. ЦАХАЛ має пріоритетне право обирати кандидатів, а соціальні групи, звільнені від військової служби, проходять альтернативну цивільну службу в суспільно важливих організаціях. Ті, хто проходить службу в ЦАХАЛ, отримують значно вищу платню [21].

В Україні принципи соціальної безпеки часто мають декларативний характер. Система соціальної безпеки формується фрагментарно, без системного та комплексного підходу,

недостатнього науково-прикладного обґрунтування та дотримання базових принципів економічно розвинених держав, зокрема ЄС [22, с. 105]. Це створює перешкоди для ефективного впровадження ізраїльської моделі підготовки громадян до оборони та потребує комплексних реформ у сфері соціальної політики та безпеки.

Одним із прикладів непослідовності державної політики у сфері соціального забезпечення є зміни у трудових гарантіях для мобілізованих працівників. Частина 3 статті 119 Кодексу законів про працю України (у попередній редакції) [23] передбачала збереження місця роботи і посади за працівниками, призваними на військову службу під час особливого періоду, незалежно від форми власності підприємства. Виплата заробітної плати мобілізованим здійснювалася за рахунок коштів Державного бюджету України відповідно до Закону України "Про соціальний і правовий захист військовослужбовців та членів їх сімей". Однак, згідно із Законом України від 01.07.2022 №2352-IX "Про внесення змін до деяких законодавчих актів України щодо оптимізації трудових відносин" [24, с. 566], з 19 липня 2022 року збереження середнього заробітку мобілізованим працівникам було скасовано.

Диспропорційність пенсійного забезпечення колишніх військовослужбовців та працівників міліції (поліцейських), що виникла внаслідок прийняття постанови Кабінету Міністрів України від 21 лютого 2018 року № 103 "Про перерахунок пенсій особам, які звільнені з військової служби, та деяким іншим категоріям осіб" [25], також негативно впливає на мотивацію до військової служби. Несвоєчасне виконання статті 63 Закону України № 2262-XII "Про пенсійне забезпечення осіб, звільнених з військової служби, та деяких інших осіб" [26] щодо перерахунку раніше призначених пенсій колишнім військовослужбовцям у відповідності до збільшення розмірів грошового забезпечення діючих військовослужбовців, поглиблює цю проблему [27].

Урядовий портал 31.01.2023 повідомив про новий порядок нарахування грошового забезпечення військовослужбовцям сил безпеки і оборони [28]. Водночас, актуальним залишається питання диференціації розмірів винагороди залежно від місця, умов та особливостей проходження служби.

Непослідовність у реалізації принципів соціальної безпеки ставить під сумнів цілісність системи кадрової політики та викликає недовіру до її засадничих принципів: універсальності, адресності, комплексності, адаптивності, превентивності, професіоналізму та наукової обґрунтованості форм, способів і методів соціальної безпеки держави [29, с. 26].

Роль особистої мотивації та колективної підготовки у забезпеченні соціальної безпеки

Усвідомлення сенсу власної підготовленості є важливим фактором для кожної людини. Цілі та матеріальні складові можуть відрізнятися залежно від обставин та етапу розвитку, але кінцевою метою підготовки є досягнення гомеостазу біологічної та соціальної системи, набуття позитивних якостей та передавання корисної інформації (зокрема генетичної). Люди, як передавачі та приймачі інформації, є взаємозалежними формувачами та відтворювачами принципів соціальної безпеки.

Компетентна людина прагне мати поруч надійних людей з подібним рівнем розвитку. Надійність можна розглядати як синонім компетентності та безпеки, через призму якої люди сприймають сутності у предметах, подіях та явищах. Узагальнений зріз даних щодо рівня колективної підготовки відображає рівень корпоративної культури та є складником загальної картини актуального стану соціальної безпеки держави.

Б.4. Культура сприйняття та виклики в управлінні різноманіттям

Загальнообов'язковий характер військової служби в Державі Ізраїль є визначальною рисою цієї країни та важливим елементом національної ідентичності. Одностайність підходу до військової служби сприяє морально-психологічній підготовці громадян, формує єдність, відповідальність і патріотичну свідомість. У збройних силах Ізраїлю жінки служать разом із

чоловіками, а також існують окремі підрозділи, такі як 33-й батальйон сухопутних військ ЦАХАЛ “Каракаль”, де жінки проходять спеціалізовану підготовку.

В Україні військова служба також набуває особливого значення в контексті національної безпеки, особливо в умовах збройного протистояння. Однак, існують відмінності в підходах до військової служби залежно від регіону та інших факторів. Запозичення іноземних моделей без урахування специфіки українського суспільства може призвести до труднощів у їх реалізації.

Недостатнє врахування аспектів гендерної політики та інклюзії в керівних документах може призвести до дискримінації певних соціальних груп, проблем, пов’язаних із проходженням служби та професійною адаптацією, а також ускладнити процес планування і проведення військової підготовки.

Непослідовність змін у чутливих питаннях військової кадрової політики може викликати негативну реакцію суспільства. Наприклад, непідготовлене суспільство може негативно відреагувати на універсалізацію військового обов’язку, що може призвести до проявів масової непокори [30].

Б.5. Психологічний тягар

Проблеми з підготовкою військ (сил), недостатнє забезпечення озброєнням і військовою технікою, затримки в постачанні [31], а також невдало зміщені акценти психологічної підготовки можуть викликати стрес та підвищувати ризик розвитку психологічних розладів серед українських військовослужбовців. Особливо це стосується випадків, коли програми (моделі) військової підготовки недостатньо адаптовані до їх ментальності та нагальних потреб.

Б.6. Міжнародна підтримка та співпраця

Держава Ізраїль має широкі міжнародні зв'язки та співпрацю у військовій сфері, що позитивно впливає на підготовку кадрів та обмін досвідом. Сполучені Штати Америки є найбільшим союзником Ізраїлю [32, с. 3], надаючи військову допомогу, технології та беручи участь у спільних навчаннях. Ізраїль та Індія розвивають спільні військово-технічні, навчальні та тренувальні проєкти. Ізраїль також входить до Групи I2U2, що об’єднує Індію, Об’єднані Арабські Емірати та США, які співпрацюють у сферах води, енергетики, транспорту, космосу, охорони здоров’я та продовольчої безпеки [33]. Крім того, Ізраїль має військово-політичні зв’язки з європейськими країнами, такими як Великобританія, Німеччина та Франція.

Україна також отримує значну міжнародну підтримку, яку можна поділити на такі складові:

А) Ініціативи НАТО щодо надання допомоги Україні, зокрема:

- Група зі сприяння безпеці та підготовці для України з боку НАТО (NSATU).
- Комплексний пакет допомоги (CAP).
- Дорожня карта взаємосумісності Україна – НАТО.
- Адаптована Річна національна програма Україна – НАТО на 2024 рік.

В) Ініціативи США щодо надання допомоги Україні, зокрема:

- USAID – реалізація проєктів з підтримки економічної стійкості.
- Ukraine Defense Contact Group (UDCG) під проводом США, що включає альянс “Рамштайн” з понад 50 країн, який підтримує оборону України шляхом постачання майна та військової техніки.
- Функціонування в рамках UDCG Коаліцій спроможностей для системного управління військовою допомогою, яка надається країнами-партнерами.
- Міжнародний донорський координаційний центр (IDCC) – координаційний орган, очолюваний Великобританією, через який країни-партнери обмінюються інформацією і синхронізують зусилля щодо надання військової техніки, навчання та допомоги ЗС України.

- Група сприяння безпеці України (SAG-U – Security Assistance Group – Ukraine) (Вісбаден, Німеччина), що забезпечує структурованість ресурсної підтримки в рамках довгострокових зусиль США для тренування і консультування сил оборони України.

С) Донорська допомога, окремі програми та проєкти з міжнародними організаціями та урядами багатьох держав, зокрема: Австралія, Великобританія, Естонія, Казахстан, Латвія, Литва, Марокко, Німеччина, ОАЕ, Пакистан, Південна Корея, Польща, США, Туреччина, Франція, Японія, а також інші азійські, арабські та латиноамериканські країни.

Однак, несприятливі зовнішньополітичні обставини, такі як заяви окремих політиків [34], свідчать про ризики для України щодо погіршення розвитку двосторонніх та багатосторонніх міжнародних відносин. Це може призвести до обмеженого доступу до міжнародних проєктів (програм), фінансової та військово-технічної допомоги, що матиме критичний вплив на систему (військової) підготовки громадян України та розвиток (військової кадрової) політики та спроможностей України в цілому.

Б.7. Політико-економічне протистояння як діалектика розвитку

У політичних процесах України та Ізраїлю спостерігається діалектичне протистояння між “новаторством” і “традиціоналізмом”, що проявляється у боротьбі реформаторських і консервативних сил, виборі політико-економічних шляхів розвитку та пошуку балансу інтересів різних акторів.

У цьому контексті підготовка громадян відіграє важливу роль у формуванні суспільної думки, політичної культури та готовності до змін. Підготовка громадян в Україні та Ізраїлі має свої особливості.

В Ізраїлі акцент робиться на загальній військовій підготовці та єдності перед зовнішніми загрозами, тоді як в Україні основний фокус спрямований на подолання радянської спадщини, побудову технологічної бази та осучаснення політичної культури.

Україна переживає складний історичний період, пов’язаний з пошуком балансу протилежностей, об’єднанням громадянського суспільства та адаптацією програм підготовки громадян до відповідних змін.

Значна частина українського суспільства, з часів розпаду СРСР, за інерцією піддається директивним методам управління, що суперечить активній громадянській позиції тих, хто визнає цінність делегування повноважень і особистої відповідальності.

Громадські організації та органи державного управління здійснюють реформування освітньої системи. У загальноосвітніх школах впроваджено оновлену навчальну програму “Захист України. Рівень стандарту” для 10-11 класів, курс “Громадянська освіта” [35] та інші ініціативи, спрямовані на формування громадянської активності та відповідальності. У перспективі ці напрацювання мають бути трансформовані у програму базової загальної військової підготовки (БЗВП) для осіб від 18 років, з подальшим розширенням набутих спроможностей у загальній системі (військової) підготовки громадян України.

Таким чином, підготовка громадян в обох державах є важливим елементом у боротьбі між модернізацією та консерватизмом, але потребує подолання численних викликів, пов’язаних з історичним контекстом та сучасними загрозами.

Б.8. Конфлікт інституціональних перетворень, інтеграції та взаємосумісності

Реформи у сфері кадрової політики можуть бути ускладнені через необхідність інтеграції новітніх структур і стандартів. Створення нових та реформування існуючих інституцій та доктринальної бази, особливо в умовах продовження дії правового режиму воєнного стану в Україні, може викликати інституціональний конфлікт. Слабке інституціональне середовище не здатне ефективно “прийняти” інститут більш високого рівня організації. Зміна інституційного середовища може зруйнувати необхідний “прошарок” соціально-економічної системи, який забезпечує реалізацію економічного потенціалу та стійкість перед викликами, ризиками та загрозами [36, с. 48, 50].

Окрім вищезазначених ризиків, існують загрози в енергетичній, демографічній, юридичній та онтологічній сферах, що є життєво важливими для громадянина, суспільства та держави, та можуть мати критичний вплив на формування кадрової політики.

Б.9. Енергетика

Ізраїль має власні енергетичні ресурси (наприклад, газові родовища) [37], але геополітична нестабільність у регіоні може загрожувати їх експлуатації та транспортуванню. Високий рівень технологічного розвитку Ізраїлю підвищує ризик кібернападів на його енергетичну інфраструктуру. Обов'язкова військова служба в Ізраїлі може впливати на наявність фахівців в енергетичному секторі.

Україна має значну залежність від імпортованих енергоносіїв, особливо газу, вартість якого зростає [17, с. 5]. Відсутність власної пересувної всепогодної системи протиповітряної оборони на кшталт ізраїльського "Залізного купола" та недостатність засобів ефективного захисту об'єктів критичної інфраструктури, враховуючи велику територію України, призводить до загрози руйнування енергетичної інфраструктури та дефіциту генеруючої потужності. Нестача кваліфікованих кадрів в енергетичному секторі (через мобілізацію, еміграцію тощо) може знизити ефективність роботи енергетичної системи. Збільшення витрат бізнесу на забезпечення "автономними" системами живлення посилює ціновий тиск [17]. Ці фактори негативно впливають на енергетичну безпеку людини, суспільства і держави.

Б.10. Перспективи використання людського капіталу

Під час війни Судного дня у 1973 році в Ізраїлі проживало близько 3,3 млн осіб. Зараз – майже 9,4 млн. З них 74% – євреї [38]. Таким чином, чисельність населення зросла майже втричі.

У 2021 році в Ізраїлі населення зросло на 1,7%, або майже 160 тис. людей. 83% приросту населення забезпечила народжуваність, а решту – репатріація та міграція. Померли близько 51 тис. громадян Ізраїлю, а 7,5 тис. громадян перебували за кордоном більше року [39].

В Україні у 2021 році зафіксовано найнижчу народжуваність за останні 10 років: 271 984 особи, а смертність сягнула 714 263 особи [40].

Дефіцит працівників у національній економіці посилюється, що, при зростанні дефіциту держбюджету, тисне на середній рівень зарплати у бік збільшення.

За оцінкою ООН, станом на 19 серпня 2024 року кількість мігрантів з України у світі сягнула 6,7 млн осіб (з початку 2024 року зросла майже на 400 тис. осіб). Найбільше українських мігрантів у Німеччині (1,1 млн), Польщі (976 тис.) та Чехії (361 тис.) [17, с. 21].

Країни-реципієнти поступово ускладнюють умови перебування українських мігрантів. В Україні дефіцит кадрів, особливо кваліфікованих, залишається значним. Після малочисельного зменшення, яке ймовірно було спричинене зменшенням попиту через зупинки в роботі підприємств унаслідок перебоїв з енергопостачанням, дефіцит кваліфікованих працівників сягнув нового максимуму. За опитуванням центру Разумкова, 60% працюючих (роботодавців, найманих працівників, працюючих співвласників підприємств, самозайнятих) повідомили про дефіцит кадрів на своєму підприємстві [17, с. 22].

З одного боку, економічно активне населення, залучене до суспільного виробництва, забезпечує соціально-економічний розвиток держави. З іншого боку, частина населення, яка перебуває на військовій службі або може бути залучена до поповнення сил оборони, має забезпечувати надійний збройний захист національних інтересів України. Водночас, існують передумови невійськового характеру, що можуть призвести до скорочення чисельності економічно активного населення.

Очікується, що падіння народжуваності в Україні триватиме. Імовірність істотного підвищення рівня народжуваності в перші роки після війни залишається низькою через зруйноване житло та інфраструктуру, політико-економічну нестабільність та інші фактори.

Затяжний характер збройної боротьби, велика кількість загиблих і зниклих безвісти, внутрішньо переміщених осіб, осіб з інвалідністю, а також висока ймовірність неповернення

значної кількості біженців з-за кордону можуть перешкоджати повноцінному компенсаційному ефекту, який зазвичай спостерігається після усунення загроз та подолання наслідків соціальних потрясінь у період постконфліктного врегулювання.

Б.11. Онтологія усвідомлення

Онтологічні ризики в контексті кадрової військової політики України та Ізраїлю можна розглядати через призму ідентичності, самоактуалізації, цінностей, філософії управління, організаційної культури та стратегічних орієнтирів. Розглянемо ключові аспекти для обох держав.

Ізраїль поєднує багато національностей, а єврейська громада є різноманітною за походженням, що створює складнощі в кадровій політиці. Різні групи мають несхожі погляди на службу в армії, що може призводити до внутрішніх напружень щодо ідентичності та мультикультуралізму. Значні відмінності між світосприйняттям світського і релігійного населення можуть стати джерелом напруженості в армії, що, за певних несприятливих політичних умов, може негативно вплинути на процес запровадження кадрової політики та результати військової підготовки громадян Ізраїлю. Часті воєнні конфлікти можуть формувати “воєнне мислення” та “синдром обложеної фортеці”, що може призводити до переоцінки цінностей, які впливають на кадрову політику – у напрямку розвитку ультимативної агресії або, навпаки, до пошуку прихованих шляхів багатоходової дипломатії.

В Україні, внаслідок багаторічної непослідовної політики (псевдо)еліт, необхідно повернутися до прозорого плану збереження та розвитку критично важливих об’єктів оборонно-промислового комплексу, інших основних засобів і нематеріальних активів, як провідних факторів економічної безпеки держави та джерел формування дохідної частини бюджетів усіх рівнів [41, с. 6]. Деструктивні тенденції викликають недовіру до інституцій та зниження мотивації людського капіталу, а також призводять до падіння рівня показників економічної безпеки держави (окрім продовольчої безпеки) [36, с. 41], що негативно впливає на систему військової підготовки громадян України.

Зазначені ризики, примножуючись наслідками активної фази збройного протистояння, підвищують ймовірність загострення питань пошуку громадянами самоактуалізації та самоідентифікаційної стійкості, а також підтвердження законодавчо визначених національних цінностей. Це може ставити під сумнів вектор державної (кадрової) політики, шкодити виконанню стратегій, програм, моделей тощо і становити загрозу ефективному запровадженню складових менеджменту: плануванню, організації, мотивації та контролю.

Воєнні конфлікти можуть загострювати питання регіональних відмінностей і різноманіття (політичних) поглядів, що може впливати на морально-психологічну підготовку населення та кадрову політику.

Теми соціальної справедливості можуть використовуватися у дестабілізаційних цілях і впливати на формування деструктивних інтерпретацій світогляду громадян. Накопичувальний ефект викривлення світогляду може створювати ризики, пов’язані з мотивацією та лояльністю громадян до соціальних інститутів, у тому числі – держави. Передумови для поглиблення соціально-політичного розколу за будь-якою з ознак нерівності (економічної, соціальної, політичної, етнокультурної тощо) можуть створювати ризики для єдності громадян, ефективності функціонування сил оборони України та негативно позначатися на військовій підготовці.

Б.12. Підготовче поле: аспекти устрою та права

З метою подальшого удосконалення нормативно-правової бази (військової) кадрової політики та створення цілісної системи підготовки громадян України, необхідно враховувати аспекти адміністративно-територіального устрою Ізраїлю.

У цій унітарній державі кадрова політика реалізується узгоджено на центральному та місцевому рівнях. Держава відповідає за реалізацію стратегічних програм із застосуванням базових принципів національної безпеки, тоді як місцева влада опікується захистом територій

у зоні своєї відповідальності. До повноважень місцевої влади належать створення оборонної інфраструктури та розроблення порядків розгортання сил і засобів для захисту цивільного населення в умовах надзвичайних ситуацій природного, техногенного характеру та бойових дій. Тобто, органи місцевої влади відповідають не лише за розвиток територій, а й за створення територіальної підсистеми оборони та захисту тилу, підтримку обороноздатності, захист цивільного населення та об'єктів критичної інфраструктури в умовах кризових ситуацій.

В Ізраїлі обрано воєнно-орієнтований підхід до управління в умовах кризи [42, с. 310].

В Ізраїлі діє правовий механізм для впровадження режиму "Особлива ситуація в тилу". Це дає змогу Міністерству оборони через Командування внутрішнього фронту (тилу) видавати обов'язкові для цивільного населення розпорядження, а органам безпеки – мати ширшу юрисдикцію щодо цивільних питань, таких як відкриття або закриття підприємств, шкіл, закладів вищої освіти, які займаються підготовкою громадян. Рішення є чинним протягом 48 годин, після чого має бути ратифіковане урядом.

Органи законодавчої, виконавчої, судової влади та органи місцевого самоврядування унітарної України також мають законні повноваження, але лише заслуховувати доповіді посадових осіб правоохоронних органів про виконання вимог законодавства щодо забезпечення громадської безпеки та правопорядку, контролювати стан допризовної підготовки і відбору громадян на військову службу, правового і соціального захисту тощо [43, стаття 7, 8].

Права людини є загальнолюдською цінністю, а рівність прав і свобод усіх людей – найвищою суспільною цінністю. Ці принципи закріплено у Загальній декларації прав людини, прийнятій Генеральною Асамблеєю ООН 10 грудня 1948 року.

Держава Ізраїль не має єдиної конституції, але правова система базується на "Основних законах", які виконують роль конституційних норм. Ці закони гарантують основні права, такі як свобода слова та захист гідності людини. У 1992 році був прийнятий Основний закон: Гідність і свобода людини, який закріпив захист прав людини як одну з ключових державних цінностей.

Ізраїль має змішану правову систему, що поєднує риси романо-германського та англосаксонського права. Також діють дві системи релігійного права – єврейська та мусульманська, які застосовуються до представників відповідних конфесій. Законодавство Ізраїлю в сфері прав людини поєднує демократичні принципи з викликами, пов'язаними зі складним політичним, етнічним та релігійним контекстами. Існують суперечливі аспекти, особливо у відносинах із палестинцями та меншинами, що залишаються предметом дискусій як всередині країни, так і на міжнародній арені.

В Україні використовується романо-германська правова система, що передбачає кодифіковане право із Конституцією, яка має найвищу юридичну силу.

Статтею 3 Конституції визначено, що людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави.

Разом з тим, існують законодавчі обмеження прав і свобод для забезпечення національної безпеки та оборони держави, зокрема визначені статтею 64 Конституції України. Наприклад: обмеження свободи пересування, цензура та обмеження свободи слова, обмеження свободи зібрань, мобілізація, обмеження економічної діяльності, обмеження права на конфіденційність та судові обмеження.

Введення обмежень прав і свобод має бути тимчасовим та пропорційним рівню загроз. Однак, сама можливість введення обмежень може використовуватися деструктивними силами для дискредитації органів державної влади та ставити під сумнів правомірність дій

уряду щодо громадянських прав і свобод у контексті національної безпеки та оборони на шляху до євроінтеграції. Адже такі цінності, як "повага до людської гідності" та "повага до прав людини, включно з правами меншин", закріплені у Статуті ЄС, є основоположними принципами його політичної та правової системи.

Дискредитація цінностей може загрожувати не лише процесам інтеграції до ЄС та вступу до НАТО, а й послабити міжнародну допомогу та відштовхнути частину суспільства, яка схвалює принципи індивідуалізму, секуляризму та верховенства права, від підтримки цих цінностей. Це може призвести до пошуку інших балансирів індивідуальної та колективної безпеки у відмінних правових системах світу, де зростає вплив таких міжнародних об'єднань, як Шанхайська організація співробітництва, Організація ісламського співробітництва та БРІКС.

Разом із тим, усіх людей, незалежно від переконань та існування у різних правових системах, об'єднує не лише вуглецева форма буття, а й спільний предок, що еволюціонував до здатності формулювання прагнення до справедливості у різних формах (звичай, релігійний текст, договір, нормативно-правовий акт, судовий прецедент, правова доктрина, віртуальне право тощо) та підходів до розуміння права (природне, історичне, критичне, позитивне тощо).

Самобутність традицій та соціально-економічні формації, що знаходять відображення у нормах права, історично формуються залежно від політичних, соціо-економічних, територіальних та інших передумов розвитку соціальних систем.

В епоху стрімкого розвитку інтернету, технологій штучного інтелекту, обробки великих даних та когнітивних технологій, у осіб, наділених владними повноваженнями, може виникати спокуса підлаштовування правового поля у меркантильних інтересах.

Оскільки права людини є основоположними, притаманними всім людям від народження, незалежно від наділення владними повноваженнями, громадянства держави та інших рамок, необхідно визначити напрямок поступового розширення прав особи та громадянина разом із забезпеченням реалізації цих прав, у контексті наближення правового статусу "громадянин" та "особа" до недоторканного правового статусу "людина".

Таким чином, для ефективної реалізації (військової) кадрової політики важливо враховувати вищезазначені юридичні аспекти та ризики, а також забезпечувати належну правову підтримку.

Більшість вищенаведених ризиків можна вважати проблемними ситуаціями, без поділу яких на окремі проблеми подальший управлінський вплив може бути неефективним.

У наступних розділах будуть окреслені шляхи розв'язання проблемних ситуацій та запропоновано низку рекомендацій щодо розвитку високоефективної системи (військової) підготовки громадян України.

Підготовка метафорами соціального закону збереження енергії та інформації

З метою оцінки меж проблемної ситуації та підвищення результативності механізмів (військової) підготовки, як аналогію можна використати фундаментальний закон фізики, згідно з яким енергія в ізольованій системі не зникає, а лише трансформується в іншу форму.

Вважається, що енергія та інформація взаємопов'язані. Енергія може переносити інформацію, а інформація може впливати на енергетичні процеси.

Сприймається та запам'ятовується лише та інформація, на якій зосереджується увага ("селективність уваги") та інтерпретується залежно від контексту, суб'єктності сприйняття та фізичних обмежень.

Інвестування часу, (інформаційних, енергетичних та інших) ресурсів у повторювані зусилля може перетворюватися на знання, вміння, навички та соціально-безпекову активність.

Історія розвитку передових суспільств демонструє, що конкурентну перевагу мають ті, які не лише використовують наявні ресурси, а й ефективно диверсифікують та трансформують їх у передові технології.

Енергію та інформацію можна назвати фундаментальною першоосновою буття, що не зникає та специфічно передається.

Інформація, єдина у своєму роді, може бути пов'язана із субстанцією через потребу у носії. На відміну від технічних джерел поширення, людина при передачі інформації не втрачає її для себе, але створює (не точну) копію у свідомості іншої людини. Таким чином, інформація може швидко розмножуватись без втрати оригіналу із делегуванням оригінальності джерела іншій особі.

Максимально достовірна, актуальна та повна інформація є ключовим ресурсом для підготовки громадян, що може передаватися та трансформуватися у прийнятні форми. Наприклад, з історичних фактів перетворюватися у навчальні матеріали, з них – у майбутні дослідження, статистичні дані та рекомендації.

До основних тенденцій розвитку оборонних технологій майбутнього відносяться когнітивні технології, які ґрунтуються на теоріях функціонування мозку та спрямовані на розвиток інтелектуальних здібностей людини, опанування методів раціонального ухвалення рішень із використанням спеціалізованих інформаційних технологій. Своєчасне використання цих технологій матиме принципове значення для організації процесу підготовки та розвитку людського капіталу.

Важливим є також "м'яке індокринування" далекоглядним гуманізмом.

Недоладне протиставлення непорівнянних багатофакторних систем, недолуга інформаційна політика начебто безальтернативності вибору, необґрунтована чи тенденційна зміна вектору пропаганди, продукування тоталітарного свавілля і вибіркової репресивної політики, а також інші приклади ідеологічної експлуатації суб'єктами владних повноважень можуть спонукати роздмухування полум'я конфліктів та радикальної зміни програм підготовки.

Разом з тим, складні часи подолання конфліктів та загроз мають позитивно впливати на гуртування людей навколо пошуку проривних шляхів виходу з криз (якщо не була пройдена точка біфуркації, яка потягне до катастрофічних наслідків).

Засвоєння людиною інформації (зокрема програм підготовки) можливе у разі нівелювання факторів безпосередньої загрози життю і пониження температури конфліктів та інших впливових факторів до прийнятного рівня. У якості профілактичних заходів зменшенню емоційно-інформаційного тиску на особу та подолання інформаційного хаосу у суспільстві, державна влада може сприяти трансформації апокрифічної державної політики у прозору актуальність порядку денного, що розкриватиметься шляхом налагодження механізмів демократичного цивільного діалогу та контролю, які б зацікавлювали громадян підтримувати державні інтереси та дохідливо доводили взаємовигідність спільного розвитку актуальних напрямків підготовки, як синергійних категорій, сприятливо-супутніх індивідуалістичним цінностям.

Успіх реалізації кадрової політики передбачає вироблення відповідних рішень і здійснення заходів, спрямованих на управління ризиками, щодо підвищення рівня довіри суспільства до органів законодавчої, виконавчої та судової гілок влади, позитивного сприйняття законослухняності та поваги до сил оборони України.

Вплив когнітивних технологій на формування відповідальності та творчого потенціалу громадян України

Упровадження когнітивних технологій, що сприяють відповідальній свободі слова та думки, потенційно здатне закріпити творчий принцип у національних традиціях. Це, в свою чергу, може позитивно вплинути на суспільний розвиток, зокрема на підвищення рівня життя, розширення джерел добробуту та формування позитивних намірів, а також сприяти впровадженню конструктивних методів підготовки громадян України до виконання завдань у сфері національної безпеки та оборони.

Поряд з удосконаленням інтелектуальних можливостей програмного забезпечення, важливим є розвиток технологій, спрямованих на підвищення уважності та сенсорної

чутливості. Усвідомлення людиною інформації відбувається лише за умови її виділення та акцентування увагою.

Надмірна концентрація на розвитку інтелекту, підсиленого технологіями, без належної уваги до розширення сприйняття, відповідальності та уважності може мати деструктивні наслідки як для особистості, так і для її оточення. Аналогія з гостротою багнета в руках непідготовленого воїна підкреслює потенційну небезпеку такого дисбалансу.

Розробка перспективних і конкурентоспроможних програм підготовки кадрів потребує не лише глибокого розуміння ризиків, тенденцій та інновацій, але й системного підходу, що базується на принципах гуманізму та враховує потенціал гнучкого застосування механізмів “жорсткої” та “м’якої” сили. Одним з ключових аспектів кадрової політики у військовій сфері залишається питання не лише про способи досягнення перемоги, але й про запобігання війні та побудову держави, здатної захищати свої інтереси шляхом збалансованого застосування конвенційних та силових методів.

Процес навчання та розвитку особистості полегшується за наявності авторитетного наставника та сприятливого середовища. На рівні суспільства і держави, розвиток національної науки є важливим фактором, що забезпечує основу для створення ефективних програм підготовки кадрів. Підтримка інтенсивного розвитку науки сприяє розширенню наукової спільноти, здатної до рефлексії, стійкої до маніпуляцій та зовнішніх когнітивних впливів, а також спроможної відповідати на нові виклики шляхом застосування широкого спектру наукових підходів, що всебічно враховують питання моралі, справедливості та цінностей.

Підготовка як система взаємодії: аналогія з третім законом Ньютона

Підготовка фахівців з використанням сучасних технологій має здійснюватися кваліфікованими викладачами, які самі досягли відповідного рівня компетентності та здатні оцінювати правильність напрямку руху в складних ситуаціях, застосовуючи відповідні методики та інструменти.

Будь-яка система освіти та підготовки є складною системою, в якій діють взаємопов’язані сили дії та протидії, аналогічні доцентровій та відцентровій силам у третьому законі Ньютона.

Ця аналогія підкреслює, що система військової освіти та підготовки не є одностороннім процесом. Викладачі впливають на громадян, але й громадяни, через свою активність, здатні впливати на систему, формуючи нові вимоги та очікування. Соціальна реальність будується на взаємодії, де кожна “дія” породжує “протидію”, що сприяє розвитку як особистості, так і суспільства в цілому.

Роль інтуїції в процесі підготовки

Ефективність підготовки залежить від тонкого налаштування індивідуальної сенсорної чутливості для взаємодії з реальністю та залученості до служіння суспільним інтересам. На відміну від суб’єктивних переконань, що формуються під впливом гормональних змін, упереджень, нестачі інформації та інших факторів, інтуїція здатна сприймати, відчувати, інтерпретувати та трансформувати інформацію, сприяючи прийняттю обґрунтованих рішень.

Антропоцентричний підхід у підготовці кадрів

Індивідуальність кожної людини визначається унікальним патерном нейронних зв’язків, але при цьому всі люди мають однакові базові потреби та прагнуть гідного ставлення.

У сучасному світі точиться боротьба за ідеї та їх носіїв. Проводяться дослідження, спрямовані на класифікацію людей за типами мислення, з використанням інструментів штучного інтелекту, психології, нейронауки та освітніх програм. Зокрема, функціональна магнітно-резонансна томографія використовується для вивчення зв’язків між активністю мозку та поведінкою, а також для прогнозування реакцій людини на основі особливостей її мозку [44].

Підготовка кадрів як фактор економічної стабільності та боротьби з корупцією в секторі безпеки та оборони

Значна частина державного бюджету спрямовується на забезпечення функціонування та розвиток сектору безпеки та оборони. У зв'язку з цим, ефективне використання цих коштів є критично важливим для забезпечення національної безпеки.

Корупція, некомпетентність та зрада підривають довіру громадян до державних інституцій, деформують пріоритети та уповільнюють розвиток. Тому, формування ефективної системи підготовки кадрів, яка базується на принципах доброчесності та професіоналізму, є ключовим завданням.

Система залучення, розвитку та утримання людського капіталу повинна виключати прояви непотизму, заохочувати розвиток і взаємодію, які зміцнюють довіру та розширюють поле безпеки. Підготовка кадрів, шляхом позитивного наслідування, має сприяти консолідації суспільства, поширювати об'єктивну інформацію та запобігати приховуванню чи спотворенню суспільно важливих даних, а також унеможливлювати отримання неправомірної вигоди.

З метою мінімізації корупційних ризиків та підвищення ефективності використання бюджетних коштів, необхідно впроваджувати наступні заходи:

- Розробка та впровадження освітніх програм з етики та антикорупційної грамотності для всіх учасників процесу підготовки.
- Раціональна цифровізація систем логістики та закупівель, включаючи введення електронних реєстрів.
- Адаптація нормативно-правової бази щодо інформації та таємниці до сучасних вимог, зокрема, перегляд Зводу відомостей, що становлять державну таємницю, з метою спрощення доступу до певних даних для міжнародних донорів, які залучені до допомоги Україні через програми навчання та підготовки.
- Впровадження інтеграційних блоків на підготовчих онлайн-платформах (можливо, на базі блокчейн-технологій) для забезпечення прозорої звітності, реєстрації учасників програм, контролю використання фінансових ресурсів та забезпечення можливості анонімних звернень щодо можливих випадків корупції.
- Налаштування ефективних систем мотивації та санкцій для учасників програм підготовки, викладачів та адміністраторів.
- Проведення інформаційних кампаній з метою підвищення обізнаності про корупційні ризики та способи їх запобігання.

Підготовка фахівців з підготовки кадрів

До формування змістовної частини програм підготовки та їх викладання слід залучати фахівців, які відповідають наступним критеріям:

- Проходження відбору не лише на основі кваліфікаційної придатності, але й доброчесності, що підтверджується комплексним психологічним обстеженням особистісних характеристик (зокрема, з використанням апаратури дослідження психофізіологічних реакцій).
- Знання історії та наслідків реформ (еволюційних, революційних, адміністративних, економічних, соціальних, політичних, інституційних, правових, міжнародних тощо).
- Обізнаність з сучасними методиками педагогіки (та особливостями андрагогіки).
- Володіння основними науковими підходами до психологічної класифікації типів особистостей та їх психологічних характеристик.

Групова та індивідуальна кастомізація підготовки

Враховуючи наявність науково підтверджених особистісних відмінностей між людьми, на рівні окремих програм підготовки доцільно організовувати пілотні проєкти, диверсифіковані за різними критеріями, такими як:

- Вікові групи: юнаки, ранній зрілий вік, середній зрілий вік.

- Типи особистості: “новатори”, “консерватори”, “конструктори”, “рефлектори”, “центристи” тощо.

В умовах короткостроковості та інтенсивності підготовки, побудова програм за подібною систематизацією може сприяти комфортнішому та ефективнішому засвоєнню нових знань, умінь та навичок. Представників відповідних (ціннісних) груп можна мотивувати різними системами заохочень. Доцільно присвоювати групам назви, що відображають їх світоглядні орієнтації та підкреслюють їх гідність. Наприклад, групи представників середнього зрілого віку з консервативними поглядами можна назвати “Основа традицій” або “Консервативний форум”.

Групові програми підготовки можуть бути інтегровані з елементами розвитку емоційної компетентності (EQ).

Важливо враховувати індивідуальні особливості та потреби кожного учасника, розробляючи індивідуальні навчальні траєкторії, що враховують рівень попередньої підготовки, спрямованість інтересів та специфічні потреби.

Емпіричним підтвердженням ефективності запропонованого підходу є бізнес-практики клієнтоорієнтованої лідогенерації у відповідності до цільових груп, а також використання метрик на кшталт “пожиттєва цінність клієнта” (CLTV), що демонструють вищу ефективність при їх застосуванні.

Висновки

З огляду на те, що на сьогодні в Україні відсутня цілісна та усталена система військової підготовки громадян, актуальним є вивчення та адаптація досвіду держав, які ефективно застосовують асиметричні дії, гібридні підходи у воєнних конфліктах, а також інших результативних практик, що довели свою ефективність у сфері національної безпеки й оборони.

Коректне тлумачення безпекового середовища, адекватна інтерпретація актуальних викликів, ризиків і загроз, здійснення наукового прогнозування, а також послідовна та скоординована реалізація процесів планування, програмування, бюджетування й виконання (ППБВ) є ключовими чинниками формування ефективної державної політики у сфері безпеки й оборони. Особливо це стосується кадрової політики у силах оборони України, спрямованої на створення функціональної та стійкої системи військової підготовки громадян.

Розробка та імплементація сучасних програм і моделей підготовки оборонного резерву у складі загальнонаціональної системи військової підготовки громадян України може стати одним із визначальних факторів якісної трансформації Збройних Сил України та інших складових сил оборони. Це сприятиме зростанню обороноздатності держави через формування професійного військового компонента, а також розвитку оборонних спроможностей і загального добробуту громадян.

В умовах критичних загроз державному суверенітету, інтереси громадянина, суспільства та держави потребують максимальної консолідації [41, с. 3]. Водночас, згідно з щорічним Звітом про глобальні ризики, основними занепокоєннями для світової бізнес-спільноти та політичних лідерів на найближчі роки є не збройні конфлікти чи кліматичні зміни, а дезінформація, поширення неправдивої інформації та поляризація суспільств [13].

У зв’язку з цим, в умовах екзистенційної загрози українській державності, необхідним є всебічний облік існуючих і потенційних загроз, а також подальша адаптація нормативно-правової бази у сфері кадрової політики загалом і військової підготовки громадян зокрема. З цією метою слід здійснювати систематичний моніторинг безпекової обстановки, поглиблений порівняльний аналіз міжнародного досвіду, всебічну оцінку ризиків, впровадження науково обґрунтованих прогнозів, а також посилення міжвідомчої та міжнародної координації з урахуванням найкращих практик провідних країн світу.

Інтеграція найбільш ефективних методів, інструментів, вмінь і практик (МІВіП) у систему військової підготовки громадян України дозволить не лише забезпечити високий рівень підготовки особового складу, а й досягти злагодженості та високих показників бойового вишколу (у тому числі з мобілізаційних питань) військових частин і оперативної підготовки органів військового управління у межах єдиної безпекової архітектури.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Список використаних джерел

1. Про внесення змін до Конституції України (щодо стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору) : Закон України від 07.02.2019 № 2680-VIII. URL : https://zakon.rada.gov.ua/laws/show/2680-19#Text (дата звернення 06.10.2024).
2. Про затвердження Порядку організації та здійснення оборонного планування в Міністерстві оборони України, Збройних Силах України та інших складових сил оборони : Наказ М-ва оборони України від 22.12.2020 № 484. URL : https://zakon.rada.gov.ua/laws/show/z0196-21#Text (дата звернення 08.09.2024).
3. Про затвердження плану пріоритетних дій Уряду на 2023 рік. *Офіційний вебпортал парламенту України.* URL : https://zakon.rada.gov.ua/rada/show/221-2023-p#n13 (дата звернення 08.09.2024).
4. Про затвердження Концепції військової кадрової політики в системі Міністерства оборони України на період до 2028 року: Наказ М-ва оборони України від 27.10.2023 № 637. URL : https://zakon.rada.gov.ua/rada/show/v0637322-23#Text (дата звернення 06.10.2024).
5. Указ Президента України № 36/2022 – Офіційне інтернет-представництво Президента України. *Офіційне інтернет-представництво Президента України*. URL : https://www.president.gov.ua/documents/362022-41285 (дата звернення 06.10.2024).
6. Про внесення змін до деяких законодавчих актів України щодо окремих питань проходження військової служби, мобілізації та військового обліку. *Офіційний вебпортал парламенту України.* URL : https://zakon.rada.gov.ua/laws/show/3633-20#Text (дата звернення: 08.09.2024).
7. Про військовий обов'язок і військову службу. *Офіційний вебпортал парламенту України.* URL: https://zakon.rada.gov.ua/laws/show/2232-12#n1713 (дата звернення: 09.09.2024).
8. Mahal. URL: https://www.mahal.org.il/en/Pages/default.aspx (дата звернення: 11.10.2024).
9. Michalowski M. How Much Data Is Generated Every Day in 2024? *Spacelift.* URL : https://spacelift.io/blog/how-much-data-is-generated-every-day (дата звернення 15.09.2024).
10. Hegel, G. W. F. Phenomenology of spirit. *Trans. AV Miller/Oxford: Oxford UP.* 1977. https://doi.org/10.1515/9780822390169-005 (дата звернення: 11.10.2024).
11. Про затвердження Указу Президента України "Про продовження строку дії воєнного стану в Україні". *Офіційний вебпортал парламенту України*. URL : https://zakon.rada.gov.ua/laws/show/3891-20#Text (дата звернення: 06.10.2024).
12. Про мобілізаційну підготовку та мобілізацію. *Офіційний вебпортал парламенту України.* URL : https://zakon.rada.gov.ua/laws/show/3543-12#Text (дата звернення: 06.10.2024).
13. Звернення Президентки Європейської Комісії Урсули фон дер Ляєн на Всесвітньому економічному форумі. World Economic Forum. Давос, 16.01.2024. URL : https://www.weforum.org/meetings/world-economic-forum-annual-meeting-

2024/sessions/special-address-by-ursula-von-der-leyen-president-of-the-european-commission-96293a5a9d/ (дата звернення: 06.10.2024).
14. World Bank Open Data. World Bank Open Data. URL : https://data.worldbank.org/indicator/NY.GDP.MKTP.CD (date of access: 05.09.2024).
15. Міністерство Фінансів України. *Міністерство Фінансів України*. URL : https://mof.gov.ua/uk/news/derzhavnii_ta_garantovanii_derzhavoiu_borg_ukraini_z_pochatku_2024_roku_stav_deshevshim_na_ponad_10-4741 (дата звернення: 09.09.2024).
16. Ukrinform. Дефіцит бюджету цьогоріч очікується на рівні 20,7% ВВП – Нацбанк. *Укрінформ,* 03.05.2024. URL : https://www.ukrinform.ua/rubric-economy/3859580-deficit-budzetu-cogoric-ocikuetsa-na-rivni-207-vvp-nacbank.html (дата звернення 12.10.2024).
17. Щомісячний макроекономічний та монетарний огляд. Київ : *Департамент монетар. політики та екон. аналізу НБУ*, вересень 2024. 32 с. URL : https://bank.gov.ua/admin_uploads/article/MMR_2024-09.pdf?v=9
18. Економічна правда. В Україні історичний розрив між експортом та імпортом. *Економічна правда*. URL : https://www.epravda.com.ua/weeklycharts/2024/05/16/713755/ (дата звернення: 12.10.2024).
19. Грушецький А. Прес-релізи та звіти – Динаміка довіри соціальним інституціям у 2021-2023 роках. *Домашня сторінка КМІС*, 18.12.2023. URL : https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1335&page=1 (дата звернення 06.10.2024).
20. Адаптація ветеранів війни до мирного життя: помічник ветерана. *Домашня сторінка НІСД*, 06.11.2023. URL : https://niss.gov.ua/news/komentari-ekspertiv/adaptatsiya-veteraniv-viyny-do-myrnoho-zhyttya-pomichnyk-veterana (дата звернення 10.11.2024).
21. Войтовський К. Досвід Ізраїлю щодо формування стратегії національної безпеки. *Домашня сторінка НІСД*, 17.06.2022. URL : https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/dosvid-izrayilyu-shchodo-formuvannya-stratehiyi-natsionalnoyi (дата звернення 10.11.2024).
22. Varnalii Z., Bilyk R., Khmelevskiy M. Social security of Ukraine: summary, problems and ways of ensuring. *University Economic Bulletin*. 2020. No. 45. P. 105–114. URL : https://doi.org/10.31470/2306-546x-2020-45-105-114 (date of access: 11.10.2024).
23. Кодекс законів про працю України. *Портал Федерації металургів України*, 19.02.2019. URL : http://fedmet.org/analytics/kodeks-zakoniv-pro-pracyu-ukraini/ (дата звернення 10.11.2024).
24. Комісарова Н., Комісаров М., Шарко Д. Питання соціального забезпечення військовослужбовців: правові та юридичні аспекти. *Наукові інновації та передові технології 2024*. №5(33). 1489 с. URL : http://socrates.vsau.org/repository/getfile.php/36064.pdf (дата звернення 06.10.2024).
25. Про перерахунок пенсій особам, які звільнені з військової служби, та деяким іншим категоріям осіб. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/103-2018-п#Text (дата звернення: 06.10.2024).
26. Про пенсійне забезпечення осіб, звільнених з військової служби, та деяких інших осіб. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/2262-12#Text (дата звернення 11.10.2024).
27. Уповноважений Верховної Ради України з прав людини – Головна. URL: https://www.ombudsman.gov.ua/storage/app/media/pensiyne-zabezpechennya.pdf (дата звернення 11.10.2024).
28. Сили безпеки і оборони інформують щодо нового порядку нарахування грошового забезпечення. Radware Captcha Page, 31.12.2023. URL: https://www.kmu.gov.ua/news/syly-bezpeky-i-oborony-informuiut-shchodo-novoho-

poriadku-narakhuvannia-hroshovoho-zabezpechennia (дата звернення: 06.10.2024).
29. Бєлоусов В. Д. Особливі принципи соціальної безпеки сучасної України. *Актуальні проблеми права: теорія і практика*. 2024. № 47. С. 26–35. URL: https://doi.org/10.33216/2218-5461/2024-47-1-26-35 (дата звернення: 11.09.2024).
30. Андаліцька І. Чи можлива зараз обов'язкова мобілізація жінок в Україні: нардеп прояснив ситуацію. *Інформаційне агентство УНІАН*, 18.10.24 URL: https://www.unian.ua/politics/chi-mozhliva-zaraz-obov-yazkova-mobilizaciya-zhinok-v-ukrajini-nardep-proyasniv-situaciyu-12791394.html?_gl=1*h0zzi1*_ga*MjAwMDk2OTIzMS4xNzI4MzI4NTM3*_ga_TECJ2YKWSJ*MTcyOTQ0MDI0NS4yLjAuMTcyOTQ0MDI0NS42MC4wLjA.*_ga_DENC12J6P3*MTcyOTQ0MDI0NS4yLjAuMTcyOTQ0MDI0NS42MC4wLjE2MzE1MDQwMg..
31. Павлушенко С., Лисенко Д. Досвід підтримання та відновлення морально-психологічного стану військовослужбовців військових частин (підрозділів) Збройних Сил України під час російсько-української війни: інформаційно-аналітичні матеріали. Київ : *НУОУ*, 2023. 28 с.
32. Eric Ciaramella Envisioning a Long-Term Security Arrangement for Ukraine. *The Carnegie Endowment for International Peace*, 08.06.2023 32 с. URL: https://carnegieendowment.org/research/2023/06/envisioning-a-long-term-security-arrangement-for-ukraine?lang=en (дата звернення 02.09.2024).
33. Joint Statement of the Leaders of India, Israel, United Arab Emirates, and the United States (I2U2) | The White House. *The White House*. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/14/joint-statement-of-the-leaders-of-india-israel-united-arab-emirates-and-the-united-states-i2u2/ (date of access: 14.09.2024).
34. Навіть найгірша угода України з РФ буде кращою за нинішню ситуацію – Трамп на передвиборчому виступі. *Інформаційне агентство Інтерфакс-Україна*. 26.09.2024 URL: https://interfax.com.ua/news/political/1016467.html (дата звернення 06.10.2024).
35. Про надання грифа оновленим навчальним програмам : Наказ М-ва освіти і науки України № 698 *Офіційний вебпортал МОН України.* URL: https://mon.gov.ua/npa/pro-nadannya-grifa-onovlenim-navchalnim-programam (дата звернення 08.09.2024)
36. Бєлік А. О. Аналіз державної політики забезпечення економічної безпеки : кваліфікаційна наукова праця на правах рукопису. Київ : *НАДУ*, 2016. 102 с.
37. The World Factbook, Israel. *CIA*. URL: https://www.cia.gov/the-world-factbook/countries/israel/ (дата звернення 15.09.2024).
38. Кущ. О. Феномен Ізраїлю, або Як виживати в несприятливих умовах. *ГЛАВКОМ*. URL: https://glavcom.ua/columns/olexkush/fenomen-izrajilju-abo-jak-vizhivati-v-nesprijatlivikh-umovakh-961329.html (дата звернення: 11.10.2024).
39. Кравченко О. Ізраїль похвалився показниками приросту населення за 2021 рік. *ГЛАВКОМ*. URL: https://glavcom.ua/world/observe/izrajil-pohvalivsya-pokaznikami-prirostu-naselennya-za-2021-rik-810782.html (дата звернення: 11.10.2024).
40. Смертність в Україні. *Опендатабот*. URL: https://opendatabot.ua/open/death-statistics (дата звернення: 11.10.2024).
41. Бєлік А. О. Конверсія воєнної економіки в період переходу до ринкових відносин : кваліфікаційна наукова праця на правах рукопису. Київ : *ВІКНУ*, 2005. 60 с.
42. Терент'єва А. Досвід Держави Ізраїль щодо управління безпекою цивільного населення в умовах кризових ситуацій. Науковий вісник: Державне управління. 2023. № 2 (14). С. 310–333. https://doi.org/10.33269/2618-0065-2023-2(14)-310-333
43. Про національну безпеку України. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 06.10.2024).
44. Knutson B., Greer S. M. Anticipatory affect: neural correlates and consequences for choice. Philosophical Transactions of the Royal Society B: Biological Sciences. 2008. Vol. 363,

No. 1511. P. 3771–3786. https://doi.org/10.1098/rstb.2008.0155 (дата звернення: 18.10.2024).

References

1. Pro vnesennja zmin do Konstytuciji Ukrajiny (shhodo strateghichnogho kursu derzhavy na nabuttja povnopravnogho chlenstva Ukrajiny v Jevropejsjkomu Sojuzi ta v Orghanizaciji Pivnichnoatlantychnogho doghovoru) : Zakon Ukrajiny vid 07.02.2019 № 2680-VIII. Available from : https://zakon.rada.gov.ua/laws/show/2680-19#Text (data zvernennja 06.10.2024).
2. Pro zatverdzhennja Porjadku orghanizaciji ta zdijsnennja oboronnogho planuvannja v Ministerstvi oborony Ukrajiny, Zbrojnykh Sylakh Ukrajiny ta inshykh skladovykh syl oborony : Nakaz M-va oborony Ukrajiny vid 22.12.2020 №484. Available from : https://zakon.rada.gov.ua/laws/show/z0196-21#Text (data zvernennja 08.09.2024).
3. Pro zatverdzhennja planu priorytetnykh dij Urjadu na 2023 rik. Oficijnyj vebportal parlamentu Ukrajiny. Available from : https://zakon.rada.gov.ua/rada/show/221-2023-r#n13 (data zvernennja 08.09.2024).
4. Pro zatverdzhennja Koncepciji vijsjkovoji kadrovoji polityky v systemi Ministerstva oborony Ukrajiny na period do 2028 roku: Nakaz M-va oborony Ukrajiny vid 27.10.2023 № 637. Available from : https://zakon.rada.gov.ua/rada/show/v0637322-23#Text (data zvernennja 06.10.2024).
5. Ukaz Prezydenta Ukrajiny № 36/2022 – Oficijne internet-predstavnyctvo Prezydenta Ukrajiny. Oficijne internet-predstavnyctvo Prezydenta Ukrajiny. Available from : https://www.president.gov.ua/documents/362022-41285 (data zvernennja 06.10.2024).
6. Pro vnesennja zmin do dejakykh zakonodavchykh aktiv Ukrajiny shhodo okremykh pytanj prokhodzhennja vijsjkovoji sluzhby, mobilizaciji ta vijsjkovogho obliku. Oficijnyj vebportal parlamentu Ukrajiny. Available from : https://zakon.rada.gov.ua/laws/show/3633-20#Text (data zvernennja: 08.09.2024).
7. Pro vijsjkovyj obov'jazok i vijsjkovu sluzhbu. Oficijnyj vebportal parlamentu Ukrajiny. Available from : https://zakon.rada.gov.ua/laws/show/2232-12#n1713 (data zvernennja: 09.09.2024).
8. Mahal. Available from : https://www.mahal.org.il/en/Pages/default.aspx (date of access: 08.10.2024).
9. Michalowski M. How Much Data Is Generated Every Day in 2024? *Spacelift.* Available from : https://spacelift.io/blog/how-much-data-is-generated-every-day (data zvernennja: 06.10.2024).
10. Hegel, G. W. F. Phenomenology of spirit. *Trans. AV Miller/Oxford: Oxford UP.* 1977. Available from : https://doi.org/10.1515/9780822390169-005 (data zvernennja: 06.10.2024).
11. Pro zatverdzhennja Ukazu Prezydenta Ukrajiny "Pro prodovzhennja stroku diji vojennogho stanu v Ukrajini". Oficijnyj vebportal parlamentu Ukrajiny. Available from : https://zakon.rada.gov.ua/laws/show/3891-20#Text (data zvernennja: 06.10.2024).
12. Pro mobilizacijnu pidghotovku ta mobilizaciju. Oficijnyj vebportal parlamentu Ukrajiny. Available from : https://zakon.rada.gov.ua/laws/show/3543-12#Text (data zvernennja: 06.10.2024).
13. Zvernennia Prezydentky Yevropeiskoi Komisii Ursuly fon der Liaien na Vsesvitnomu ekonomichnomu forumi. World Economic Forum. Davos, 16.01.2024. Available from : https://www.weforum.org/meetings/world-economic-forum-annual-meeting-2024/sessions/special-address-by-ursula-von-der-leyen-president-of-the-european-commission-96293a5a9d/ (data zvernennia: 06.10.2024).
14. World Bank Open Data. World Bank Open Data. Available from : https://data.worldbank.org/indicator/NY.GDP.MKTP.CD (date of access: 05.09.2024).
15. Ministerstvo Finansiv Ukrajiny. Ministerstvo Finansiv Ukrajiny. Available from :

https://mof.gov.ua/uk/news/derzhavnii_ta_garantovanii_derzhavoiu_borg_ukraini_z_pochatku_2024_roku_stav_deshevshim_na_ponad_10-4741 (data zvernennja: 09.09.2024).
16. Ukrinform. Deficyt bjudzhetu cjoghorich ochikujetjsja na rivni 20,7% VVP – Nacbank. Ukrinform, 03.05.2024. Available from : https://www.ukrinform.ua/rubric-economy/3859580-deficit-budzetu-cogoric-ocikuetsa-na-rivni-207-vvp-nacbank.html (data zvernennja 12.10.2024).
17. Shhomisjachnyj makroekonomichnyj ta monetarnyj oghljad. Kyjiv : Departament monetar. polityky ta ekon. analizu NBU, veresenj 2024. 32 s. Available from : https://bank.gov.ua/admin_uploads/article/MMR_2024-09.pdf?v=9
18. Ekonomichna pravda. V Ukrajini istorychnyj rozryv mizh eksportom ta importom. Prote je i pozytyvni novyny. Ekonomichna pravda. Available from : https://www.epravda.com.ua/weeklycharts/2024/05/16/713755/ (data zvernennja: 12.10.2024).
19. Ghrushecjkyj A. Pres-relizy ta zvity – Dynamika doviry socialjnym instytucijam u 2021-2023 rokakh. Domashnja storinka KMIS, 18.12.2023. Available from : https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1335&page=1 (data zvernennja 06.10.2024).
20. Adaptacija veteraniv vijny do myrnogho zhyttja: pomichnyk veterana. Domashnja storinka NISD, 06.11.2023. Available from : https://niss.gov.ua/news/komentari-ekspertiv/adaptatsiya-veteraniv-viyny-do-myrnoho-zhyttya-pomichnyk-veterana (data zvernennja 10.11.2024).
21. Vojtovsjkyj K. Dosvid Izrajilju shhodo formuvannja strateghiji nacionaljnoji bezpeky. Domashnja storinka NISD, 17.06.2022. Available from : https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/dosvid-izrayilyu-shchodo-formuvannya-stratehiyi-natsionalnoyi (data zvernennja 10.11.2024).
22. Varnalii Z., Bilyk R., Khmelevskiy M. Social security of Ukraine: summary, problems and ways of ensuring. University Economic Bulletin. 2020. No. 45. P. 105–114. https://doi.org/10.31470/2306-546x-2020-45-105-114 (date of access: 11.10.2024).
23. Kodeks zakoniv pro pracju Ukrajiny. Portal Federaciji metalurghiv Ukrajiny, 19.02.2019. Available from : http://fedmet.org/analytics/kodeks-zakoniv-pro-pracyu-ukraini/ (data zvernennja 10.11.2024).
24. Komissarova N., Komissarov M., Sharko D. Pytannja socialjnogho zabezpechennja vijsjkovosluzhbovciv: pravovi ta jurydychni aspekty. Naukovi innovaciji ta peredovi tekhnologhiji 2024. №5(33). 1489 s. Available from : http://socrates.vsau.org/repository/getfile.php/36064.pdf (data zvernennja 06.10.2024).
25. Pro pererakhunok pensij osobam, jaki zviljneni z vijsjkovoji sluzhby, ta dejakym inshym kateghorijam osib. Oficijnyj vebportal parlamentu Ukrajiny. Available from : https://zakon.rada.gov.ua/laws/show/103-2018-p#Text (data zvernennja: 06.10.2024).
26. Pro pensijne zabezpechennja osib, zviljnenykh z vijsjkovoji sluzhby, ta dejakykh inshykh osib. Oficijnyj vebportal parlamentu Ukrajiny. Available from : https://zakon.rada.gov.ua/laws/show/2262-12#Text (data zvernennja 11.10.2024).
27. Upovnovazhenyj Verkhovnoji Rady Ukrajiny z prav ljudyny – Gholovna. Available from : https://www.ombudsman.gov.ua/storage/app/media/pensiyne-zabezpechennya.pdf (data zvernennja 11.10.2024).
28. Syly bezpeky i oborony informujutj shhodo novogho porjadku narakhuvannja ghroshovogho zabezpechennja. Radware Captcha Page, 31.12.2023. Available from : https://www.kmu.gov.ua/news/syly-bezpeky-i-oborony-informuiut-shchodo-novoho-poriadku-narakhuvannia-hroshovoho-zabezpechennia (data zvernennja: 06.10.2024).
29. Bjelousov V. D. Osoblyvi pryncypy socialjnoji bezpeky suchasnoji Ukrajiny. Aktualjni problemy prava: teorija i praktyka. 2024. № 47. S. 26–35. https://doi.org/10.33216/2218-5461/2024-47-1-26-35 (data zvernennja: 11.09.2024).

30. Andalicjka I. Chy mozhlyva zaraz obov'jazkova mobilizacija zhinok v Ukrajini: nardep projasnyv sytuaciju. Informacijne aghentstvo UNIAN, 18.10.24 Available from : https://www.unian.ua/politics/chi-mozhliva-zaraz-obov-yazkova-mobilizaciya-zhinok-v-ukrajini-nardep-proyasniv-situaciyu-12791394.html?_gl=1*h0zzi1*_ga*MjAwMDk2OTIzMS4xNzI4MzI4NTM3*_ga_TECJ2YKWSJ*MTcyOTQ0MDI0NS4yLjAuMTcyOTQ0MDI0NS42MC4wLjA.*_ga_DENC12J6P3*MTcyOTQ0MDI0NS4yLjAuMTcyOTQ0MDI0NS42MC4wLjE2MzE1MDQwMg.
31. Pavlushenko S., Lysenko D. Dosvid pidtrymannja ta vidnovlennja moraljno-psykhologhichnogho stanu vijsjkovosluzhbovciv vijsjkovykh chastyn (pidrozdiliv) Zbrojnykh Syl Ukrajiny pid chas rosijsjko-ukrajinsjkoji vijny: informacijno-analitychni materialy. Kyjiv : NUOU, 2023. 28 s.
32. Eric Ciaramella Envisioning a Long-Term Security Arrangement for Ukraine. The Carnegie Endowment for International Peace, 08.06.2023 32 s. Available from : https://carnegieendowment.org/research/2023/06/envisioning-a-long-term-security-arrangement-for-ukraine?lang=en (data zvernennja 06.10.2024).
33. Joint Statement of the Leaders of India, Israel, United Arab Emirates, and the United States (I2U2) | The White House. The White House. Available from : https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/14/joint-statement-of-the-leaders-of-india-israel-united-arab-emirates-and-the-united-states-i2u2/
34. Navitj najghirsha ughoda Ukrajiny z RF bude krashhoju za nynishnju sytuaciju – Tramp na peredvyborchomu vystupi. Informacijne aghentstvo Interfaks-Ukrajina. 26.09.2024. Available from : https://interfax.com.ua/news/political/1016467.html
35. Pro nadannia hryfa onovlenym navchalnym prohramam : Nakaz M-va osvity i nauky Ukrainy № 698 Ofitsiinyi vebportal MON Ukrainy. Available from : https://mon.gov.ua/npa/pro-nadannya-grifa-onovlenim-navchalnim-programam (data zvernennia 08.09.2024)
36. Byelik A. O. Analiz derzhavnoji polityky zabezpechennja ekonomichnoji bezpeky : kvalifikacijna naukova pracja na pravakh rukopysu. Kyjiv : NADU, 2016. 102 s.
37. The World Factbook, Israel. CIA. Available from : https://www.cia.gov/the-world-factbook/countries/israel/
38. Kushh. O. Fenomen Izrajilju, abo Jak vyzhyvaty v nespryjatlyvykh umovakh. GhLAVKOM. Available from : https://glavcom.ua/columns/olexkush/fenomen-izrajilju-abo-jak-vizhivati-v-nesprijatlivikh-umovakh-961329.html (data zvernennja: 11.10.2024).
39. Kravchenko O. Izrajilj pokhvalyvsja pokaznykamy pryrostu naselennja za 2021 rik. GhLAVKOM. Available from : https://glavcom.ua/world/observe/izrajil-pohvalivsya-pokaznikami-prirostu-naselennya-za-2021-rik-810782.html (data zvernennja: 11.10.2024).
40. Smertnistj v Ukrajini. Opendatabot. Available from : https://opendatabot.ua/open/death-statistics (data zvernennja: 11.10.2024).
41. Byelik A. O. Konversija vojennoji ekonomiky v period perekhodu do rynkovykh vidnosyn : kvalifikacijna naukova pracja na pravakh rukopysu. Kyiv : VIKNU, 2005. 60 s.
42. Terent'jeva A. Dosvid Derzhavy Izrajilj shhodo upravlinnja bezpekoju cyviljnogho naselennja v umovakh kryzovykh sytuacij. Naukovyj visnyk: Derzhavne upravlinnja. 2023. # 2 (14). S. 310–333. https://doi.org/10.33269/2618-0065-2023-2(14)-310-333
43. Pro nacionaljnu bezpeku Ukrajiny. Oficijnyj vebportal parlamentu Ukrajiny. Available from : https://zakon.rada.gov.ua/laws/show/2469-19#Text (data zvernennja: 06.10.2024).

Еволюція хімічних, біологічних, радіологічних та ядерних небезпек. Нові виклики та загрози національній безпеці

Evolution of chemical, biological, radiological and nuclear hazards. New challenges and threats national security

Олексій Соломицький [A]
д. військ. н., старший науковий співробітник, начальник відділу – заступник начальника управління, e-mail: solosa1@gmail.com, ORCID: 0000-0001-8061-8895

Андрій Бачинський [A]
Corresponding author: ад'юнкт, e-mail: bachinsky1985@ukr.net, ORCID: 0009-0001-3251-0326

Oleksii Solomytskyi [A]
Dr of military Sciences, senior researcher, chief of section-deputy chief of derectorate, e-mail: solosa1@gmail.com, ORCID: 0000-0001-8061-8895

Andrii Bachynskyi [A]
Corresponding author: PhD student, e-mail: bachinskyl985@ukr.net, ORCID: 0009-0001-3251-0326

[A] Центральний науково-дослідний інститут Збройних Сил України м. Київ, Україна

[A] Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine

Received: April 3, 2025 | Revised: April 22, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.10

Мета роботи: дослідження еволюції ХБРЯ небезпек та визначення впливу розвитку науково-технічної сфери на характер ХБРЯ загроз в майбутньому.

Метод дослідження: методи аналізу та синтезу, метод формалізації, кон'юнктурний аналіз.

Результати дослідження: проведено ретроспективний аналіз еволюції ХБРЯ небезпек за різними періодами, визначено основні особливості їх еволюції за кожним періодом, сформовано сучасні тенденції їх трансформації в подальшому та можливі сценарії їх реалізації.

Теоретична цінність дослідження: стаття поглиблює наше розуміння значних трансформацій в сфері ХБРЯ захисту, зумовлених технологічним прогресом, змінами в геополітичній динаміці та еволюцією на тлі широкого використання штучного інтелекту, робототехніки, аналізу великих даних, цифрової біології та біотехнологій, нано- і квантових технологій, технологій 3D-друку, кібертехнологій, а також фізики високих енергій.

Цінність: дослідження пропонує значну цінність у розумінні та прогнозуванні природи та характеру майбутніх ХБРЯ небезпек та можливих сценаріїв їх реалізації, а також надає різні позиції, через які можна аналізувати дані небезпеки та розробляти стратегії відповідно до нових загроз національній безпеці.

Майбутні дослідження: напрямками подальших досліджень можуть бути визначення та обґрунтування шляхів для ефективного реагування на майбутні ХБРЯ загрози, що враховують науково-технологічні зміни та можуть конкретно вплинути на майбутнє безпекове середовище, а також розробка концепцій, військових стратегій, оперативних планів, де визначатимуться реалізації цих шляхів.

Тип статті: теоретичний**,** описовий.

Purpose: to investigate the evolution of CBRN hazards and to assess the impact of scientific and technological advancement on the nature of future CBRN threats.

Method: methods of analysis and synthesis, formalization, and conjunctural analysis.

Findings: a retrospective analysis of the evolution of CBRN hazards across different periods was conducted. Key characteristics of each evolutionary stage were identified. The study outlines current trends in the transformation of such threats and possible future scenarios for their realization.

Theoretical implications: this article deepens our understanding of significant transformations in the field of CBRN defense, driven by technological progress, shifts in geopolitical dynamics, and evolution in the context of the widespread application of artificial intelligence, robotics, big data analytics, digital biology and biotechnology, nanotechnology, quantum technologies, 3D printing, cyber technologies, and high-energy physics.

Value: the research provides significant value in understanding and forecasting the nature and character of future CBRN hazards and their potential scenarios. It also offers analytical frameworks through which these hazards can be assessed and strategies can be developed in response to emerging national security threats.

Future research: further research may focus on identifying and justifying effective response strategies to future CBRN threats, considering scientific and technological changes that may influence the future security environment. It may also include the development of concepts, military strategies, and operational plans outlining the implementation of such responses.

Paper type: theoretical, descriptive.

Ключові слова: хімічний, біологічний, радіологічний і ядерний захист; БпЛА, штучний інтелект, роботизована техніка, хімічні, біологічні, радіологічні і ядерні загрози; ризики, хімічна зброя, ядерна зброя, біологічна зброя, науково-технічна сфера, технології, еволюція, інновації.

Key words: chemical, biological, radiological, and nuclear defense; UAVs, artificial intelligence, robotics, CBRN threats, risks; chemical weapons; nuclear weapons; biological weapons; scientific and technological domain; technology; evolution; innovation.

Вступ

Сучасні сценарії загроз виявляють нові типи постійно зростаючих динамічних і агресивних викликів, що зумовлює необхідність переходу від традиційного управління безпекою до стратегічного бачення захисту громадян у більш комплексний спосіб. За останні роки суттєво зросли масштаб і складність як традиційних, так і нетрадиційних загроз миру й безпеці, зокрема асиметричних конфліктів високої інтенсивності, глобального тероризму, піратства, транснаціональної організованої злочинності, технологій ведення мережевих та безконтактних дій, розширення протиборства у кіберпросторі, а також загроз безпеці ресурсів і критичної інфраструктури. Окрему небезпеку становить зростання ризиків виробництва та розповсюдження зброї масового знищення (ЗМЗ) [1].

В такому середовищі ризик інцидентів із застосуванням хімічних, біологічних, радіологічних і ядерних (ХБРЯ) агентів, які можуть призвести до масових втрат серед населення, є вкрай високим.

Протягом останнього десятиліття глобальне середовище ХБРЯ-безпеки зазнало кардинальних змін. Сьогодні ми живемо у світі, де можливість використання ХБРЯ матеріалів або ЗМЗ державними та недержавними суб'єктами залишається однією з ключових загроз міжнародній безпеці. Зменшення ефективності міжнародних норм і механізмів нерозповсюдження, посилене науково-технічними інноваціями та іншими трендами, сприяє підвищенню ХБРЯ-ризиків. Деякі міжнародні угоди втратили чинність, а відповідні норми стали розмитими і послабленими. Резолюції Ради Безпеки ООН щодо порушників договорів не завжди виконуються, що в умовах загострення суперництва між великими державами ускладнює прийняття ефективних контрзаходів.

Корейська Народно-Демократична Республіка (КНДР) продовжує розширення ядерного і ракетного потенціалу, порушуючи відповідні резолюції Ради Безпеки ООН. Іран здійснює розбудову ракетних можливостей і подальший розвиток ядерної програми, що становить тривалий виклик регіональній безпеці та безпеці НАТО. Поведінка Китайської Народної Республіки (КНР) створює системні загрози міжнародному порядку, заснованому на нормах і правилах, важливих для глобальної безпеки. КНР стрімко розширює свій ядерний арсенал, збільшуючи кількість боєголовок та сучасних систем доставки, що на фоні відсутності прозорості та обмеженої участі у міжнародних режимах контролю над озброєннями викликає особливе занепокоєння [2; 3].

Тривожні зміни у російській ядерній доктрині, оголошені в листопаді 2024 року, свідчать про наміри розширити умови застосування ядерної зброї.

Глобальні норми, закріплені Конвенцією про заборону хімічної зброї, були суттєво порушені після 2013 року, коли в Сирії неодноразово застосовувалася хімічна зброя як державними (хлор, зарин), так і недержавними суб'єктами (іприт). КНДР у 2017 році застосувала бойову отруйну речовину VX у Малайзії.

Росія систематично застосовує хімічні агенти у ході збройної агресії проти України. З лютого 2022 по січень 2025 року російські війська здійснили 6376 випадків застосування хімічних боєприпасів, зокрема: гранати К-51 із CS (2-хлорбензальмалононітрилом) – 1488 разів, гранати РГ-ВО з CN (хлорацетофеноном) – 821 раз, та інші небезпечні хімічні речовини – 4067 разів.

Росія продовжує зберігати неоголошену програму розробки хімічної зброї. Її наукові установи — 33-й науково-дослідний і випробувальний інститут, 27-й науковий центр, Державний науково-дослідний інститут органічної хімії і технології — активно займаються розробкою бойових отруйних речовин і технологій їх доставки [4; 5].

Згідно з щорічним звітом США про дотримання Конвенції про заборону хімічної зброї, станом на 2024 рік Конвенцію порушують: Бірма — через незадекларовану програму та

невиконане знищення виробничих потужностей; КНР — через потенційну розробку речовин, що діють на центральну нервову систему; Іран — через виробництво, випробування та неповне декларування об'єктів виробництва хімічної зброї; Сирія — через незадеклароване виробництво хімічної зброї та перешкоджання перевіркам [4; 6].

Недержавні суб’єкти також дедалі активніше нехтують міжнародними нормами у сфері ХБРЯ-безпеки. У період 1990–2020 років зафіксовано 565 інцидентів застосування ХБРЯ агентів недержавними суб’єктами, серед яких: повстанці, терористичні організації, наркокартелі, транснаціональні банди, приватні військові компанії. Із них 434 інциденти стосувалися хімічних агентів, 123 – біологічних, 57 – радіологічних, 18 – ядерних (деякі події включали кілька видів агентів одночасно). Загальні втрати склали 980 загиблих і 7649 поранених, при цьому найбільші втрати спричинені застосуванням хімічних агентів. П’ятірка країн, у яких було зафіксовано найбільше інцидентів: США (118), РФ (49), Ірак (43), Японія (40), Велика Британія (30) [7].

З огляду на стрімкий розвиток науки і технологій, не можна очікувати, що потенційний супротивник використовуватиме лише відомі ХБРЯ агенти або традиційні засоби їх доставки. Це обумовлює можливість загострення картини загроз у майбутньому, коли ХБРЯ агенти та засоби їх застосування можуть стати інструментом проти військових і цивільних цілей у широкому спектрі сценаріїв — від мирного часу до конфлікту чи війни.

Теоретичні основи дослідження

Сьогодні стрімкий технологічний прогрес визначає темп розвитку суспільства та життя кожної людини. Він відбувається у геометричній прогресії, що суттєво впливає на всі сфери життєдіяльності. Наука, технології та інновації відіграють ключову роль у глобальному розвитку й сприяють вирішенню світових проблем, зокрема в галузі забезпечення національної безпеки та захисту держав від можливих викликів і загроз. Не є винятком і сфера хімічної, біологічної, радіологічної та ядерної (ХБРЯ) безпеки, де новітні технології відкривають можливості для безпечнішого поводження з небезпечними матеріалами й об’єктами, а також для запобігання, виявлення й реагування на злочини, пов’язані з ХБРЯ загрозами.

Водночас сучасні технічні рішення, покликані забезпечувати безпеку, можуть також генерувати нові ризики. Передові технології, за умови їхнього зловмисного використання, здатні створювати нові виклики для безпеки. З розвитком науково-технічного прогресу середовище ХБРЯ безпеки еволюціонує, що призводить до зростання рівня небезпеки для суспільства. Нині глобальні наукові досягнення та технологічні мегатренди, зокрема діджиталізація, мініатюризація, автономізація та автоматизація, сприяють значному ускладненню спектра ХБРЯ загроз. Відповідно, зростає різноманітність потенційних загроз, що вимагає перегляду підходів до систем виявлення, фізичного захисту та медичних контрзаходів [8].

Актуальним завданням стає аналіз і осмислення глобального впливу технологічних змін, а також визначення їхніх можливостей і викликів у ХБРЯ сфері. До технологій, які нині мають суттєве значення, належать штучний інтелект (ШІ) і робототехніка, нано- і квантові технології, технології тривимірного друку (3D-друку), кібертехнології, синтетична біологія та біотехнології, а також фізика високих енергій [9; 10].

Комп’ютерні системи, робототехнічні комплекси та інші пристрої на основі ШІ здатні миттєво обробляти великі обсяги інформації та формувати рішення, що лягають в основу управлінських процесів. Основною характеристикою ШІ-пристроїв є здатність до постійного навчання, накопичення знань, їхньої обробки й ефективного застосування. Уже сьогодні ШІ стимулює появу інновацій, а його застосування у сфері ХБРЯ захисту може змінити основні підходи до створення і використання засобів ураження.

Розвиток озброєння та військової техніки, зокрема роботизованих систем, демонструє тенденцію до масового впровадження, що розширює спектр завдань, які можуть виконуватися автоматизованими засобами. Високу ефективність у різноманітних завданнях вже довели

безпілотні системи. Однак ці ж системи можуть бути використані зловмисниками для доставки й застосування засобів масового знищення (ЗМЗ) або для ураження критичних об'єктів.

Нанотехнології, що пов'язані зі створенням нових матеріалів, пристроїв і систем шляхом маніпуляцій на молекулярному й атомному рівнях, відкривають нові можливості для ХБРЯ захисту. Зокрема, вони можуть сприяти розробці високоефективних засобів ураження й захисту, що вимагає посиленої уваги до питань контролю і регулювання.

Тенденція розширення протиборства у кіберпросторі є характерною ознакою війн останнього покоління. Розвиток кібертехнологій призвів до появи кіберзброї, яка за рівнем впливу може бути співставною із традиційними засобами масового ураження. За допомогою кібератак можна дистанційно впливати на технологічні процеси критичної інфраструктури та системи управління небезпечними ХБРЯ матеріалами, що створює ризик виникнення катастрофічних наслідків.

Ми живемо в епоху безпрецедентних біологічних ризиків, спричинених стрімким розвитком синтетичної біології. Застосування технологій редагування геному, таких як CRISPR і RT-PCR, набуло широкого поширення навіть у цивільних лабораторіях, що підвищує ризик їх зловмисного використання для створення нових біологічних засобів ураження.

Активне зростання інвестицій у квантові технології, що пропонують практично необмежену обчислювальну потужність, стало глобальним явищем. Використання принципів квантової механіки (суперпозиція, квантова заплутаність, тунелювання) відкриває нові можливості для обчислень, шифрування та комунікацій. Наприклад, тоді як сучасному суперкомп'ютеру для розкладання числа з 30–40 символів на прості множники знадобився б мільярд років, квантовий комп'ютер виконає цю задачу за 18 секунд. Водночас такі можливості породжують серйозні ризики для міжнародної безпеки.

Аналіз новітніх і передових технологій дозволяє краще усвідомити тенденції розвитку ХБРЯ загроз, оцінити можливі сценарії їх реалізації та визначити шляхи протидії. Це сприятиме формуванню більш глибокого розуміння проблематики нових викликів у сфері ХБРЯ безпеки, а також оцінці впливу науково-технічного прогресу на їхню еволюцію.

Постановка проблеми

Сучасні технологічні тенденції засвідчують, що більше не можна покладатися виключно на наявні переліки відомих агентів ХБРЯ-загроз або традиційні засоби їх доставки. Новітні технології значно розширюють можливості виготовлення та застосування ХБРЯ зброї як державними, так і недержавними суб'єктами, спрощуючи доступ до небезпечних агентів. Це, у свою чергу, підвищує ймовірність здійснення ХБРЯ атак у майбутньому.

Крім того, розвиток технологій спричиняє зростання ризику навмисного або ненавмисного порушення функціонування об'єктів атомної енергетики та хімічної промисловості, що може призвести до масштабних людських жертв і завдати суттєвих економічних збитків.

Новітні ХБРЯ загрози становлять серйозний виклик для існуючих систем безпеки та захисту. Забезпечення ХБРЯ безпеки традиційно є складним завданням, а стрімкий розвиток технологій призводить до ускладнення ландшафту ризиків, роблячи його ще більш динамічним і небезпечним. Усвідомлення й аналіз нових ризиків має вирішальне значення для ефективного запобігання інцидентам або мінімізації наслідків потенційних катастроф, пов'язаних із використанням ХБРЯ агентів.

Метою даного дослідження є аналіз еволюції ХБРЯ небезпек та окреслення змін характеру загроз у майбутньому в контексті швидкого розвитку і впровадження новітніх технологій. Вивчення впливу науково-технічного прогресу на ХБРЯ середовище дозволить своєчасно оцінити потенційні ризики та небезпеки, пов'язані з розширенням спектра загроз, а також сприятиме підвищенню ефективності заходів із запобігання й реагування на них.

Результати

Еволюція ядерної зброї

Початок ядерної ери, що стартував із першого випробування ядерної зброї 16 липня 1945 року, характеризувався сприйняттям ядерної зброї як різновиду звичайних бомб із суттєво вищою руйнівною силою. До середини 1950-х років військові стратегії ядерних держав не передбачали чіткої диференціації між застосуванням звичайної та ядерної зброї. Усвідомлення глобальної загрози, яку несе ядерна зброя для безпеки людства та розвитку цивілізації, формувалося поступово. Переломним моментом стала Корейська війна, що продемонструвала перехід ядерної зброї з розряду виключно військового засобу у сферу політичного тиску, стримування та дипломатії. Карибська криза стала другою важливою віхою, що спонукала провідні держави до усвідомлення необхідності правового регулювання та глобального контролю над розповсюдженням ядерної зброї та відповідних технологій [11].

З часу першого застосування ядерної зброї кількість ядерних випробувань перевищила 2000, з яких 528 було здійснено над поверхнею землі. Ці випробування сприяли постійному вдосконаленню ядерного арсеналу. Уже на початку 1950-х років було створено термоядерні бомби, що використовували реакції синтезу та поділу, забезпечуючи багаторазово більший вихід енергії порівняно з першими ядерними зразками. У середині 1970-х років з'явилися нейтронні боєприпаси, що мали відносно невелику вибухову силу, але генерували надзвичайно потужне радіаційне випромінювання [12].

Після Другої світової війни ядерні держави активно модернізували свій ядерний потенціал і засоби його доставки. У 1940–1950-х роках основними носіями були стратегічні бомбардувальники (США: Boeing B-29, B-50, B-52 Superfortress, Convair B-36 Peacemaker, B-47 Stratojet; СРСР: Ту-4, Ту-16, Ту-95; Велика Британія: Vickers Valiant, Handley Page Victor), здатні доставляти ядерні та термоядерні бомби на великі відстані. Також використовувалися надводні кораблі, здатні нести ядерні артилерійські боєприпаси.

Із появою крилатих (Regulus I) і балістичних ракет (Polaris A-1, P-13, P-21, P-27) спектр засобів доставки розширився за рахунок підводних човнів (США: USS Tunny (SSG-282), USS George Washington; СРСР: К-19 проекту 658, К-129 проекту 629), що мали ракети з дальністю польоту від 1000 до 3000 км.

У кінці 1950-х — на початку 1960-х років розпочалася розробка міжконтинентальних балістичних ракет (МБР) з ядерними боєголовками. Перші зразки (СРСР: Р-7, SS-6, Р-16; США: SM-65 Atlas, LGM-25C Titan II) забезпечували доставку зарядів потужністю 3–9 Мт на відстань від 8800 до 15000 км. Перші МБР запускалися зі стаціонарних платформ, однак із підвищенням уразливості таких об’єктів ракети почали розміщувати у захищених шахтах.

Із кінця 1960-х років почалася розробка мобільних комплексів для запуску МБР (СРСР: РТ-2П, РС-10 “Піонер”, РТ-2ПМ “Тополь”; КНР: DF-4) із дальністю пуску 5500–10500 км, а також залізничних комплексів (СРСР: РТ-23УТТХ “Молодець”) з дальністю до 11000 км. Паралельно розроблялися балістичні ракети для підводних човнів (СРСР: Р-29, Р-29Р, Р-29РМ) з декількома боєголовками, високою точністю наведення та можливістю ураження кількох цілей одночасно.

У подальшому зусилля ядерних держав були спрямовані на зменшення розмірів боєзарядів та інтеграцію їх у широкий спектр носіїв, що дозволяло застосовувати їх на полі бою. У 1970–1980-х роках поряд зі стратегічною зброєю розвивалася тактична ядерна зброя (ТЯЗ) з потужністю від 1 до 100 кт, призначена для обмеженого застосування по тактичних цілях, мінімізуючи супутні втрати серед цивільного населення [11]. Носіями ТЯЗ були артилерія, авіаційні та крилаті ракети, ракети малої та середньої дальності, торпеди та глибинні бомби.

Технологічний прогрес у мініатюризації привів до створення компактних ядерних пристроїв, таких як портативні заряди для спецоперацій Mk-54 SADM (вага 27 кг, потужність 0,1–1 кт) і “ядерні рюкзаки” (30 кг, 0,5–2 кт).

У 2013 році з’явилися відомості про нібито випробування СРСР компактних боєприпасів на основі Каліфорнію-251, проте через надзвичайно високу вартість ізотопу їх широке виробництво залишилось нереалізованим.

На сьогодні реальні ядерні кулі для АК не створено, однак розвиваються інші концепції, зокрема використання радіологічної зброї — куль із урановими осердями або полонієвими отруйними елементами, а також “брудних бомб”, що можуть спричиняти радіаційне зараження.

Стратегічна ядерна зброя залишається ключовим елементом глобального стримування. Водночас ризики застосування тактичної ядерної зброї у конфліктах зберігаються, причому її застосування може призвести до неконтрольованої ескалації та розгортання повномасштабної ядерної війни.

Станом на 2023 рік, згідно з даними Стокгольмського міжнародного інституту дослідження проблем миру (SIPRI), США, росія, Велика Британія, Франція, Китай, Індія, Пакистан та КНДР продовжують модернізацію своїх ядерних арсеналів. Сучасні тенденції розвитку ядерної зброї включають мініатюризацію боєголовок, удосконалення мобільних систем доставки, підвищення точності навігаційних систем і впровадження гіперзвукових технологій.

Росія, зокрема, планує до 2025–2030 років розгорнути гіперзвуковий бойовий блок “Авангард” із ракетою РС-28 “Сармат” (потужність 1–2 Мт, дальність понад 10000 км, швидкість понад 20 Махів), а також розробляє стратегічну крилату ракету “Буревісник” із ядерним двигуном. США модернізують тактичні ядерні бомби B61-12 і B61-13 та розробляють морську крилату ракету SLCM-N. Франція продовжує розробку атомних підводних човнів третього покоління та нових крилатих ракет повітряного базування.

Еволюція хімічних небезпек

Аналіз застосування хімічної зброї свідчить про проходження нею кількох етапів розвитку [13].

Перше покоління хімічної зброї бере початок із розвитком органічної та неорганічної хімії у XVIII–XIX століттях, що сприяло створенню штучних отруйних речовин. У 1774 році в ході хімічного експерименту був отриманий хлор, у 1812 році — фосген, а у 1822 році — іприт. У першій половині XIX століття синтезували численні речовини, які стали основою для майбутніх бойових отруйних речовин: у 1811 році — ціаноген; у 1820-х роках — стрихнін і морфін (попередники нейротоксинів); у 1854 році — нітрофенол (попередник фосфорорганічних сполук). Також розпочалося дослідження механізмів дії отрут на живі організми.

У цей період зафіксовано випадки застосування отруйних речовин у військових конфліктах: використання отруйного диму французькими військами під час колоніальної війни проти населення Марокко (1844–1845 роки); застосування миш'яку та сірчистого газу англійською армією у 1856 році під час Кримської війни для викурювання російських гарнізонів із фортифікаційних споруд під час облоги Севастополя; застосування пікринової кислоти англійцями під час англо-бурської війни наприкінці XIX століття.

Офіційним початком масового використання хімічної зброї в бойових діях вважається 22 квітня 1915 року, коли німецькі війська під час Першої світової війни здійснили газову атаку біля містечка Іпр, встановивши на фронті завширшки 6 км близько 6000 балонів, що містили 180 тонн хлору, і випустивши газ у напрямку французьких позицій. Саме з цього моменту розпочалася епоха “війни газу з протигазом”.

Надалі французькі (1916 рік) та англійські (1917 рік) війська також використовували хімічні речовини проти німецької армії. Французи застосовували суміші фосгену з

чотирихлористим оловом і трихлористим миш'яком, а також комбінацію синильної кислоти з трихлористим миш'яком. Англійці використовували рідкий дифосген і хлорпікрин. Німецькі війська 13 липня 1917 року вперше застосували іприт. Загалом, у період з квітня 1915 до листопада 1918 року, німці здійснили понад 50 газобалонних атак, англійці — 150, французи — 20. Було вироблено близько 180 тис. тонн отруйних речовин. Загальні втрати внаслідок застосування хімічної зброї оцінюються у 1,3 млн осіб, з яких до 100 тисяч загинули.

Завершенням етапу хімічної зброї першого покоління стало створення азотистих іпритів. До цього покоління належать три групи отруйних речовин:

- стійкі отруйні речовини шкірно-наривної та загальнотоксичної дії (сірчаний і азотисті іприти — HD та HN);
- нестійкі отруйні речовини (фосген (CG), дифосген (DP), синильна кислота (AC), люїзит (L));
- речовини подразливої дії — іританти (адамсит (DM), дифенілхлорарсин (DA), хлорпікрин (PS), дифенілціанарсин (DC), 2-хлорбензальмалононітрил (CS)).

До хімічної зброї першого покоління також відносять психотропні речовини-інкапаситанти (наприклад, LSD) та лакриматори (наприклад, хлорацетофенон (CN)), які викликали тимчасову втрату боєздатності особового складу противника.

Основними характеристиками хімічної зброї першого покоління були висока летальність за умови масового застосування та потужний психологічний вплив на особовий склад, що призводив до переляку, паніки й деморалізації. Одночасно це стимулювало розвиток засобів індивідуального захисту (протигазів, захисних костюмів) і сприяло формуванню наступних поколінь хімічної зброї.

Починаючи з 1932 року, у різних країнах розпочалися інтенсивні дослідження фосфорорганічних отруйних речовин нервово-паралітичної дії — хімічної зброї другого покоління (1930–1950-ті роки). У Німеччині були створені:

- 1936 рік — табун (GA);
- 1938 рік — зарин (GB);
- 1944 рік — зоман (GD).

У цей період було вдосконалено люїзит і включено його до бойових арсеналів. У 1950-х роках у США, в межах програм психологічної війни, був розроблений 3-квіноцилідиніл бензилат (BZ). Також розвивалися нові засоби застосування хімічної зброї, зокрема хімічні боєприпаси.

Створення хімічної зброї другого покоління стало результатом цілеспрямованого наукового підходу, заснованого на нових знаннях в органічній хімії, біохімії та токсикології. Вперше було здійснено спробу створити хімічну зброю на основі глибокого розуміння фізіології людини. Почалися системні дослідження фосфорорганічних сполук з метою підвищення їхньої токсичності, проникності через шкіру та легені й стійкості у довкіллі.

Виробництвом та накопиченням хімічної зброї у цей період займалися Німеччина, США, СРСР, Японія, Велика Британія та Італія. Після доведення високої ефективності хімічної зброї у Першій світовій війні вона стала символом "технологічної війни". У 1930-х роках, на тлі неминучості нової глобальної війни, провідні країни світу (особливо Німеччина, СРСР і США) активно готувалися до використання усіх типів зброї масового ураження, включно з хімічною. Паралельно здійснювалося масове виготовлення засобів індивідуального захисту, систем фільтрації повітря та регулярно проводилися навчання із захисту від хімічних атак. Хімічна зброя стала невід'ємною частиною бойового планування.

Таким чином, відбувалася цілеспрямована підготовка держав до можливості хімічної війни, яка, втім, не набула масштабного характеру у Другій світовій війні завдяки взаємному стримуванню. Однак розробки хімічної зброї тривали, що призвело до появи ще більш небезпечних бойових отруйних речовин у XX столітті.

Холодна війна стала каталізатором гонки озброєнь, спрямованої на створення нових типів зброї масового ураження, включаючи хімічну зброю. Держави прагнули розробити хімічні агенти з високою токсичністю, стійкістю та можливістю прихованого застосування. У цей період формується хімічна зброя третього покоління (1950–1980 роки).

У 1952 році у Великій Британії було синтезовано речовину VG, що започаткувала розробку новітніх нервово-паралітичних агентів серії V. У тому ж році був створений VX, а в СРСР у 1963–1965 роках синтезовано VR (також відомий як "Р-33") — аналог VX, а у 1970-х роках — GV, що поєднував властивості агентів серій G і V.

Хімічна зброя третього покоління включала не лише нові типи токсичних речовин, а й удосконалені засоби їх застосування, зокрема касетні артилерійські та авіаційні боєприпаси, а також бойові хімічні частини ракет ближнього і середнього радіусу дії.

У 1960–1970-х роках внаслідок пошуків безпечніших і ефективніших способів зберігання, транспортування та застосування токсичних речовин була створена бінарна хімічна зброя. З'явилися перші серійні бінарні системи: VX2 для VX та GB2 для зарину (GB). Бінарні системи започаткували нову еру "інтелектуальної" хімічної зброї, яка істотно ускладнювала її виявлення та контроль і стала прототипом сучасних засобів диверсійного ураження.

Найбільш інтенсивні роботи зі створення хімічної зброї третього покоління здійснювалися у СРСР у 1973–1976 роках. Вироблені запаси хімічних боєприпасів дозволяли забезпечити багатотисячні смертельні дози на кожного жителя планети.

Хімічна зброя третього покоління відіграла ключову роль в еволюції нервово-паралітичних агентів XX століття, поєднуючи високу бойову ефективність, стійкість до впливу зовнішнього середовища, складність виявлення та ефективність навіть за умов точкового застосування. В умовах Холодної війни вона використовувалася не лише як тактичний засіб ураження, але й як важливий елемент психологічного та стратегічного стримування.

Після створення хімічної зброї третього покоління розпочався пошук шляхів подальшого підвищення її бойових характеристик. На основі цих напрацювань було започатковано розробку хімічної зброї четвертого покоління (1980-ті роки — дотепер).

Попри те, що США у 1969 році офіційно оголосили про припинення виробництва хімічної зброї, СРСР зробив це лише у 1987 році. До цього часу, в межах програми "Фоліант", були розроблені, випущені у дослідних партіях та випробувані новітні отруйні речовини серії "Новичок", які успадкували ключові риси V-серії, однак були виведені на якісно новий рівень.

У кінці 1970-х років у Вольському філіалі Державного науково-дослідного інституту органічної хімії та технології у Шиханах були синтезовані агенти "А-232", "А-230", "А-234", що мали надзвичайно високу токсичність (приблизно у десять разів вищу за VX), складність виявлення та можливість застосування у бінарній формі. На початку 1990-х років були розроблені бінарні токсичні агенти "Новичок-5" і "Новичок-7".

Отруйні речовини четвертого покоління поєднали надзвичайну токсичність, стійкість, бінарність, високу проникність, складність виявлення та ідентифікації, що забезпечує ідеальну адаптацію до прихованого і точкового застосування та утруднює лікування. Їх поява відкрила нову еру загроз — невидимих, непередбачуваних та з великим потенціалом для зловживань.

На сьогодні науково-дослідні роботи з удосконалення та створення нових зразків хімічної зброї тривають. У світі понад 30 держав володіють технологіями або потенціалом для створення хімічної зброї [25]. Розвиток науки робить створення нових високотоксичних речовин та вдосконалення засобів їх доставки цілком реальним завданням.

Таким чином, еволюція хімічної зброї свідчить про її постійне вдосконалення в аспектах ефективності, прихованості та здатності обходити засоби захисту й міжнародні заборони. На кожному історичному етапі хімічна зброя:

- ставала дедалі небезпечнішою, зменшуючи необхідну дозу для ураження;

- набувала нових форм застосування — від примітивних газів до високотоксичних аерозолів і речовин шкірно-нервової дії;
- адаптувалася до вимог сучасного поля бою, зокрема в умовах гібридних воєн і терористичних актів;
- дедалі частіше маскувалася під мирну діяльність через використання технологій подвійного призначення.

Хімічна зброя трансформувалася від засобу масового ураження до інструмента високоточного, гібридного та потенційно терористичного застосування, що робить її особливо небезпечною у глобалізованому безпековому середовищі XXI століття.

Водночас хімічні загрози не обмежуються виключно хімічною зброєю. До них належать також ризики, пов'язані з виробництвом, транспортуванням і використанням токсичних хімічних речовин у промисловості. Аварії на хімічних підприємствах, як-от у Севезо (1976 р., Італія), Бхопалі (1984 р., Індія) та Бейруті (2020 р., Ліван), призвели до значних людських жертв і тривалого забруднення довкілля, за масштабами наслідків прирівнюючись до застосування хімічної зброї.

Еволюція хімічної промисловості пройшла кілька ключових етапів, що були зумовлені як науковими відкриттями, так і технологічними інноваціями:

Перший етап — період наукових відкриттів (XVIII — початок XIX століття). У цей період формувалися основи хімічної науки: А. Лавуазьє сформулював закон збереження маси та описав хімічні реакції з наукової точки зору; Д. Прістлі й К. Шеєле відкрили кисень; Дж. Дальтон розробив атомну теорію хімічних сполук. Хімія набула рис самостійної науки, що заклала підвалини для розвитку промислових технологій. Промислова революція стимулювала створення перших хімічних виробництв, що забезпечило основу для майбутніх досягнень у галузі синтетичних матеріалів, фармацевтики та технічної хімії.

Другий етап — період індустріальної хімії (XIX — початок XX століття). Відбувся стрімкий розвиток хімічної промисловості завдяки науковим відкриттям, індустріалізації та формуванню нових виробничих галузей. Створення великих хімічних корпорацій, таких як BASF, Bayer, DuPont, IG Farben, сприяло розширенню хімічного виробництва. Інтенсивно розвивалася органічна хімія, було започатковано виробництво синтетичних матеріалів, упроваджено синтез аміаку та створено перші пластмаси й полімери. Хімія набула вагомого значення у військовій справі (винайдення динаміту, виробництво тринітротолуолу, створення бойових отруйних речовин). Поряд із досягненнями індустріалізація хімічної промисловості породила нові загрози — зокрема, масштабне хімічне забруднення довкілля.

Третій етап — період масового виробництва (друга половина XX століття). Цей етап ознаменувався глобалізацією виробництва хімічних речовин і масовим поширенням хімічних технологій у всіх сферах життя — економіці, медицині, сільському господарстві, військовій справі. Зросли обсяги інвестицій у наукові дослідження, що сприяло відкриттю нових матеріалів, хімічних каталізаторів та біотехнологій. Водночас масове виробництво синтетичних матеріалів, розвиток нафтохімії, біохімії та агрохімії призвели до суттєвого забруднення атмосфери, водних ресурсів і ґрунтів. Саме в цей період були закладені основи для модернізації хімічної промисловості й пошуку рішень щодо екологічних проблем.

Четвертий етап — період екологічної переоцінки (друга половина XX — початок XXI століття). Стрімке зростання екологічних ризиків, пов'язаних із хімічним виробництвом, призвело до усвідомлення необхідності реформування підходів до промислового розвитку. Масове використання отруйних хімікатів, пластмас, пестицидів і промислових викидів стало причиною численних екологічних катастроф. У 1970-х роках виникли перші міжнародні ініціативи, спрямовані на зменшення промислового впливу на довкілля. У 1990-х роках була сформульована концепція "зеленої хімії", яка орієнтувалася на мінімізацію шкідливих

відходів, використання відновлюваної сировини та безпечних технологій. Хімічна промисловість почала активно адаптуватися до нових екологічних вимог, а міжнародне регулювання стало загальноприйнятою практикою.

П’ятий етап — сучасний період (XXI століття — дотепер). Хімічна промисловість продовжує розвиватися під впливом новітніх технологій, глобальних викликів і посилення екологічних стандартів. Основними напрямами її еволюції є цифровізація виробничих процесів, впровадження екологічно безпечних рішень, використання біотехнологій, а також створення нових матеріалів із заданими унікальними властивостями.

Таким чином, еволюція хімічної промисловості засвідчує, що науково-технічний прогрес у цій сфері має двоїсту природу: з одного боку — сприяє інноваціям і технічному розвитку, з іншого — породжує нові небезпеки для життя, здоров’я людей і довкілля. Використання токсичних речовин у військових цілях, масштабні техногенні аварії, екологічне забруднення є прямими наслідками такого розвитку. Сьогодні, на тлі цифровізації, глобалізації та поширення технологій подвійного призначення, загрози хімічного характеру набувають дедалі складніших форм. У майбутньому вони можуть проявитися через кібератаки на хімічні об'єкти, терористичне використання отруйних речовин і синтез нових небезпечних хімічних сполук.

Еволюція біологічних небезпек

Сучасні експерти все частіше наголошують, що людство вступило в нову еру — еру реальної та постійно зростаючої загрози біологічних небезпек [14]. Їхня еволюція пройшла декілька ключових етапів — від примітивних методів давнини до високотехнологічних розробок у військових лабораторіях.

Перший період. Біологічна зброя давніх часів

У VI столітті до нашої ери ассирійці отруювали колодязі житніми ріжками — смертельно отруйним грибом. Війська Олександра Македонського залишали на ворожій території тіла людей і коней, загиблих від інфекційних захворювань. Скіфські лучники змащували стріли кров’ю і тканинами розкладених трупів, використовуючи трупну отруту як ефективний засіб боротьби. У 1346 році татаро-монголи під час облоги генуезької фортеці Каффа (сучасна Феодосія) катапультували через мури міста тіла померлих від чуми. Наслідком стало розповсюдження епідемії до Константинополя, Генуї, Венеції та інших середземноморських портів, що призвело до пандемії в Європі та на Близькому Сході. Біологічна зброя цього періоду, незважаючи на свою примітивність, забезпечувала масове ураження шляхом використання природних патогенів.

Другий період. Біологічна зброя у Першій та Другій світових війнах

Під час Першої світової війни німецькі агенти транспортували до США пластирі, заражені правцевими паличками, що призвело до спалахів правця. У 1933 році нацистська Німеччина розпочала інтенсивні дослідження біологічної зброї у Воєнному інституті мікробіології в Берліні, зокрема щодо використання збудника сибірки. Було запатентовано численні пристрої для розпилення біологічних агентів.

Під час Другої світової війни японський Загін №731 здійснював біологічні атаки проти Китаю, використовуючи збудників сибірки, холери, шигельозу, сальмонельозу й чуми. У СРСР з початку 1930-х років також велися секретні розробки біологічної зброї: створено 27 наукових установ, 6 виробничих підприємств і 7 резервних заводів. Дослідження охоплювали генну модифікацію бактерій чуми та створення гібридів натуральної віспи з вірусом гарячки Ебола.

У цей період розпочалися систематичні наукові дослідження біологічної зброї, формувалася відповідна інфраструктура, розроблялися методи розпилення патогенів для стратегічного військового застосування.

Третій період. Біологічна зброя в епоху “Холодної війни”

Після Другої світової війни США та СРСР значно розширили свої програми створення біологічної зброї. США здійснювали випробування збудників небезпечних захворювань у реальних умовах, розробляли аерозольні технології поширення патогенів та вивчали вірусні агенти як зброю. З метою тестування механізмів поширення біоагентів у міських умовах було проведено понад 239 секретних експериментів, серед яких операція "Sea-Spray" у Сан-Франциско та розпилення Bacillus atrophaeus у метро Нью-Йорка.

СРСР у 1973 році започаткував програму "Біопрепарат", що під прикриттям цивільних досліджень займалася розробкою смертоносних біологічних агентів. Завдання програми включали генетичну модифікацію патогенів, створення антибіотикостійких штамів та випробування біозброї, зокрема на людях. Продуктивність радянських підприємств дозволяла масово виробляти високоефективні штами збудників, як-от сибірки та вірусу Марбург.

Аварії, що сталися на біологічних об'єктах, такі як витоки віспи на Аралі (1971) та сибірської виразки в Свердловську (1979), свідчать про високу небезпеку біологічних розробок навіть у мирний час. Незважаючи на підписання Женевського протоколу (1925) та Конвенції про заборону біологічної зброї (1972), таємні дослідження тривали.

Четвертий період. Біологічна зброя нового покоління (кінець XX століття — сучасність)

Попри офіційне припинення розробок біологічної зброї США та СРСР у другій половині XX століття, діяльність у цій сфері триває. За даними Державного департаменту США, Росія зберігає біотехнології подвійного призначення і може підтримувати програми наступальної біологічної зброї. Вважається, що КНДР активно працює над біологічною зброєю, а Іран здійснює дослідження у галузі біотехнологій із потенційним військовим застосуванням.

Досягнення генної інженерії зумовили появу нового покоління біологічної зброї, здатної вибірково вражати певні етнічні або расові групи. Сучасні технології дозволяють змінювати ДНК та РНК мікроорганізмів, створюючи патогени з новими властивостями.

Серед природних або випадкових біологічних загроз XXI століття слід відзначити пандемію свинячого грипу (2009–2010), епідемії Еболи (2014–2016, 2018–2020), Близькосхідний респіраторний синдром (з 2012 року) та пандемію COVID-19 (з 2019 року), а також спалах віспи мавп (з 2022 року). Ці події доводять здатність біологічних загроз руйнувати суспільства та вимагати значних ресурсів для подолання наслідків.

Очікується, що зміна клімату сприятиме пришвидшенню появи нових зоонозних захворювань і підвищенню ризику пандемій.

Еволюція біологічних небезпек — від отруєння води до створення генно-інженерних вірусів — свідчить про зростаючу серйозність цієї загрози. Незважаючи на міжнародні заборони, технологічний прогрес підвищує імовірність використання біологічної зброї, що вимагає глобального моніторингу, прозорості наукових досліджень та посилення міжнародного контролю у сфері біотехнологій.

Проведене дослідження еволюції ХБРЯ-небезпек — від перших згадок до сучасності — дозволяє стверджувати, що ці загрози не зникають, а, навпаки, постійно еволюціонують. Прогрес у науково-технічній сфері на кожному етапі змінював характер ХБРЯ-небезпек, роблячи їх дедалі серйознішими: від розщеплення атома до термоядерних бомб мегатонного класу, від отруйних стріл до токсичних речовин четвертого покоління, від трупної отрути до масштабних вірусних пандемій. У сучасних умовах розвиток науки й технологій ще більше розширює спектр потенційних ХБРЯ-загроз, збільшуючи ризики для безпеки людства.

Технології, що викликають особливе занепокоєння в короткостроковій перспективі, включають:

1. Впровадження елементів штучного інтелекту (ШІ). Штучний інтелект суттєво впливає на розширення спектра ХБРЯ загроз [16], підвищуючи можливості як у сфері захисту, так і щодо потенційного застосування нових видів загроз. Використання ШІ дозволяє

розробляти алгоритми для моделювання ефективності ядерних реакцій, що може сприяти створенню нових типів ядерної зброї. Також ШІ застосовується для розробки та синтезу небезпечних хімічних речовин, оптимізації існуючих агентів, прогнозування токсичності сполук і підвищення їх ефективності як засобів хімічного ураження. У біологічній сфері штучний інтелект використовується для редагування ДНК, моделювання вірусів і бактерій, що створює передумови для виникнення нових біологічних загроз. Алгоритми ШІ дозволяють аналізувати геномні дані для прогнозування ефективності патогенів.

2. Зростання ролі безпілотних систем. Безпілотні системи істотно розширюють можливості застосування ХБРЯ агентів, створюючи нові виклики для систем безпеки та захисту [6, 17, 18, 22]. Використання безпілотників для доставки або розпилення небезпечних речовин забезпечує нові способи проведення атак, змінюючи традиційну тактику. Завдяки можливості прихованого транспортування на низьких висотах і в умовах поганої видимості, безпілотні системи ускладнюють виявлення атак та забезпечують рівномірний розподіл ХБР агентів, підвищуючи ефективність зараження. Вони можуть здійснювати прицільні атаки на місця масового скупчення людей або важливі об’єкти інфраструктури, доставляючи радіоактивні матеріали, бактерії, віруси чи токсини у повітря або водні джерела, що підвищує ризик масштабного зараження. Крім того, безпілотні системи можуть збирати розвідувальні дані про ХБР об'єкти для планування диверсій або атак, а також безпосередньо їх уражати, що може призвести до значних екологічних та гуманітарних наслідків.

3. Активне впровадження кібертехнологій. Дії у кіберпросторі створюють можливості для дистанційного впливу на технологічні процеси об'єктів, що працюють із ХБРЯ агентами, а також на їхні системи управління [19]. Кібератаки на об’єкти хімічного виробництва, біотехнологічні центри, лабораторії або системи управління ядерними об'єктами можуть призвести до неконтрольованого викиду небезпечних речовин, що спричинить масштабне зараження навколишнього середовища. Ураження систем управління та охолодження на атомних електростанціях може викликати катастрофи, аналогічні Чорнобильській або Фукусімській. Кібератаки також можуть виводити з ладу системи фізичного захисту об’єктів, відкриваючи можливості для фізичних атак або крадіжки ХБР матеріалів, а також використовуватися для саботажу або шантажу шляхом ураження критично важливих систем.

4. Розвиток технологій 3D-друку (адитивне виробництво). Технології 3D-друку відкривають можливості для виготовлення складних компонентів, зокрема для створення мініатюрних хімічних реакторів, обладнання для синтезу небезпечних речовин, лабораторного обладнання (центрифуг, інкубаторів, мікрофлюїдних систем), а також систем транспортування і розпилення ХБР агентів [21, 22]. Зокрема, за допомогою 3D-принтерів можливо виготовляти компоненти для “брудних бомб” або центрифуг для збагачення урану. Простота використання, відносна дешевизна, децентралізований характер виробництва та складність контролю за поширенням 3D-друкованих елементів створюють серйозні виклики для міжнародної безпеки, особливо у контексті держав, що перебувають під міжнародними санкціями.

5. Темна павутина (даркнет). Темна павутина, або даркнет, є прихованим сегментом Інтернету, доступ до якого здійснюється через спеціалізоване програмне забезпечення і який не індексується традиційними пошуковими системами. Вона слугує платформою для анонімного спілкування та обміну інформацією, пов’язаною з незаконною діяльністю, включаючи обіг матеріалів подвійного призначення, технологій та компонентів для створення ХБРЯ зброї [6]. На ринках даркнету пропонуються на продаж небезпечні матеріали та обладнання, необхідні для виготовлення ХБРЯ засобів. Транзакції зазвичай здійснюються за допомогою криптовалют (зокрема Bitcoin), що ускладнює їхнє відстеження і контролювання з боку правоохоронних органів. Існує також загроза використання даркнету як платформи для об'єднання терористичних груп із фахівцями, які володіють необхідними знаннями для розробки ХБРЯ зброї.

Нанотехнології. Нанотехнології являють собою інноваційну галузь науки, що оперує матеріалами з розмірами в діапазоні від 1 до 100 нанометрів. Завдяки можливості маніпулювання речовинами на молекулярному та атомному рівнях, нанотехнології потенційно розширюють спектр хімічних, біологічних, радіологічних та ядерних (ХБРЯ) загроз. Використання нанотехнологій відкриває можливості для створення ХБРЯ зброї нового покоління, яка характеризується ускладненим виявленням та нейтралізацією. Зокрема, наночастинки здатні підвищувати токсичність хімічних агентів та їхню проникність через захисні бар'єри. Нанокапсули забезпечують контрольоване вивільнення хімічних чи біологічних агентів у визначеному місці або в заданий час. Слід зазначити, що деякі наночастинки мають настільки малі розміри, що їх ідентифікація традиційними методами виявлення ускладнена, що підвищує їхню ефективність у хімічних атаках та ускладнює детекцію й нейтралізацію. Крім того, наночастинки можуть посилювати вірулентність патогенів, підвищуючи їхню стійкість до імунної відповіді організму. Також, зазначені частинки можуть бути використані для створення аерозолів, що містять радіоактивні матеріали, які здатні легко поширюватися та проникати в організм. Наноструктуровані матеріали спрощують створення більш компактної ядерної зброї та дозволяють підвищувати ефективність ядерних боєголовок завдяки покращенню характеристик вибухових речовин. Розвиток нанотехнологій відкриває можливості для створення мініатюрних детекторів ядерних матеріалів, які можуть бути використані для приховування нелегальної ядерної діяльності.

Фізика високих енергій. Фізика високих енергій – це галузь фізики, що досліджує властивості та взаємодію субатомних частинок при надзвичайно високих енергіях [10]. Вона сприяє розвитку сучасних технологій у ядерній енергетиці, військовій промисловості та медицині. Разом із цим, фізика високих енергій також потенційно розширює спектр ХБРЯ загроз.

Експерименти з високими енергіями можуть призводити до утворення хімічних сполук або матеріалів з унікальними властивостями, які можуть бути використані для створення високотоксичних речовин. Дослідження процесів вибуху на рівні молекулярних структур можуть сприяти створенню ефективніших хімічних вибухових пристроїв. Високі енергії можуть викликати мутації у вірусах і бактеріях, що створює можливість для розробки нових біологічних загроз, зокрема стійких і важко контрольованих патогенів. Фізичні методи, що базуються на використанні високих енергій, можуть бути застосовані для створення систем доставки біологічних агентів у аерозольній формі.

Дослідження в галузі фізики високих енергій дозволяють створювати компактні та ефективні ядерні боєголовки, що значно удосконалює ядерну зброю, роблячи її важчою для виявлення та транспортування. Також з'являється можливість удосконалення боєголовок з використанням нового типу детонаційних хвиль, що підвищують потужність вибуху без збільшення розмірів заряду. Використання передових детонаційних технологій підвищує ефективність ядерного вибуху. Зазначена технологія сприятиме покращенню конструкції термоядерних пристроїв (водневих бомб), що використовують ядерний синтез для досягнення значно більшої руйнівної потужності. Фізика високих енергій сприяє створенню "брудних бомб" та нестабільних ізотопів із високою радіоактивністю, які можуть використовуватися для забруднення територій. Завдяки дослідженням із високими енергіями можна розробляти методи для оптимального розсіювання радіоактивних частинок на великих площах.

Квантові технології. Незважаючи на позитивний потенціал для науки та промисловості, квантові технології також можуть розширити спектр ХБРЯ загроз. Квантові комп'ютери здатні моделювати складні ядерні, хімічні та біологічні реакції з високою точністю. Це може сприяти розробці більш ефективних та компактних ядерних боєголовок. Квантові алгоритми дозволяють оптимізувати відомі отруйні агенти з метою підвищення їхньої токсичності або створювати нові високотоксичні хімічні сполуки з новою молекулярною

структурою, що ускладнює їх виявлення існуючими детекторами. За допомогою квантових технологій стає можливим створення нових патогенів із заданими характеристиками, що підвищує ризик біологічної зброї. Квантові комп'ютери можуть порушити безпеку систем управління та контролю над ядерною зброєю. Крім того, за допомогою таких комп'ютерів можуть бути зламані сучасні системи захисту даних, що охороняють інформацію про ядерні технології. Квантові алгоритми, зокрема алгоритм Шора, можуть розшифрувати криптографічні ключі, які використовуються для захисту даних про ядерні технології, що створює загрозу витоку конфіденційної інформації про ядерні програми або іншої секретної інформації про ХБРЯ технології.

Синтетична біологія та біотехнології. Синтетична біологія та біотехнології передбачають використання штучного інтелекту, молекулярної біології, біохімії, інженерії та біоінформатики для моделювання, проектування та синтезу біологічних систем. Передові технології даної сфери можуть спричинити появу нових видів біологічної зброї. Використання штучного інтелекту та генетичних баз даних дозволить розробляти нові агресивні віруси та бактерії, що матимуть більш стійкі характеристики до навколишнього середовища. З розвитком біотехнологій з'являється можливість створення патогенів із високою смертністю або спрямованістю на певні групи населення. Наприклад, одна з програм штучного інтелекту, яка спочатку була розроблена для фармацевтичних досліджень, змогла згенерувати понад 40 000 потенційних нових токсинів всього за шість годин. Модифікація бактерій для стійкості до антибіотиків може зробити лікування інфекцій утрудненим або навіть неможливим. Крім того, існують потенційні можливості використання синтетичної біології для створення бактерій або клітин, які можуть виробляти хімічні отруйні речовини, наприклад, нервово-паралітичні агенти. Генетично модифіковані організми можуть самостійно продукувати такі токсини в природному середовищі, що ускладнює їх виявлення [20].

Використання ХБР агентів подвійного призначення. Хімічні, біологічні та радіаційні речовини, а також технології, що можуть бути використані як у цивільних, так і у військових цілях, визначаються як ХБР агенти подвійного призначення. Їхня амбівалентна природа розширює спектр ХБРЯ загроз, оскільки вони є відносно доступними, складними для контролю та легко адаптуються для створення ХБРЯ зброї. Значна кількість ХБР агентів подвійного призначення легально виробляється та широко використовується у промисловості та науці [20]. Наразі, розмежування між законною діяльністю з цими агентами та прихованою підготовкою до їх використання як ХБРЯ зброї є складним завданням. Розвиток нових методів синтезу, генної інженерії, біотехнологій та хімічного аналізу збільшує ризик та спрощує створення відповідної зброї в лабораторних умовах. Глобалізація суспільства сприяє міжнародним поставкам, що, в свою чергу, зумовлює неконтрольоване поширення ХБР агентів подвійного призначення та полегшує виробництво ХБРЯ зброї.

Як приклади таких ХБРЯ агентів можна навести:

- Фосген – важливий компонент для промислового синтезу пластмас, виробництва пестицидів, барвників, безводних оксидів металів, але також відомий як бойовий отруйний газ.
- Сибірка (*Bacillus anthracis*) – може використовуватися для створення біологічної зброї, але також застосовується у вакцинах та наукових дослідженнях.
- Цезій-137 – використовується для медичних цілей, але може бути використаний для створення радіологічної зброї.
- Центрифуги для збагачення урану – використовуються для виробництва палива для АЕС, але також можуть бути використані для створення збройового урану.

Таким чином, розвиток науково-технічної сфери дозволяє окреслити зміни характеру ХБРЯ загроз та оцінити потенційні ризики та небезпеки, пов'язані з ними, у майбутньому. Впровадження нових технологій значно розширює можливості для створення більш складних

і прихованих ХБРЯ загроз, а також дає змогу визначити потенційні сценарії їхньої реалізації. З огляду на вищезазначене, такі сценарії можуть бути представлені у таблицях 1-3.

Таблиця 1 – Основні сценарії загроз радіаційного та ядерного характеру

Ядерний тероризм	Розробка, виготовлення (в тому числі кустарно), захоплення та застосування ядерної бомби чи ядерного підривного пристрою
	Викрадення, контрабанда або незаконний обіг радіоактивних матеріалів
	Диверсійно-терористичні дії на ядерних об’єктах цивільного та військового призначення (хакерська атака, виведення з ладу технологічного обладнання, захоплення, мінування, вибух)
	Використання (в тому числі приховане) радіоактивних матеріалів чи бойових радіоактивних аерозолів в т.ч брудної бомби
	Поширення технологій виготовлення ядерної зброї чи засобів її доставки
Використання ядерної зброї державними суб’єктами	Навмисне застосування стратегічних ядерних сил
	Навмисне застосування не стратегічних ядерних сил
	Інциденти під час зберігання та поводження з ядерною зброєю
	Бойове зіткнення із застосуванням набоїв з ^{238}U
	Навмисне руйнування радіаційно-небезпечних об’єктів на території іншої держави
Ядерні, радіаційні аварії та інциденти на радіаційно-небезпечних об’єктах	Аварії на АЕС
	Аварії під час перевезення та транспортування радіоактивних матеріалів
	Інциденти під час зберігання та використання радіоактивних матеріалів
	Неконтрольований викид радіоактивних аерозолів
Забруднення навколишнього середовища	Радіоактивне зараження місцевості після ядерних інцидентів
	Розпилення радіоактивних матеріалів в атмосфері
	Розчинення радіоактивних матеріалів в поверхневих чи підземних водах
	Змішування радіонуклідів з харчовими продуктами
Ядерний шантаж для досягнення політичних чи економічних цілей	Прямий ядерний шантаж (загроза безпосереднього застосування ядерної зброї)
	Опосередкований ядерний шантаж (демонстративне підвищення бойової готовності ядерних сил або випробування ядерних боєголовок)
	Ядерний шантаж пов’язаний з радіаційно-небезпечними об’єктами

Таблиця 2 – Основні сценарії загроз хімічного характеру

Аварії та інциденти на хімічно-небезпечних об'єктах	Аварії на хімічно-небезпечних об’єктах
	Аварії чи інциденти під час перевезення та транспортування ОХР, ОНХР, НХР
	Неправильне поводження з ОХР, ОНХР, НХР
Хімічний тероризм	Диверсії на хімічно небезпечних об’єктах (хакерська атака, виведення з ладу технологічного обладнання, захоплення, мінування, вибух)
	Навмисне використання БОР, ОХР, ОНХР, НХР
	Придбання, викрадення, контрабанда або незаконний обіг БОР, ОХР, ОНХР, НХР
	Розробка, виробництво, імпорт БОР, ОХР, ОНХР, НХР (в тому числі хімічних речовин подвійного використання)
	Поширення технологій виготовлення хімічної зброї чи засобів її доставки
Використання хімічної зброї державними суб’єктами	Створення та накопичення хімічної зброї
	Навмисне застосування хімічної зброї
	Інциденти під час зберігання та поводження з хімічною зброєю
	Навмисне руйнування ХНО на території іншої держави
	Забруднення місцевості після хімічних інцидентів (в тому числі і під час та після бойових дій)

Забруднення довкілля хімічними речовинами	Розпилення БОР, ОР, ОХР, ОНХР, НХР, в атмосфері
	Розчинення хімічних речовин у поверхневих та підземних водах
Хімічні катастрофи природного походження (виверження вулканів, підводні викиди нафти, викиди метану)	

Примітки:

БОР – бойові отруйні речовини, спеціально синтезовані або відібрані токсичні хімічні сполуки, призначені для застосування у військових цілях з метою ураження живої сили противника шляхом інгаляційного, шкірного або контактного впливу.

НХР – небезпечна хімічна речовина, що потенційно може завдати шкоду здоров'ю людини та/або довкіллю;

ОНХР – особливо небезпечна хімічна речовина, яка має мутагенні та/або канцерогенні властивості, та/або є токсичною для репродуктивної системи людини, та/або має здатність до руйнування ендокринної системи людини, та/або є стійкою, біоакумулятивною і токсичною для довкілля;

ОХР – отруйна хімічна речовина, яка може спричинити виникнення гострого або відстроченого тяжкого отруєння, яке призводить до хвороб, порушення роботи систем організму або його загибелі, у разі її перорального надходження, потрапляння на шкіру або під час вдихання [24];

ХНО – хімічно-небезпечні об'єкти: підприємства хімічної, нафтопереробної, нафтоперегінної галузі; залізничні станції з парком для відстою потягів з отрутохімікатами; порти; підприємства харчової промисловості; підприємства целюлозно-паперової промисловості; водогінні і водоочисні станції, що використовують хлор (водоканал); підприємства, що використовують холодоагенти; склади та бази із речовинами для дезінфекції, дезінсекції, дератизації; склади з ракетним паливом, ракетні частини із шахтами; лабораторії, науково-дослідні інститути, де використовують НХР; склади та бази для зберігання НХР, отруйних речовин, отрутохімікатів [23].

Таблиця 3 – Основні сценарії загроз біологічного характеру

Аварії та інциденти на біологічно-небезпечних об’єктах	Аварії на біологічно небезпечних об’єктах
	Інциденти під час зберігання та використання біологічних агентів
	Аварії під час перевезення та транспортування біологічних агентів
	Інциденти на природних резервуарах патогенних мікроорганізмів
Природні та штучні спалахи інфекційних хвороб	Епідемія (інфекційне захворювання людини)
	Епізоотія (інфекційне захворювання тварини)
	Епітофітія (інфекційне захворювання рослин)
	Поява нових, мало або невивчених інфекцій
Біологічний тероризм	Диверсії на біологічно-небезпечних об’єктах (хакерська атака, виведення з ладу технологічного обладнання, захоплення, мінування, вибух)
	Навмисне використання патогенів
	Викрадення, контрабанда або незаконний обіг біологічних агентів
	Неправильне поводження з біологічними агентами
	Розробка, виробництво, імпорт, біологічних агентів (в тому числі подвійного використання)
	Поширення технологій виготовлення біологічної зброї чи засобів її доставки
Транскордонне перенесення патогенних мікроорганізмів	Неконтрольоване перенесення патогенних мікроорганізмів людиною
	Неконтрольоване перенесення патогенних мікроорганізмів (зоонозів) твариною
	Розповсюдження біотехнологій подвійного призначення
Забруднення навколишнього середовища біологічними агентами	Біологічне забруднення ґрунтів
	Біологічне забруднення атмосфери
	Біологічне забруднення поверхневих та підземних вод
	Біологічні інвазії
Застосування біологічної зброї державними суб’єктами	Створення або генерація, біологічної зброї
	Відкрите застосування біологічної зброї
	Приховане застосування біологічної зброї
	Гібридне застосування біологічної зброї

	Навмисне руйнування біологічно небезпечних об’єктів на території іншої держави
	Генетичний геноцид

Висновки

На формування сучасного безпекового середовища, окрім політичних, екологічних, демографічних, географічних та економічних факторів, значний вплив має розвиток і доступність новітніх технологій. ХБРЯ сфера не є винятком. Прискорене впровадження технологічного прогресу в цій галузі ставить під сумнів попередні оцінки ризиків, пов’язаних із ХБРЯ загрозами.

Проведений аналіз еволюції ХБРЯ небезпек демонструє, що вони були, є і залишаються постійною загрозою протягом історії людства – як під час збройних конфліктів, так і в мирний час, незважаючи на відносну стриманість та міжнародні угоди. Глобальна і регіональна загроза ХБРЯ агентів зростає через розширення можливостей випадкового вивільнення або навмисного застосування всупереч світовому порядку, заснованому на правилах, а також через зловмисне використання технологій подвійного призначення.

Новітні технології трансформували всі аспекти життєдіяльності. Водночас, вони можуть бути не лише засобами реалізації потенційних ХБРЯ загроз, але й відігравати ключову роль у запобіганні, виявленні та реагуванні на ці загрози.

В епоху постійної еволюції загроз, здатність ефективно реагувати на них є надзвичайно важливою. У цьому контексті технологічний розвиток відкриває широкі можливості для посилення ХБРЯ захисту шляхом впровадження нових, вдосконалених та економічно ефективних рішень, що є запорукою безпеки та оперативного реагування на сучасні ХБРЯ загрози. Використання штучного інтелекту та аналізу великих даних сприятиме прогнозуванню можливих атак із застосуванням ХБРЯ агентів та оптимізації заходів реагування. Роботизовані системи та безпілотні апарати можуть стати ефективним інструментом для виявлення та реагування на ХБРЯ інциденти, виконуючи небезпечні завдання дистанційно, забезпечуючи підвищений рівень безпеки як для військовослужбовців, так і для цивільного населення. Інноваційні підходи до дезактивації та нейтралізації забруднень забезпечать ефективніше усунення загроз. ХБРЯ захист необхідно розглядати як інтегровану систему з взаємозалежними компонентами. Окремі сили, засоби та технології повинні оцінюватися з точки зору їхнього впливу на всю систему ХБРЯ захисту, а також на інші оборонні сили та засоби, а не розглядатися ізольовано. Розвиток ХБРЯ сил і засобів має бути невід’ємною частиною оборонного планування та забезпечувати державі надійний інструмент для протидії новітнім загрозам [8].

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Nikolay I. Padarev. Chemical, biologycal, radiologycal and nuclear threats in the hybrid war context. International scientific journal “Science, business, society”. WEB ISSN 2534-8485. 2019. Republic of Bulgaria. P.118-119.
2. NATO’s Chemical, Biological, Radiological and Nuclear (CBRN) Defence. NATO 2022. URL: https://www.nato.int/cps/fr/natohq/official_texts_197768.htm?selectedLocale=e [дата звернення 19.02.25].

3. Su, F., Anthony, I. Reassessing CBRN. Threats in a Changing Global Environment. Stockholm international peace research institute. June 2019. URL: https://www.jstor.org/stable/resrep24499 [дата звернення 26.02.25].
4. Condition (10)(C) Annual Report on Compliance with the Chemical Weapons Convention (CWC). Report. Bureau of Arms Control. April 4, 2024. URL: https://www.state.gov/condition-10c-annual-report-on-compliance-with-the-chemical-weapons-convention-cwc/ [дата звернення 10.02.25].
5. Porter, J. G. Russian Chemical and Biological Weapons: Limiting the Effects of Russian CBW Programs on NATO Security Through 2035. Missouri State University. 2024. URL: https://bearworks.missouristate.edu/cgi/viewcontent.cgi?article=4986&context=theses [дата звернення 12.02.25].
6. Rimpler-Schmid, A., Trapp, R., Leonard, S., Kaunert, C., Dubucq, Y., Lefebvre, C., Mohn, H. EU preparedness and responses to Chemical, Biological, Radiological and Nuclear (CBRN) threats. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653645/EXPO_STU(2021)653645_EN.pdf [дата звернення 15.12.24].
7. Tin, D., Cheng, L., Shin, H., Hata, R., Granholm, F., Braitberg, G. A Descriptive Analysis of the Use of Chemical, Biological, Radiological, and Nuclear Weapons by Violent Non-State Actors and the Modern-Day Environment of Threat. Prehosp Disaster Med. 2023.38(3). P.395–400. https://doi.org/10.1017/S1049023X23000481.
8. Bjerkeseth L. Vitenskapelige og teknologiske fremskritts innvirkning pi CBRN-vern frem mot 2030 - konklusjoner fra en langtidsstudie i regi av NATO Science & Technology Organization. FFI-RAPPORT 22/002472. URL: https://www.ffi.no/en/publications-archive/vitenskapelige-og-teknologiskefremskritts-innvirkning-pa-cbrnvern-frem-mot-2030konklusioner-fra-en-langtidsstudie-i-regi-av-nato-science-technology-organization. [дата звернення 19.12.24].
9. Reding, D.F., Eaton, J. Science & Technology Trends 2020-2040. NATO Science & Technology Organization. Brussels, Belgium. 2020. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422ST_Tech_Trends_Report_2020-2040.pdf [дата звернення 09.01.25].
10. Гасанов, А., Тахіров, Р., & Іскандаров, Х. (2024). Майбутнє війни. Передбачувані зміни у військових трендах. *Social Development and Security*, *14*(5), 1-18. https://doi.org/10.33445/sds.2024.14.5.1.
11. Gichki, A. A. The Evolution of Nuclear Weapons: From Battlefield Tools to Political Instruments. Modern Diplomacy. 2024. URL: https://moderndiplomacy.eu/2024/07/20/the-evolution-of-nuclear-weapons-from-battlefield-tools-to-political-instruments/ [дата звернення 14.01.25].
12. Park, S. How Have Nuclear Weapons Evolved Since Oppenheimer and the Trinity Test? 2023. URL: https://blog.ucs.org/sulgiye-park/how-have-nuclear-weapons-evolved-since-oppenheimer-and-the-trinity-test/ [дата звернення 14.01.25].
13. Дядченко В., Петрухін Ю., Новіков О. Бойові токсичні хімічні речовини. Підручник у 3 т. Т. 1. Хімічна зброя. Х.: ФОП Бровін О.В.,2018. С.532. ISBN 978-617-7555-31-4.
14. Ніколаєнко Н. Біологічна зброя як зброя терору сучасного світу. Філософський альманах. 2018. Випуск 3–4 (165–166) С. 67-75. https://doi.org/10.35423/2078-8142.2018.3-4.06.
15. Benolli, F., Guidotti, M., Bisogni, F. The CBRN Threat. Perspective of an Interagency Response. Advanced Sciences and Technologies for Security Applications. URL: https://link.sprinRer.com/chapter/10.1007/978-3-03Q-42523-4 [дата звернення 13.12.24].
16. Bhatia, R. T. AI CBRN Risks: Governance Lessons from the Most Dangerous Misuses of AI. 2024. URL: https://www.credo.ai/blog/ai-cbrn-risks-governance-lessons-from-the-most-dangerous-misuses-of-ai [дата звернення 13.12.24].
17. Patrick F. Walsh. Evolving chemical, biological, radiological and nuclear (CBRN) terrorism. Intelligence community response and ethical challenges National Security Intelligence and Ethics P.261-279.

https://doi.org/10.4324/9781003164197-23 [дата звернення 13.12.24].
18. Nintanavongsa, P., Pitimon, I. On the Threat of Unmanned Aerial Vehicle as Weapon of Mass Destruction. *Information Technology Journal*. Vol. 16, No. 2. 2020. 1-9 с.
19. Abaimov, S., Martellini, M. Selected Issues of Cyber Security Practices in CBRNeCy Critical Infrastructure. Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges. Threats and Counter Efforts. Terrorism, Security, and Computation. Switzerland. 2017. C.11-35. https://doi.org/10.1007/978-3-319-62108-1.
20. Schmidt, R., Schmidt, J. Chemical, biological, radiological and nuclear threats: the herculean challenge of modern toxikons. Journal of High Threat & Austere Medicine. 2024. 6(1):1-3. Australia. https://doi.org/10.33235/JHTAM.6.1.1-3 [дата звернення 17.12.24].
21. Kaszeta, D. Horizon scanning the future of CBRN threats. 7. October 2024 URL: https://euro-sd.com/2024/10/articles/40656/horizon-scanning-the-future-of-cbrn-threats/ [дата звернення 24.02.25].
22. Cetina i. Impact of the New Technologies on CBRN Terrorist Threats: General Perspective and Perspective of Republic of Croatia. *Vojenske rozhledy*. 2022. №4. P.119-134. https://doi.org/10.3849/2336-2995.31.2022.04,119-139.
23. Поплавець, С., Гузченко, С., Воробйов, О., Авраменко, О., & Шумейко, В. (2022). Можливий підхід щодо визначення раціонального складу сил та засобів радіаційного, хімічного, біологічного захисту для виконання заходів в умовах радіоактивного та хімічного зараження. *Social Development and Security*, *12*(5), 130-146. https://doi.org/10.33445/sds.2022.12.5.12
24. Про забезпечення хімічної безпеки та управління хімічною продукцією: Закон України. Відомості Верховної Ради. 2023. № 55. ст.161.
25. Устінова Л., Сагло В., Баркевич В., Курділь Н., Євтодьєв О., Каплюк О. Актуальні питання медичного захисту військовослужбовців Збройних сил України від бойових отруйних речовин. Медицина невідкладних станів. No 8 (103), 2019. Київ. С. 72-80. https://doi.org/10.22141/2224-0586.8.103.2019.192375.

References

1. Nikolay I. Padarev. Chemical, biologycal, radiologycal and nuclear threats in the hybrid war context. International scientific journal “Science, business, society”. WEB ISSN 2534-8485. 2019. Republic of Bulgaria. P.118-119.
2. NATO’s Chemical, Biological, Radiological and Nuclear (CBRN) Defence. NATO 2022. Available from : https://www.nato.int/cps/fr/natohq/official_texts_197768.htm?selectedLocale=e [дата звернення 19.02.25].
3. Su, F., Anthony, I. Reassessing CBRN. Threats in a Changing Global Environment. Stockholm international peace research institute. June 2019. Available from : https://www.jstor.org/stable/resrep24499 [дата звернення 26.02.25].
4. Condition (10)(C) Annual Report on Compliance with the Chemical Weapons Convention (CWC). Report. Bureau of Arms Control. April 4, 2024. Available from : https://www.state.gov/condition-10c-annual-report-on-compliance-with-the-chemical-weapons-convention-cwc/ [дата звернення 10.02.25].
5. Porter, J. G. Russian Chemical and Biological Weapons: Limiting the Effects of Russian CBW Programs on NATO Security Through 2035. Missouri State University. 2024. Available from : https://bearworks.missouristate.edu/cgi/viewcontent.cgi?article=4986&context=theses [дата звернення 12.02.25].
6. Rimpler-Schmid, A., Trapp, R., Leonard, S., Kaunert, C., Dubucq, Y., Lefebvre, C., Mohn, H. EU preparedness and responses to Chemical, Biological, Radiological and Nuclear (CBRN) threats. Available from :

https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653645/EXPO_STU(2021)653645_EN.pdf [дата звернення 15.12.24].

7. Tin, D., Cheng, L., Shin, H., Hata, R., Granholm, F., Braitberg, G. A Descriptive Analysis of the Use of Chemical, Biological, Radiological, and Nuclear Weapons by Violent Non-State Actors and the Modern-Day Environment of Threat. Prehosp Disaster Med. 2023.38(3). P.395–400. https://doi.org/10.1017/S1049023X23000481.
8. Bjerkeseth L. Vitenskapelige og teknologiske fremskritts innvirkning pi CBRN-vern frem mot 2030 – konklusjoner fra en langtidsstudie i regi av NATO Science & Technology Organization. FFI-RAPPORT 22/002472. Available from : https://www.ffi.no/en/publications-archive/vitenskapelige-og-teknologiskefremskritts-innvirkning-pa-cbrnvern-frem-mot-2030konklusioner-fra-en-langtidsstudie-i-regi-av-nato-science-technology-organization. [дата звернення 19.12.24].
9. Reding, D.F., Eaton, J. Science & Technology Trends 2020-2040. NATO Science & Technology Organization. Brussels, Belgium. 2020. Available from : https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422ST_Tech_Trends_Report_2020-2040.pdf [дата звернення 09.01.25].
10. Hasanov, A., Tahirov, R., & Iskandarov, K. (2024). The future of warfare. Anticipated changes in military trends. *Social Development and Security*, *14*(5), 1-18. https://doi.org/10.33445/sds.2024.14.5.1
11. Gichki, A. A. The Evolution of Nuclear Weapons: From Battlefield Tools to Political Instruments. Modern Diplomacy. 2024. Available from : https://moderndiplomacy.eu/2024/07/20/the-evolution-of-nuclear-weapons-from-battlefield-tools-to-political-instruments/ [дата звернення 14.01.25].
12. Park, S. How Have Nuclear Weapons Evolved Since Oppenheimer and the Trinity Test? 2023. Available from : https://blog.ucs.org/sulgiye-park/how-have-nuclear-weapons-evolved-since-oppenheimer-and-the-trinity-test/ [дата звернення 14.01.25].
13. Dyadchenko, V., Petrukhin, Y., Novikov, O. Chemical warfare agents. Textbook in 3 volumes. Vol. 1: Chemical weapons. Kh. FOP Brovin O.V. 2018. C.532. ISBN 978-617-7555-31-4
14. Nikolaienko, N. (2018). Biological weapons as weapons of terror of the modern world. *Multiversum. Philosophical Almanac*, (3-4), 67-75. https://doi.org/10.35423/2078-8142.2018.3-4.06
15. Benolli, F., Guidotti, M., Bisogni, F. The CBRN Threat. Perspective of an Interagency Response. Advanced Sciences and Technologies for Security Applications. Available from : https://link.sprinRer.com/chapter/10.1007/978-3-03Q-42523-4 [дата звернення 13.12.24].
16. Bhatia, R. T. AI CBRN Risks: Governance Lessons from the Most Dangerous Misuses of AI. 2024. Available from : https://www.credo.ai/blog/ai-cbrn-risks-governance-lessons-from-the-most-dangerous-misuses-of-ai [дата звернення 13.12.24].
17. Patrick F. Walsh. Evolving chemical, biological, radiological and nuclear (CBRN) terrorism. Intelligence community response and ethical challenges National Security Intelligence and Ethics P.261-279. https://doi.org/10.4324/9781003164197-23 [дата звернення 13.12.24].
18. Nintanavongsa, P., Pitimon, I. On the Threat of Unmanned Aerial Vehicle as Weapon of Mass Destruction. *Information Technology Journal*. Vol. 16, No. 2. 2020. 1-9 c.
19. Abaimov, S., Martellini, M. Selected Issues of Cyber Security Practices in CBRNeCy Critical Infrastructure. Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges. Threats and Counter Efforts. Terrorism, Security, and Computation. Switzerland. 2017. C.11-35. https://doi.org/10.1007/978-3-319-62108-1.
20. Schmidt, R., Schmidt, J. Chemical, biological, radiological and nuclear threats: the herculean challenge of modern toxikons. Journal of High Threat & Austere Medicine. 2024. 6(1):1-3. Australia. https://doi.org/10.33235/JHTAM.6.1.1-3 [дата звернення 17.12.24].

21. Kaszeta, D. Horizon scanning the future of CBRN threats. 7. October 2024 Available from : https://euro-sd.com/2024/10/articles/40656/horizon-scanning-the-future-of-cbrn-threats/ [дата звернення 24.02.25].
22. Cetina i. Impact of the New Technologies on CBRN Terrorist Threats: General Perspective and Perspective of Republic of Croatia. *Vojenske rozhledy*. 2022. №4. P.119-134. https://doi.org/10.3849/2336-2995.31.2022.04,119-139.
23. Poplavetz, S., Huzchenko, S., Vorobiov, O., Avramenko, O., & Shumeiko, V. (2022). A possible approach to determining the rational composition of forces and means of radiation, chemical, biological protection for performing measures in conditions of radioactive and chemical contamination. *Social Development and Security*, *12*(5), 130-146. https://doi.org/10.33445/sds.2022.12.5.12
24. "Law of Ukraine 'On Ensuring Chemical Safety and Management of Chemical Products'. Bulletin of the Verkhovna Rada. 2023. No. 55. p. 161.
25. Ustinova, L., Saglo, V., Barkevich, V., Kurdil, N., Yevtodiev, A., & Kaplyuk, O. (2019). Current problems of the health protection of Ukrainian Armed Forces servicemen from military toxic agents. *EMERGENCY MEDICINE*, (8.103), 72–80. https://doi.org/10.22141/2224-0586.8.103.2019.192375

Система управління евакуацією населення під час надзвичайних ситуацій

Emergency Evacuation Management System

Олег Башинський [A]

Corresponding author: к.тех.н., доцент, доцент кафедри наглядово-профілактичної діяльності та пожежної автоматики, e-mail: malinovskaya.yuliya2017@gmail.com, ORCID: 0000-0002-0243-7519

Марта Пелешко [A]

к.тех.н., доцент, доцент кафедри наглядово-профілактичної діяльності та пожежної автоматики, e-mail: malinovskaya.yuliya2017@gmail.com, ORCID: 0000-0002-9315-1590

Тарас Бережанський [A]

к.тех.н., доцент, доцент кафедри наглядово-профілактичної діяльності та пожежної автоматики, e-mail: malinovskaya.yuliya2017@gmail.com, ORCID: 0000-0002-1290-706X

Андрій Беседа [A]

науковий співробітник відділу організації науково-дослідної діяльності науково-дослідного центру, e-mail: malinovskaya.yuliya2017@gmail.com, ORCID: 0009-0004-6252-1431

Oleh Bashynskyi [A]

Corresponding author: Candidate of Engineering Sciences, Associate Professor, Associate Professor of the Department, e-mail: malinovskaya.yuliya2017@gmail.com, ORCID: 0000-0002-0243-7519

Marta Peleshko [A]

Candidate of Engineering Sciences, Associate Professor, Associate Professor of the Department, e-mail: malinovskaya.yuliya2017@gmail.com, ORCID: 0000-0002-9315-1590

Taras Berezhanskyi [A]

Candidate of Engineering Sciences, Associate Professor, Associate Professor of the Department, e-mail: malinovskaya.yuliya2017@gmail.com, ORCID: 0000-0002-1290-706X

Andrii Beseda [A]

Researcher of the Department of Organization of Scientific and Research Activities of the Scientific and Research Center, e-mail: malinovskaya.yuliya2017@gmail.com, ORCID: 0009-0004-6252-1431

[A] Львівський державний університет безпеки життєдіяльності, Львів, Україна

[A] Lviv State University of Life Safety, Lviv, Ukraine

Received: March 12, 2025 | Revised: April 23, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.11

Мета роботи: є дослідження сучасних підходів до організації евакуації населення в умовах надзвичайних ситуацій природного, техногенного та воєнного характеру. Робота спрямована на виявлення ключових викликів у сфері управління евакуаційними заходами та розробку рекомендацій для підвищення їхньої ефективності.

Метод дослідження: методи системного аналізу, моделювання та синтезу.

Результати дослідження: Розроблено структурну модель управління евакуацією, яка включає спеціалізовані органи, такі як евакуаційні комісії та пункти, а також автоматизовані підсистеми для моніторингу й реагування. Доведено, що гнучкі способи евакуації (одночасний, послідовний, вибірковий, комбінований) дозволяють мінімізувати ризики залежно від типу та масштабу надзвичайної ситуації.

Теоретична цінність дослідження: Робота розширює теоретичні основи управління евакуаційними процесами шляхом класифікації рівнів реагування та факторів, що впливають на поведінку людей під час евакуації, зокрема часу, щільності скупчення та відстані до виходу. Запропоновано математичну модель для оцінки критичного рівня паніки, що збагачує розуміння психоемоційних аспектів у кризових ситуаціях.

Практична цінність дослідження: Рекомендації, розроблені в статті, можуть бути використані органами влади для вдосконалення планування та реалізації евакуаційних заходів на національному та регіональному рівнях. Запропонована модель управління евакуацією з інтеграцією автоматизованих систем підвищує оперативність реагування та безпеку населення. Результати дослідження корисні для розробки нормативних документів і підготовки спеціалізованих служб до дій у надзвичайних ситуаціях.

Тип статті: теоретичний з практичними рекомендаціями.

Purpose: is to study modern approaches to organizing the evacuation of the population in conditions of natural, man-made and military emergencies. The work is aimed at identifying key challenges in the field of managing evacuation measures and developing recommendations to increase their effectiveness.

Method: Methods of system analysis, modeling and synthesis.

Findings: It was established that an effective evacuation system involves clear planning and coordination of the movement of the population from dangerous areas, taking into account their professional, educational or territorial affiliation. A structural model of evacuation management was developed, which includes specialized bodies, such as evacuation commissions and points, as well as automated subsystems for monitoring and response. It is proven that flexible evacuation methods (simultaneous, sequential, selective, combined) allow minimizing risks depending on the type and scale of the emergency.

Theoretical implications: The work expands the theoretical foundations of evacuation process management by classifying response levels and factors affecting people's behavior during evacuation, in particular time, crowd density and distance to the exit. A mathematical model is proposed for assessing the critical level of panic, which enriches the understanding of psycho-emotional aspects in crisis situations.

Practical implications: The recommendations developed in the article can be used by authorities to improve the planning and implementation of evacuation measures at the national and regional levels. The proposed evacuation management model with the integration of automated systems increases the efficiency of response and the safety of the population. The results of the study are useful for developing regulatory documents and preparing specialized services for action in emergency situations.

Paper type: theoretical with practical recommendations.

Ключові слова: евакуація населення, управління надзвичайними ситуаціями, цивільний захист, система оповіщення, логістика евакуації, технології у кризовому управлінні.

Key words: population evacuation, emergency management, civil protection, warning system, evacuation logistics, technologies in crisis management.

Вступ

Актуальність дослідження системи управління евакуацією населення під час надзвичайних ситуацій (НС) є надзвичайно важливою, особливо з огляду на сучасні загрози, з якими стикається Україна. Постійне зростання кількості кризових ситуацій природного, техногенного та воєнного характеру підкреслює необхідність створення ефективних механізмів захисту населення. Евакуація є одним із ключових заходів цивільного захисту, що спрямований на організоване виведення людей із зон небезпеки для збереження їхнього життя та здоров'я. Цей процес передбачає не лише переміщення населення, а й забезпечення його розміщення в безпечних районах з належними умовами для проживання. Ефективне управління евакуаційними заходами потребує чіткої координації дій державних органів, своєчасного оповіщення населення, а також наявності детальних планів евакуації. Законодавчі норми, зокрема стаття 33 Кодексу цивільного захисту України та постанова Кабінету Міністрів України № 841 від 30.10.2013, регламентують порядок проведення евакуації на державному рівні (Кодекс цивільного захисту України, 2013). Отже, дослідження механізмів управління евакуацією є надзвичайно важливим для гарантування безпеки громадян, мінімізації людських жертв та зниження матеріальних втрат під час кризових ситуацій. Вдосконалення та впровадження ефективних систем евакуації є стратегічно важливим завданням для забезпечення національної безпеки та сталого розвитку держави.

Теоретичні основи дослідження

У широкому розумінні евакуація населення – це комплекс заходів, спрямованих на організоване переміщення людей, а також матеріальних і культурних цінностей із зон загрози до безпечних територій. Вона проводиться у разі виникнення військових конфліктів, стихійних лих, техногенних аварій та інших надзвичайних ситуацій, що можуть створювати загрозу життю та здоров'ю населення (Потеряйко, Бєлікова, Твердохліб, 2022). Як визначають (Снагощенко, 2020) та (Idoudi, Li, Ameli, González, 2024) ефективність системи евакуації залежить від оперативності прийняття рішень, координації дій відповідних органів управління, а також від готовності населення до швидкого переміщення в умовах кризи. До основних складових евакуаційних заходів, згідно наукових доробків (Клименко, 2022), (Havrys, Khlevnoi, 2022) належать: переміщення населення із зон можливих небезпек у заздалегідь визначені безпечні райони, які розташовані поза межами впливу руйнівних факторів джерела надзвичайної ситуації; організоване виведення працівників підприємств та організацій з територій, що зазнають негативного впливу надзвичайної ситуації, із забезпеченням безперервності критично важливих процесів та функцій держави; відселення населення, яке може бути тимчасовим (з поверненням після усунення наслідків надзвичайної ситуації) або постійним (у разі неможливості відновлення безпечних умов для життя); реевакуація, тобто повернення евакуйованих осіб до місць постійного проживання після нормалізації ситуації та завершення відновлювальних заходів.

Організаційні аспекти управління евакуацією розглядаються у праці (Geng, 2024), де підкреслюється важливість міжвідомчої координації, планування логістичних ресурсів та підготовки населення до можливих надзвичайних ситуацій. Автори наголошують, що ефективність евакуації значною мірою залежить від попередньої підготовки, регулярних навчань та взаємодії між місцевими та центральними органами влади.

Постановка проблеми

В умовах зростаючої кількості надзвичайних ситуацій природного, техногенного та військового характеру, що загрожують життю та здоров'ю населення, питання ефективної організації та управління евакуаційними заходами набуває особливої актуальності. Система управління

евакуацією населення потребує вдосконалення, включаючи застосування сучасних цифрових технологій, розширення механізмів міжвідомчої взаємодії та створення гнучких моделей евакуаційного процесу, які можна адаптувати до різних сценаріїв розвитку надзвичайних ситуацій.

Мета статті – дослідження підходів до організації евакуації населення, визначення основних викликів у сфері управління евакуаційними заходами та розробка рекомендацій щодо підвищення рівня ефективності управління процесами евакуації населення при настанні надзвичайної ситуації.

Методологія дослідження

Використано системний підхід, який передбачає вивчення принципів планування, організації та реалізації евакуаційних заходів з урахуванням виробничо-територіального принципу. Дослідження охопило різні категорії населення (працівники, студенти, мешканці), а також специфіку координації евакуаційних процесів територіальними органами виконавчої влади та спеціалізованими евакуаційними органами, такими як евакуаційні комісії, збірні та приймальні евакуаційні пункти (ЗЕП і ПЕП), проміжні пункти евакуації тощо. Особливу увагу приділено класифікації евакуаційних заходів за рівнями реагування (об’єктова, міська, регіональна, міжрегіональна) та способами їх проведення (одночасний, послідовний, вибірковий, комбінований).

Методологічною основою для оцінки ефективності запропонованих рішень став аналіз концептуальних моделей евакуаційних систем, доповнений порівняльним вивченням їхніх управлінських особливостей і очікуваної результативності. У процесі дослідження використано методи системного аналізу, моделювання та синтезу, що дозволили обґрунтувати доцільність інтеграції управлінських заходів та визначити оптимальні підходи до організації евакуації в умовах різних типів надзвичайних ситуацій.

Результати

В умовах виникнення надзвичайних ситуацій природного, техногенного або воєнного характеру система управління евакуацією населення передбачає чітке планування, організацію та реалізацію заходів з переміщення громадян із небезпечних зон відповідно до виробничо-територіального принципу, що регламентує порядок евакуації різних категорій населення залежно від їхнього місця роботи, навчання або проживання. Зокрема, організоване вивезення чи виведення працівників підприємств, установ та організацій, а також студентів вищих навчальних закладів, учнів середніх спеціальних навчальних закладів та професійно-технічних училищ здійснюється безпосередньо за місцем їхньої професійної або освітньої діяльності під керівництвом відповідних адміністративних органів та керівництва установ. В той самий час евакуаційні заходи для решти населення, яке не залучене до виробничої чи сервісної сфери, проводяться за місцем їхнього постійного проживання і координуються відповідними територіальними органами виконавчої влади, які забезпечують організацію переміщення громадян у безпечні райони (Македон, 2012).

Окремим елементом надійного функціонування системи евакуації є те, що заходам переміщення підлягають усі особи, які перебувають у зоні потенційної небезпеки, незалежно від того, чи є вони місцевими мешканцями, працівниками чи випадковими перехожими, адже головним завданням є збереження людських життів і мінімізація ризиків для здоров’я. Виняток становлять ті громадяни, для яких передбачена можливість перебування у захисних спорудах за місцем їхнього розташування, що зменшує необхідність їхнього переміщення, а також особи, які через стан здоров’я є нетранспортабельними й потребують спеціального підходу до організації їхньої безпеки.

З метою ефективного управління процесами евакуації та забезпечення організованого переміщення населення в умовах надзвичайних ситуацій створюється комплексна система спеціалізованих евакуаційних органів, які координують усі етапи евакуаційного процесу та здійснюють контроль за своєчасним виконанням заходів. До основних складових такої системи належать евакуаційні комісії, збірні евакуаційні пункти (ЗЕП), приймальні евакуаційні пункти (ПЕП), проміжні пункти евакуації, адміністрації пунктів посадки та висадки евакуйованих осіб, евакоприймальні комісії, а також групи управління на маршрутах евакуації, які забезпечують контроль за рухом транспортних колон і регулюють оперативні зміни маршрутів у разі виникнення непередбачених ускладнень або загроз (Wu, Nie, Zeng, Cheng, Pan, Han, Hosamo, 2024).

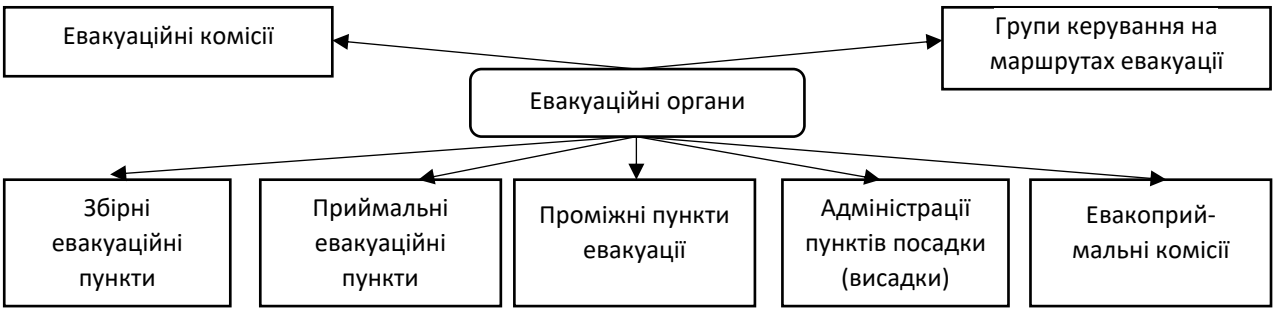


Рисунок 1 – Порядок управлінської взаємодії органів евакуації населення при настанні надзвичайних ситуацій

Джерело: сформовано на основі (Комяк, Кязімов, 2020; Idoudi, Li, Ameli, González, 2024)

Основним завданням цих органів є створення належних умов для швидкого, організованого та безпечного переміщення населення із зон можливих небезпек у заздалегідь визначені безпечні райони, що мінімізує ризики для життя та здоров'я громадян. У містах, які мають особливе стратегічне значення або віднесені до певних категорій за рівнем небезпеки в рамках системи цивільного захисту, формуються спеціалізовані евакуаційні комісії, які відповідають за координацію всіх евакуаційних заходів, а також функціонують збірні евакуаційні пункти (ЗЕП), що є проміжними локаціями для збору та організації переміщення осіб, які підлягають евакуації.

У свою чергу, у регіонах, визначених як безпечні зони, розгортаються приймальні евакуаційні пункти (ПЕП), призначені для прийняття та первинного розміщення евакуйованого населення перед їх подальшою дислокацією у житлових будівлях, адміністративних установах або спеціально підготовлених тимчасових поселеннях. Особлива увага при цьому приділяється ефективній організації транспортування осіб, які не мають можливості самостійно дістатися до безпечних зон, що включає використання спеціального транспорту, визначення оптимальних маршрутів та забезпечення безперебійного руху колони евакуаційного транспорту в умовах можливих обмежень на дорогах (Abioye, Dulebenets, Ozguven, Moses, Boot, Sando, 2020).

Ефективна система управління евакуацією населення під час надзвичайних ситуацій вимагає комплексного підходу, що включає моніторинг небезпек, координацію дій та інтеграцію автоматизованих підсистем. На рисунку представлена структура такої системи, яка складається з ключових компонентів, що забезпечують контроль за температурним режимом електроустановок, будівельними конструкціями та трафіком відвідувачів. Центральна підсистема управління відповідає за моніторинг пожежної безпеки, оповіщення та евакуацію населення. Крім того, автоматизовані механізми пожежогасіння, димовидалення та управління евакуаційними маршрутами сприяють мінімізації ризиків та оперативному

реагуванню у критичних ситуаціях (рис. 2.) (Havrys, Khlevnoi, 2022). У разі виникнення надзвичайних ситуацій природного чи техногенного походження на території населеного пункту чи регіону процес евакуації повинен бути чітко регламентованим, з урахуванням рівня небезпеки, можливих наслідків для життєдіяльності населення та доступності безпечних районів для його розміщення. Локальна евакуація застосовується у випадках, коли зона впливу небезпечних факторів надзвичайної ситуації обмежена територією, що охоплює одну або кілька організацій, а її наслідки не поширюються на значні територіальні масиви. У такому випадку евакуаційні заходи стосуються переважно працівників підприємств та установ, які можуть бути оперативно переміщені до заздалегідь визначених безпечних місць у межах населеного пункту або його околиць, мінімізуючи таким чином загрозу для їхнього життя та здоров'я (Муконін, 2024).

На процес виникнення та поширення паніки у людей у процесі евакуації у разі НС може впливати зовнішнє середовище, а також поведінка інших людей, що евакуюються. У роботі показано, що рівень психоемоційного стану або ступеня паніки евакуйованих може залежати від трьох основних факторів:

- час знаходження на території евакуації *t*;
- щільність скупчення людей *D*;
- відстань до виходу *l.*

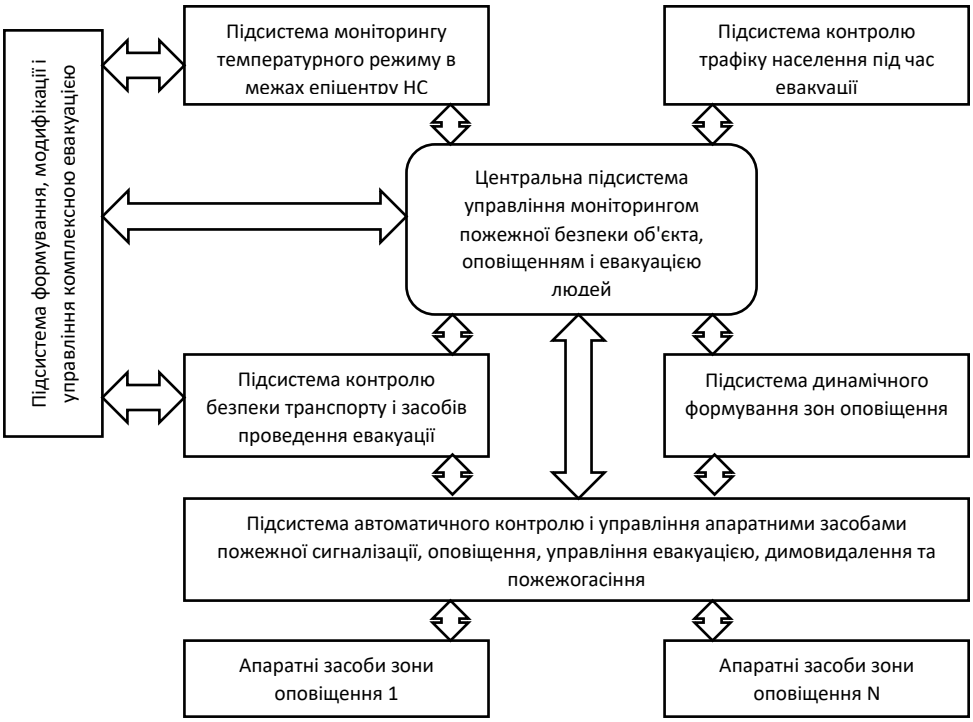


Рисунок 2 – Структурна модель системи управління евакуацією населення під час надзвичайних ситуацій

Джерело: сформовано авторами

Вплив даних факторів пропонується описати відповідними монотонно зростаючими функціями $f_1(t)$, $f_2(D)$, $f_3(l)$, оскільки очевидно, що почуття страху, а значить і панічного стану в евакуйованого не зменшується при розвитку критичної ситуації (Idoudi, Li, Ameli, González, 2024).

У моделі пропонується зробити ще одне припущення, що полягає в тому, що існує певний критичний час t_c з відповідним значенням функції $f_1(t_c)$, для якої в випадку $t < t_c$ час

перебування людей у критичній ситуації ще незначно і недостатньо, щоб вони почали входити в панічний стан та виявляти відповідну реакцію. Якщо ж $t > t_c$, то вже можливий прояв у панічного стану, що евакуюється. Час, коли починає проявлятися панічна реакція в евакуйованих, може бути визначено на основі порогового рівня паніки P_L:

$$\begin{cases} P_L = \min(f_1(t_c), f_2(D_c), f_3(l_c)) \\ f_1(t) = (1 + e^{-\left(\frac{10.6t}{t_{max}} - 5.3\right)})^{-1}, \ 0 \le f_1(t) \le 1 \\ f_2(D) = (1 + e^{-\left(\frac{10.6D}{D_{max}} - 5.3\right)})^{-1}, \ 0 \le f_2(D) \le 1 \\ f_3(l) = (1 + e^{-\left(\frac{10.6l}{l_{max}} - 5.3\right)})^{-1}, \ 0 \le f_3(l) \le 1 \end{cases} \quad (1)$$

де t_c – критичний час, значення якого дорівнює 60 секунд, до якого не починається процес евакуації і, отже, прояв можливої панічної реакції в евакуйованих;

D_c – критичне значення щільності, яке встановлюється на рівні 3,4 (ч/м^2);

l_c – критичну відстань до виходу, тобто. відстань від виходу до точки, від якої той, хто евакуюється, вже точно не заблукає і зможе гарантовано переміститися назовні;

t_{max} – максимально допустиме значення часу перебування людей, яка є прогнозованим часом до початку впливу небезпечних факторів;

D_{max} – максимально допустиме значення густини, яке встановлено на рівні 5,0 (ч/м^2);

l_{max} – максимально можливе значення відстані до виходу, яке є відстанню від найдальшої точки розташування до виходу.

Зазвичай евакуйоване населення розміщується у безпечних регіонах, що територіально прилягають до зони надзвичайної ситуації, оскільки це дає змогу мінімізувати логістичні труднощі та забезпечити оперативне повернення людей після ліквідації загрози.

У випадках виникнення раптових небезпек, які потребують негайного реагування, застосовується екстрена (невідкладна) евакуація, що здійснюється за умов мінімального часу на підготовку та часто проводиться в умовах безпосереднього впливу небезпечних факторів надзвичайної ситуації. Така евакуація зазвичай застосовується, коли загроза життю населення є критичною та вимагає негайного вивезення людей з ураженої території, наприклад, під час аварій на хімічно небезпечних підприємствах, землетрусів, масштабних пожеж чи військових дій. Окрім цього, невідкладна евакуація проводиться у ситуаціях, коли порушення функціонування інфраструктури або систем життєзабезпечення створює загрозу для здоров'я населення, що також вимагає термінових дій для його переміщення у безпечні райони (рис. 2.).

Терміни проведення евакуаційних заходів значною мірою залежать від можливостей транспортного забезпечення та здатності органів управління оперативно організувати першочергове розміщення евакуйованих у регіонах тимчасового перебування, де їм надаються базові засоби життєзабезпечення. Важливим критерієм, який визначає масштабність евакуації, є категорія населення, що підлягає переміщенню, оскільки у кризових ситуаціях можливе проведення як загальної евакуації, що передбачає виведення всіх осіб, які перебувають у зоні небезпеки, так і часткової евакуації, яка стосується лише окремих груп населення, зокрема дітей дошкільного віку, школярів, осіб з обмеженими можливостями, пенсіонерів або пацієнтів медичних закладів, які не можуть самостійно покинути небезпечну територію (Комяк, Кязімов, 2020).

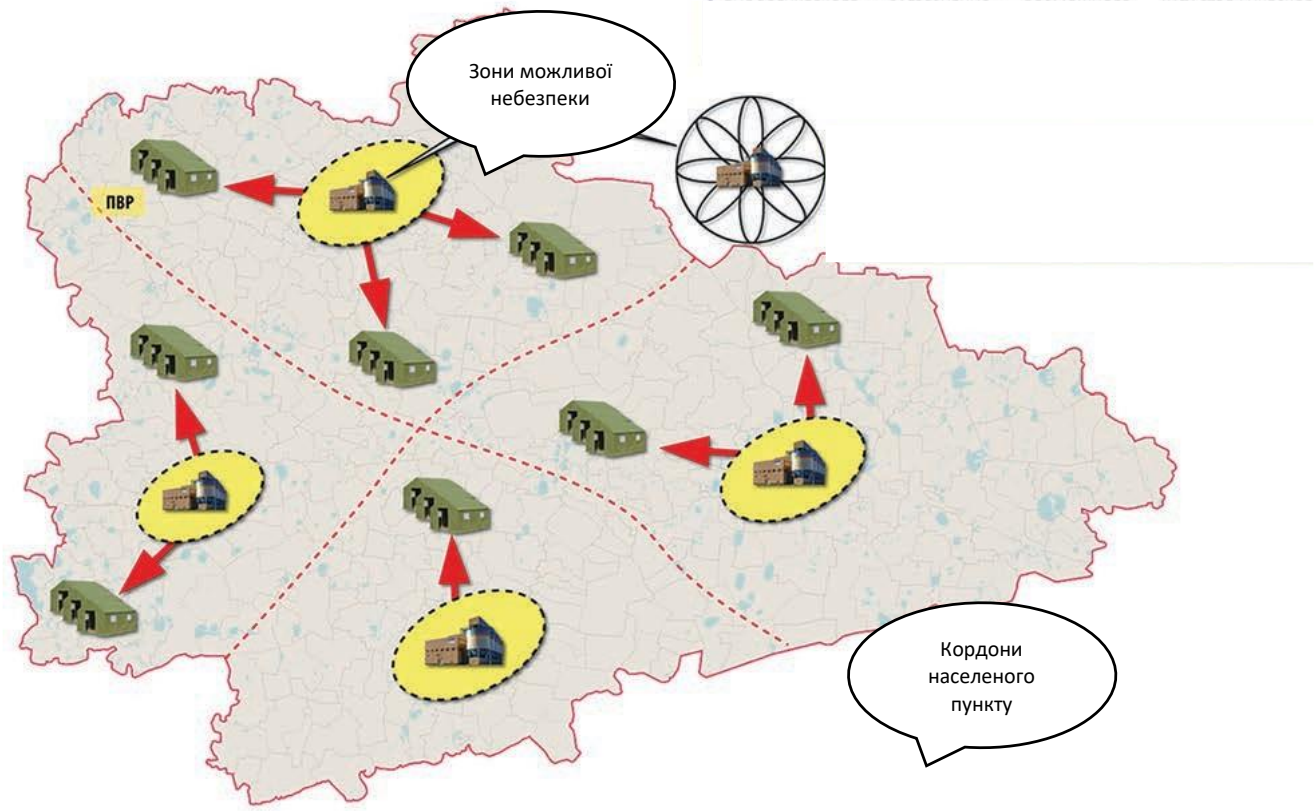


Рисунок 2 – Концептуальна модель планування, підготовки та управління евакуаційними заходами на території окремого населеного пункту за небезпеки виникнення надзвичайної ситуації природного та техногенного характеру

Джерело: сформовано авторами

Ефективність реалізації евакуаційних заходів значною мірою залежить від масштабу небезпечної зони, загальної чисельності населення, що перебуває в зоні ризику, рівня транспортної забезпеченості та місцевих умов, що можуть ускладнювати або, навпаки, сприяти оперативному переміщенню людей у безпечні райони (рис. 3.).

Способи проведення евакуації можуть бути різними та застосовуються залежно від ситуації, що склалася. Найпоширенішими є одночасний, послідовний, вибірковий та комбінований способи евакуації.

Одночасний спосіб евакуації передбачає негайне виведення або вивезення всіх категорій населення, яке перебуває в небезпечній зоні, незалежно від соціального статусу чи рівня загрози. Наведений підхід застосовується у випадках, коли необхідно швидко звільнити територію регіону, області або навіть декількох суміжних регіонів, якщо ризик є масштабним і загрожує життю значної кількості людей. Такий спосіб є оптимальним у разі техногенних аварій, стихійних лих або загроз застосування зброї масового ураження, коли зволікання може призвести до катастрофічних наслідків (Голубок, Бабков, Жабінський, 2021).

Послідовний спосіб евакуації передбачає етапність у процесі переміщення населення, коли спочатку евакуюється одна категорія осіб (наприклад, діти, люди похилого віку, особи з обмеженими можливостями), а потім інші групи населення за визначеним порядком. Аналогічно може проводитися евакуація спочатку в одному населеному пункті чи адміністративному районі, а згодом у наступних регіонах залежно від розвитку надзвичайної ситуації. Цей метод зазвичай застосовується в умовах, коли загроза розвивається поступово, даючи можливість організувати процес більш керовано та уникнути паніки серед населення.

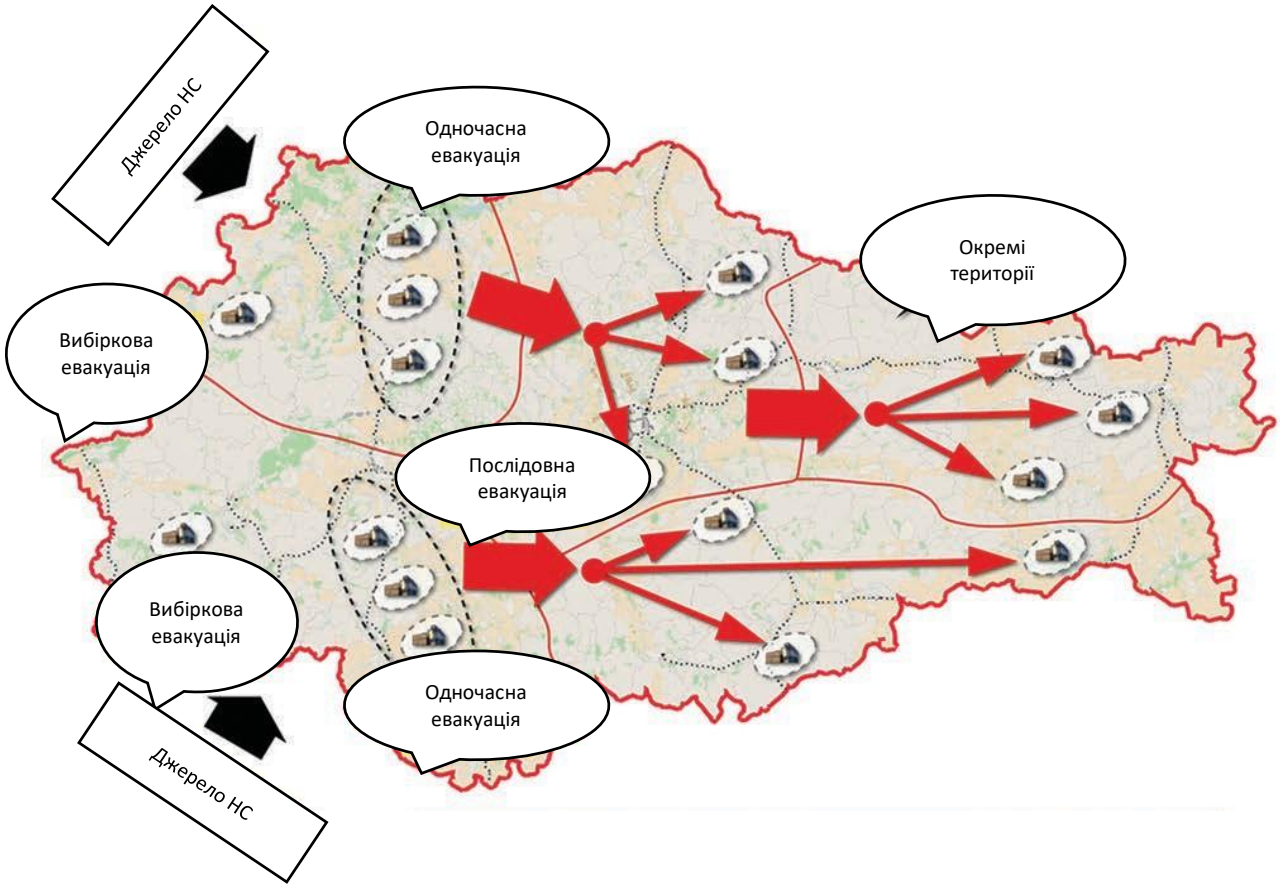


Рисунок 3 – Концептуальна модель планування, підготовки та проведення евакуаційних заходів на території регіону України у разі небезпеки виникнення надзвичайної ситуації природного та техногенного характеру

Джерело: сформовано авторами

Вибірковий спосіб евакуації застосовується у ситуаціях, коли безпосередню загрозу становлять певні категорії осіб або окремі території, що найбільше піддаються впливу негативних факторів надзвичайної ситуації. У цьому випадку евакуюються лише ті групи населення, які знаходяться під найбільшою загрозою, або ж переміщується тільки один об'єкт чи район, що безпосередньо потрапив у зону ураження (Клименко, 2022). Такий метод є доцільним у ситуаціях локальних техногенних аварій, обмежених природних катастроф або при проведенні цілеспрямованих рятувальних операцій.

Комбінований спосіб евакуації передбачає гнучке використання різних варіантів переміщення населення залежно від конкретної ситуації, що може змінюватися у процесі розвитку надзвичайної ситуації. Це означає, що певні групи населення можуть евакуюватися одночасно, тоді як для інших застосовується послідовний або вибірковий підхід. Такий підхід забезпечує адаптивність системи евакуації та дає змогу мінімізувати втрати часу в критичних умовах (табл. 1).

Таблиця 1 – Оцінка способів евакуації населення за умов настання надзвичайної ситуації та їх управлінські особливості

Вид евакуації	Головна перевага	Складність проведення	Управлінське забезпечення	Очікувана ефективність і результативність
Одночасна евакуація	Швидке звільнення небезпечної зони	Потребує значної кількості транспорту та ресурсів	Координація на національному та регіональному рівні	Максимальне зменшення людських жертв у найкоротший термін
Послідовна евакуація	Чітка організація та уникнення паніки	Вимагає ретельного планування та контролю	Децентралізоване управління з місцевими координаційними центрами	Ефективне переміщення без створення хаосу
Вибіркова евакуація	Оптимізація ресурсів на критично важливі групи	Складність у визначенні груп населення, що підлягають евакуації	Залучення аналітичних груп та екстрених служб	Раціональне використання ресурсів при мінімізації ризиків
Комбінована евакуація	Гнучкість та адаптивність до ситуації	Необхідність швидкого аналізу ситуації та прийняття рішень	Гнучка взаємодія різних рівнів управління	Оптимальне співвідношення швидкості та безпеки
Екстрена евакуація	Миттєве реагування на загрозу	Обмеженість часу для організації заходів	Рішення приймаються в умовах високої невизначеності	Збереження життів при мінімальних втратах часу
Попереджувальна евакуація	Забезпечення підготовки до можливих ризиків	Необхідність детального прогнозування ризиків	Попереднє планування та формування евакуаційних резервів	Мінімізація наслідків за рахунок заздалегідь підготовлених заходів

Джерело: сформовано авторами

Евакуація вважається завершеною лише тоді, коли всі особи, які підлягали переміщенню, безпечно покинули небезпечну територію, яка перебуває в зоні впливу загрозливих чинників надзвичайної ситуації. Ключовим фактором для ухвалення рішення про проведення евакуаційних заходів є оцінка ступеня загрози життю та здоров'ю громадян, що визначається на основі заздалегідь розроблених критеріїв, затверджених Міністерством надзвичайних ситуацій України, які враховують специфіку кожного типу небезпеки та рівень загрози для населення.

Обговорення

Отримані результати дослідження знаходяться у кореляції з висновками багатьох науковців, які наголошують на важливості вдосконалення систем евакуації шляхом інтеграції сучасних цифрових технологій та підвищення рівня координації між державними структурами, що є ключовим фактором для ефективного реагування на надзвичайні ситуації.

Зокрема, дослідження (Потеряйко, Бєлікова, Твердохліб, 2022), де підкреслено критичну роль міжвідомчої взаємодії у процесі управління евакуаційними заходами, що знаходить відображення у наших висновках щодо необхідності створення єдиної централізованої системи моніторингу, оповіщення та управління евакуацією, яка забезпечувала б оперативну координацію дій усіх залучених органів. Одночасно, в роботах (Клименко, 2022) та (Abioye, Dulebenets, Ozguven, Moses, Boot, Sando, 2020) звертаємо увагу на проблеми, пов'язані з правовим регулюванням евакуаційних заходів, вказуючи на недостатню чіткість процедур евакуації у швидкоплинних кризових ситуаціях, що підтверджується нашими результатами, які обґрунтовують потребу в модернізації законодавчих актів та розробці деталізованих механізмів управління евакуацією.

Незважаючи на значний обсяг досліджень у сфері цивільного захисту, окремі аспекти управління евакуацією залишаються предметом наукових дискусій. Наприклад, Havrys A., Khlevnoi O. вважають, що централізована система евакуації є оптимальним рішенням для кризових ситуацій, тоді як дослідник (Havrys, Khlevnoi, 2022) наполягає на необхідності децентралізованих підходів, які передбачають розширення повноважень місцевих органів влади та впровадження адаптивних моделей управління на регіональному рівні. Поточне дослідження демонструє, що найбільш ефективним є гібридний підхід, який поєднує централізоване планування з гнучкими механізмами реагування на місцевому рівні, що дозволяє враховувати специфіку різних регіонів та умов.

Новизна дослідження полягає в розробці концептуальної моделі управління евакуацією населення, яка інтегрує організаційні, технологічні та соціальні аспекти, враховуючи динамічні зміни у середовищі надзвичайних ситуацій та адаптуючись до різних сценаріїв розвитку подій. На відміну від більшості попередніх робіт, які фокусуються на окремих аспектах евакуації (при плануванні маршрутів або нормативно-правовій базі), наше дослідження пропонує системний підхід, що охоплює весь процес – від прогнозування загроз до після евакуаційного розміщення населення, що набуває саме комплексне вирішення проблем.

Висновки

Проведено детальний аналіз функцій та значення ключових органів, які відповідають за організацію евакуаційних процесів та надано ґрунтовну оцінку переваг та недоліків різних методів евакуації, включаючи одночасну, послідовну, вибіркову, комбіновану, екстрену та попереджувальну, що дозволило визначити їхню доцільність у різних умовах надзвичайних ситуацій, а також встановити оптимальні підходи до реалізації евакуаційних заходів, враховуючи масштаби та характер загрози. Обґрунтовано доцільність і необхідність впровадження автоматизованих систем моніторингу та управління евакуаційними процесами, які інтегрують у собі цифрові технології для аналізу ризиків, сучасні системи оповіщення, механізми управління транспортними потоками та інструменти контролю зон безпечного розміщення евакуйованих осіб, що забезпечує комплексний підхід до організації евакуації.

Розроблено концептуальну модель забезпечення ефективного управління невідкладними заходами з евакуації населення, які охоплюють критичні етапи, починаючи з підготовки, проведення та завершення евакуаційних заходів. Цей алгоритм сприяє не тільки мінімізації рівня втрат серед цивільних, але й зниженню рівня паніки, а також більш

раціональному потоку використання доступних ресурсів у надзвичайних умовах. Запропоновано комплексний підхід до підвищення ефективності евакуаційних заходів, який включає вдосконалення нормативно-правової бази, модернізацію технічних засобів оповіщення, активне використання інформаційних систем, підготовку населення до дій і поведінки у кризових ситуаціях, а також впровадження критичних моделей управління евакуаційними процесами, що дозволяє забезпечити гнучкість та оперативність у реагуванні на надзвичайні ситуації.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Голубок, М., Бабков, Ю., & Жабінський, В. (2021). Місце та роль Національної гвардії України в системі забезпечення обов'язкової евакуації певної категорії населення. Науковий вісник Національної академії Національної гвардії "Честь і закон", 1(76), 33–39. https://doi.org/10.33405/2078-7480/2021/1/76/229504
2. Клименко, Н. (2022). Особливості забезпечення цивільного захисту в умовах воєнного стану. Науковий вісник: Державне управління, (2 (12), 218–233. https://doi.org/10.33269/2618-0065-2022-2(12)-218-233
3. Кодекс цивільного захисту України: Закон України від 02.10.2012 р. № 5403-VI. Дата оновлення: 01.01.2023. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text
4. Комяк, В., & Кязімов, К. (2020). Варіантне моделювання евакуації людей з висотних будівель у разі виникнення надзвичайної ситуації. Сучасні проблеми моделювання, (17), 27-35. https://doi.org/10.33842/2313-125X/2019/17/27/35
5. Македон, В. В. (2012). Дослідження процесів забезпечення соціальної відповідальності у провідних моделях корпоративного управління. Вісник Харківського національного технічного університету сільського господарства: Економічні науки, (126), 198–206.
6. Муконін, Ю. В. (2024). Організація та проведення заходів з евакуації: навчально-методичний посібник. Кропивницький: НМЦ ЦЗ та БЖД Кіровоградської області.
7. Потеряйко, С. П., Бєлікова, К. Г., & Твердохліб, О. С. (2022). Проблемні питання евакуації населення в безпечні місця в умовах воєнного стану. український кейс. Публічне урядування, (5 (33), 58-63. https://doi.org/10.32689/2617-2224-2022-5(33)-8
8. Снагощенко, А. О. (2020). Особливості здійснення евакуації населення в надзвичайних ситуаціях. У В. П. Титаренко та А. М. Хлопов (Ред.), Безпека життя і діяльності людини: теорія та практика (с. 389–391). ПНПУ імені В. Г. Короленка.
9. Abioye, O. F., Dulebenets, M. A., Ozguven, E. E., Moses, R., Boot, W. R., & Sando, T. (2020). Assessing perceived driving difficulties under emergency evacuation for vulnerable population groups. Safety and Emergency Planning Sciences, 100878. https://doi.org/10.1016/j.seps.2020.100878
10. Geng, J. (2024). An overview of emergency logistics routing and location: Models and future research directions. SHS Web of Conferences, 181, Article 03005. https://doi.org/10.1051/shsconf/202418103005
11. Havrys, A., & Khlevnoi, O. (2022). Software-based method of determining the necessary population evacuation zone in case of a chemical accident. Emergencies: Prevention and Liquidation, 6(2), 116–128. https://doi.org/10.31731/2524.2636.2022.6.2.116-128

12. Idoudi, H., Li, W., Ameli, M., & González, M. C. (2024). Population evacuation in motion: Harnessing disaster evolution for effective dynamic emergency response. IEEE Transactions on Intelligent Vehicles, 9(1), 1–13. https://doi.org/10.1109/TIV.2024.3498099
13. Makedon, V., Myachin, V., Plakhotnik, O., Fisunenko, N., Mykhailenko, O. (2024). Construction of a model for evaluating the efficiency of technology transfer process based on a fuzzy logic approach. Eastern-European Journal of Enterprise Technologies, no 2(13(128)), 47-57. https://doi.org/10.15587/1729-4061.2024.300796.
14. Wu, H., Nie, R., Zeng, X., Cheng, C., Pan, J., Han, D., & Hosamo, H. (2024). Review of advanced emergency evacuation procedures in hospital buildings: comprehensive analysis and insights. Frontiers in Built Environment, 10. https://doi.org/10.3389/fbuil.2024.1381813

References

1. Holubok, M., Babkov, Yu., & Zhabinskyi, V. (2021). Place and role of the National Guard of Ukraine in the system of ensuring mandatory evacuation of a certain population category. The Scientific Journal of the National Academy of National Guard "Honor and Law", 1(76), 33–39. https://doi.org/10.33405/2078-7480/2021/1/76/229504
2. Klymenko, N. (2022). Features of civil protection under martial law conditions. Scientific Bulletin: Public Administration, (2(12)), 218–233. https://doi.org/10.33269/2618-0065-2022-2(12)-218-233
3. Law of Ukraine “Code of Civil Protection of Ukraine” from October 02, 2012, No 5403-VI]. (n.d.). zakon.rada.gov. ua. Retrieved from : https://zakon.rada.gov.ua/laws/show/5403-17#Text
4. Komyak, V., & Kyazimov, K. (2020). Variantal modeling of evacuation of people from altitude buildings in the event of an emergency situation. Modern Problems of Modeling, (17), 27-35. https://doi.org/10.33842/2313-125X/2019/17/27/35
5. Makedon, V. V. (2012). Research on processes ensuring social responsibility in leading corporate governance models. *Bulletin of Kharkiv National Technical University of Agriculture: Economic Sciences*, (126), 198–206.
6. Mukonin, Y. V. (2024). Organization and conduct of evacuation measures: A training manual. NMTS CZ and BZhD of the Kirovohrad region.
7. Poteriaiko, S. P., Bielikova, K. H., & Tverdokhlib, O. S. (2022). Problemy evakuatsii naselennia v bezpechni mistsia v umovakh voiennoho stanu: Ukrainskyi keis [Issues of population evacuation to safe areas under martial law conditions: The Ukrainian case]. Publichne uriaduvannia [Public Administration], (5(33)), 58–63. https://doi.org/10.32689/2617-2224-2022-5(33)-8
8. Snagoshchenko, A. O. (2020). Peculiarities of population evacuation in emergency situations. In V. P. Tytarenko & A. M. Khlopov (Eds.), Safety of human life and activity: theory and practice V. G. Korolenko PNPU. pp. 389–391.
9. Abioye, O. F., Dulebenets, M. A., Ozguven, E. E., Moses, R., Boot, W. R., & Sando, T. (2020). Assessing perceived driving difficulties under emergency evacuation for vulnerable population groups. Safety and Emergency Planning Sciences, 100878. https://doi.org/10.1016/j.seps.2020.100878
10. Geng, J. (2024). An overview of emergency logistics routing and location: Models and future research directions. SHS Web of Conferences, 181, Article 03005. https://doi.org/10.1051/shsconf/202418103005
11. Havrys, A., & Khlevnoi, O. (2022). Software-based method of determining the necessary population evacuation zone in case of a chemical accident. Emergencies: Prevention and Liquidation, 6(2), 116–128. https://doi.org/10.31731/2524.2636.2022.6.2.116-128

12. Idoudi, H., Li, W., Ameli, M., & González, M. C. (2024). Population evacuation in motion: Harnessing disaster evolution for effective dynamic emergency response. *IEEE Transactions on Intelligent Vehicles*, 9(1), 1–13. https://doi.org/10.1109/TIV.2024.3498099
13. Makedon, V., Myachin, V., Plakhotnik, O., Fisunenko, N., Mykhailenko, O. (2024). Construction of a model for evaluating the efficiency of technology transfer process based on a fuzzy logic approach. *Eastern-European Journal of Enterprise Technologies*, no 2(13(128)), 47-57. https://doi.org/10.15587/1729-4061.2024.300796.
14. Wu, H., Nie, R., Zeng, X., Cheng, C., Pan, J., Han, D., & Hosamo, H. (2024). Review of advanced emergency evacuation procedures in hospital buildings: comprehensive analysis and insights. *Frontiers in Built Environment*, 10. https://doi.org/10.3389/fbuil.2024.1381813

Удосконалення методу запобігання виникненню надзвичайних ситуацій місцевого рівня за результатами моніторингу акустичного простору

Improving the Method of Preventing Local Emergencies Based on the Results of Acoustic Space Monitoring

Вадим Тютюник [A]

Corresponding author: д.тех.н., професор, e-mail: tutunik.vadim.72@gmail.com, ORCID: 0000-0001-5394-6367

Дмитро Усачов [A]

ад'юнкт, e-mail: usachovrabotadsns21@gmail.com, ORCID: 0000-0002-1140-9798

Vadym Tiutiunyk [A]

Corresponding author: Doctor of Technical Sciences, Professor, e-mail: tutunik.vadim.72@gmail.com, ORCID: 0000-0002-0243-7519

Dmytro Usachov [A]

PhD student, e-mail: usachovrabotadsns21@gmail.com, ORCID: 0000-0002-1140-9798

[A] Національний університет цивільного захисту України, м. Харків, Україна

[A] National University of Civil Protection of Ukraine, Kharkov, Ukraine

Received: March 12, 2025 | Revised: April 23, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.12

Мета роботи: удосконалення процесу запобігання виникненню надзвичайних ситуацій місцевого рівня, шляхом впровадження акустичного моніторингу для виявлення та ідентифікації на території міст їх джерел.

Метод дослідження: методи аналізу та синтезу акустичних сигналів; методи системного аналізу.

Теоретична цінність дослідження: проведені дослідження можливостей акустичного методу для ідентифікації джерел надзвичайних ситуацій місцевого рівня, які пов'язані з масштабними пожежами рідких органічних речовин, застосуванням вогнепальної зброї та безпілотних літальних апаратів. Результати виконаних експериментів укладаються в довірчі інтервали, розраховані за критерієм Стьюдента з надійністю 0,95, та свідчать про відповідний рівень достовірності та надійності акустичного методу щодо виявлення та ідентифікації джерел надзвичайних ситуацій місцевого рівня.

Практична цінність дослідження: розроблено керуючий алгоритм методу запобігання виникненню надзвичайних ситуацій місцевого рівня за умов функціонування міської системи оперативного акустичного моніторингу небезпечних подій в місті і прогнозування надзвичайних ситуацій місцевого рівня, який передбачає виконання п'яти процедур: 1) моніторинг акустичного простору міста (за допомогою системи наземних автоматизованих пристроїв акустичного контролю та пасивної локації джерел небезпек) та аналіз прийнятого акустичного сигналу (шляхом фільтрації шумів та частотного аналізу «корисного» сигналу); 2) виявлення та ідентифікації небезпечної події (шляхом порівняння амплітудно-частотних характеристик прийнятого акустичного сигналу з даними банку даних та знань характеристик акустичних сигналів від відомих небезпечних подій); 3) моделювання та аналіз загрози виникнення надзвичайних ситуацій місцевого рівня; 4) ухвалення рішень щодо недопущення розвитку небезпечної події на території міста до надзвичайної ситуації місцевого рівня; 5) координація дій відповідних служб міста.

Тип статті: теоретичний, практичний.

Purpose: improving the process of preventing local emergencies by implementing acoustic monitoring to detect and identify their sources in urban areas.

Method: methods of analysis and synthesis of acoustic signals; systems analysis methods.

Theoretical implications: conducted studies of the possibilities of the acoustic method for identifying sources of local emergencies associated with large-scale fires of liquid organic substances, the use of firearms and unmanned aerial vehicles. The results of the experiments performed fit into confidence intervals calculated using the Student's t-test with a reliability of 0.95, and indicate an appropriate level of reliability and validity of the acoustic method for detecting and identifying sources of local emergency situations.

Practical implications: a control algorithm has been developed for a method aimed at preventing the occurrence of local-level emergencies under the functioning of the urban system of operational acoustic monitoring of hazardous events and forecasting local-level emergencies. The algorithm involves the execution of five procedures: 1) monitoring the city's acoustic environment (using a system of ground-based automated acoustic control and passive hazard source localization devices) and analyzing the received acoustic signal (through noise filtering and frequency analysis of the "useful" signal); 2) detection and identification of a hazardous event (by comparing the amplitude-frequency characteristics of the received acoustic signal with data from a database and knowledge base containing acoustic signal characteristics of known hazardous events); 3) modeling and analysis of the threat of a local-level emergency; 4) decision-making to prevent the escalation of a hazardous event into a local-level emergency within the city; 5) coordination of actions of the relevant city services.

Paper type: theoretical, practical.

Ключові слова: надзвичайна ситуація, запобігання виникненню надзвичайних ситуацій, моніторинг надзвичайних ситуацій, обробка акустичних сигналів, моделювання, підтримка прийняття рішень.

Key words: emergency, emergency prevention, emergency monitoring, acoustic signal processing, modeling, decision support.

Вступ

Сучасні міста України являють собою складні системи з рознесеними у просторі та часі параметрами життєдіяльності, які у процесі свого функціонування та розвитку створюють передумови для виникнення надзвичайних ситуацій (НС), що негативно впливають на стан соціально-психологічного, природно-екологічного та економіко-технічного балансу на території міста. Це свідчить про необхідність розробки комплексу ефективних правових, соціально-економічних, політичних, організаційно-технічних, санітарно-гігієничних та інших заходів, спрямованих на запобігання виникненню НС місцевого рівня, шляхом недопущення переростання небезпечних подій, які виникають на території міста, у НС місцевого рівня або пом'якшення їх можливих наслідків. Умови реалізації заходів запобігання виникненню НС місцевого рівня, при виникненні на території міста різного роду небезпечних подій, представлені на рис. 1.



Рисунок 1 – Представлення умов реалізації заходів запобігання виникненню НС місцевого рівня, при виникненні на території міста різного роду небезпечних подій

Згідно даних рис. 1, запобігання виникненню НС місцевого рівня включає реалізацію на окремій території наступних заходів: державне регулювання діяльності суб'єктів господарювання у сфері цивільного захисту та управління ризиками виникнення НС техногенного характеру та пожеж; забезпечення техногенної безпеки; забезпечення пожежної безпеки; державний нагляд (контроль) у сфері техногенної та пожежної безпеки.

При цьому, державне регулювання діяльності суб'єктів господарювання у сфері цивільного захисту здійснюється шляхом: проведення експертизи проектів містобудівної документації та проектів будівництва; ліцензування послуг і виконання робіт протипожежного призначення; технічного регулювання у визначеній сфері відповідальності; державного ринкового нагляду щодо засобів цивільного захисту; державного нагляду (контролю) у сфері пожежної та техногенної безпеки; страхування відповідальності; моніторингу і прогнозування НС.

Ефективна реалізація цих заходів не можлива без даних моніторингу, експертизи, досліджень та прогнозів щодо можливого виникнення та перебігу різного роду небезпечних подій на території міста. Згідно з Кодексом цивільного захисту України, моніторинг НС є системою безперервних спостережень, лабораторного та іншого контролю для оцінки стану захисту населення і територій та небезпечних процесів, які можуть призвести до загрози або виникнення НС, а також своєчасне виявлення тенденцій до їх зміни. Спостереження, лабораторний та інший контроль включають збирання, опрацювання і передавання інформації про стан навколишнього природного середовища, забруднення продуктів харчування, продовольчої сировини, фуражу, води радіоактивними та хімічними речовинами, зараження збудниками інфекційних хвороб та іншими небезпечними біологічними агентами. Для проведення моніторингу і прогнозування НС в Україні створюється та функціонує система моніторингу і прогнозування НС [1].

Ці обставини указують на необхідність інтегрування в систему безпеки міста додаткових автоматизованих датчиків контролю різного роду джерел небезпек, які працюються на різних фізико-хімічних принципах. Розробка такої системи моніторингу джерел НС дозволить об'єднати функцій спостереження та обробки інформації про джерела небезпеки, а також функції прогнозування виникнення на території міста НС різного характеру, з подальшою розробкою ефективних рішень щодо управління службами безпеки та комунальними службами міста [2].

Одним із напрямків раннього виявлення на території міста джерел НС різного характеру є контроль акустичного простору міста за допомогою наземних стаціонарних автоматичних аналізаторів сигналів у акустичному діапазоні [3]. Це і обумовило мету наших досліджень.

Теоретичні основи дослідження

Реалізація спектрального аналізу акустичного простору міста досягається тим, що безперервний та тривалий у реальному масштабі часу оперативний моніторинг за територією міста здійснюється за рахунок об'єднання у систему моніторингу наземних автоматизованих пристроїв контролю акустичного простору та пасивної локації джерел небезпек, а також отримання й обробки інформації від наземних пристроїв акустичного контролю ситуаційним центром, функціонування якого пов'язано з системою виконання антикризових рішень щодо запобігання, локалізації та ліквідації наслідків НС [4].

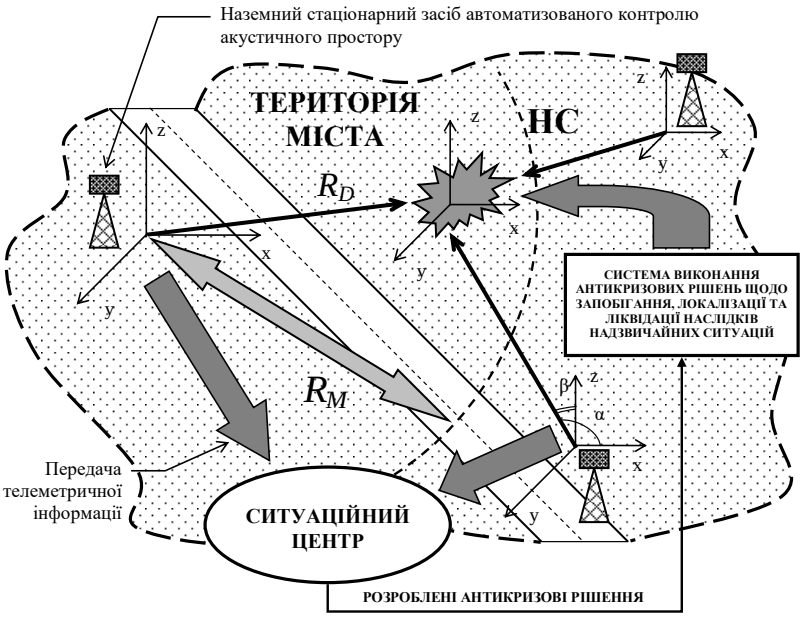


Рисунок 2 – Схема функціонування системи наземних стаціонарних засобів автоматизованого контролю акустичного простору на території міста, ситуаційного центру, підсистеми зв'язку та передавання телеметричної інформації, а також підсистеми виконання антикризових рішень щодо запобігання, локалізації та ліквідації наслідків НС різного характеру на території міста

Методи пасивної акустичної локації джерел небезпек мають свої специфічні особливості, а саме: в умовах відсутності інформації про тривалість акустичного випромінювання дальність до джерела випромінювання не можливо визначити за даними прийому тільки одного наземного засобу автоматизовано контролю акустичного простору. У зв'язку з цим, для визначення координат джерела небезпеки необхідно застосовувати

комплекс двох або декількох рознесених у просторі засобів автоматизовано контролю акустичного простору, які з'єднані каналами зв'язку та утворюють комп'ютерну мережу; прийом прямого, а не відбитого сигналу, полегшує виявлення і вимір координат джерела небезпеки, але незнання форми сигналу та наявність інших джерел акустичного випромінювання ускладнює процес оперативного моніторингу за зоною НС; відсутність передавальних пристроїв при пасивній локації спрощує апаратуру, а також підвищує її енергозбереження та скритність.

Функціональну схему цієї системи наземних стаціонарних засобів автоматизованого контролю акустичного простору, ситуаційного центру, підсистеми зв'язку та передачі телеметричної інформації, а також підсистеми виконання антикризових рішень щодо запобігання, локалізації та ліквідації наслідків НС, представлено на рис. 2.

Функціонування розробленої підсистеми оперативного акустичного моніторингу зони НС на території міста повинно здійснюватися у складі функціонуючої в Україні єдиної державної системи цивільного захисту (ЄДСЦЗ) та в межах класичного контуру управління, який забезпечує: 1) збір, обробку та аналіз інформації; 2) моделювання НС різного характеру на території міста; 3) розробку та ухвалення (в рамках ситуаційного центру) управлінських рішень щодо запобігання, локалізації та ліквідації НС різного характеру, а також мінімізації їх наслідків; 4) виконання рішень щодо запобігання, локалізації та ліквідації НС, а також мінімізації їх наслідків [5].

Основним показником ефективності функціонування підсистеми оперативного акустичного моніторингу зони НС на території міста є достовірність ідентифікації джерела небезпеки за видом та місцем виникнення.

Постановка проблеми

Перспективою для держави є створення геоінформаційної системи акустичного моніторингу джерел небезпек, як інструменту проведення високоточних вимірювань в реальних умовах експлуатації для надійного функціонування єдиної мережі ситуаційних центрів при розробці управлінських рішень щодо запобігання виникненню НС місцевого рівня.

Методологія дослідження

Для оцінки особливостей застосування наземних стаціонарних автоматичних аналізаторів сигналів у акустичному діапазоні для проведення моніторингу НС місцевого рівня в роботі проведені експериментальні дослідження можливостей акустичного методу для ідентифікації джерел небезпек, які пов'язані з масштабними пожежами рідких органічних речовин (РОР), застосуванням вогнепальної зброї та безпілотних літальних апаратів (БПЛА).

Для цієї цілі розроблено вимірювальну схему (рис. 3), з багатомірною обробкою експериментальних даних шляхом поєднаного використання спектрального, фрактального, кластерного і вейвлет аналізів амплітудно-часових характеристик прийнятих акустичних сигналів від небезпечних подій.

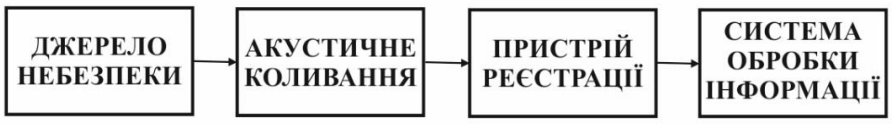


Рисунок 3 – Концепція проведення лабораторних досліджень можливостей акустичного методу щодо ідентифікації джерел НС місцевого рівня

За результатами дослідження можливостей акустичного методу щодо ідентифікації джерел НС, пов'язаних з масштабними пожежами РОР, встановлено, що динаміка процесу

високотемпературного окиснення (горіння), тобто залежності кількості максимумів амплітудно-часових та амплітудно-частотних характеристик прийнятого акустичного сигналу при ефекті акустичної емісії, визначається фізичними та фізико-хімічними термодинамічними параметрами процесу. Досліджено ефект “спалаху”, тобто час первинного процесу горіння парів РОР, та встановлено однозначну залежність тривалості даного процесу від парціального тиску парів над чистим розчинником та температурою спалаху або займання. Встановлено, що чим більше парціальний тиск парів і менше температурою спалаху (займання), тим менше час «спалаху», тобто тривалість горіння парів органічних речовин [6].

Встановлено, що незалежно від природи досліджених органічних речовин значення показників Херста і фрактальної розмірності залишаються постійними для дослідженого ряду легкозаймистих рідин. При цьому встановлено тенденцію підвищення показника Херста і відповідно зниження показника фрактальної розмірності для ізомерів спиртів. Практична сталість параметрів Херста і фрактальної розмірності для органічних речовин з лінійною та ізомерною структурою *С*-каркасів молекул органічних речовин свідчить про відповідний рівень достовірності та надійності отриманих результатів щодо обробки акустичних сигналів при ефекті акустичної емісії реакції високотемпературного окислення (горіння) деяких органічних речовин, що дозволяє зменшити ступінь помилкових спрацьовувань акустичного пристрою виявлення на території міста джерел масштабних пожеж та встановлення природи пального матеріалу в осередку займання [7].

За результатами дослідження можливостей акустичного методу щодо ідентифікації джерел НС, пов’язаних із застосуванням різних типів вогнепальної зброї, удосконалено метод ідентифікації фактів застосування різних типів вогнепальної зброї за параметрами та характеристиками акустичних спектрів пострілів. Застосування удосконаленого методу для дослідження характеристик акустичних спектрів пострілів з пістолету Макарова калібру 9 мм, травматичного пістолету “Форт-14Р” та автомату АК-74 калібру 5,45 мм дозволило з ймовірністю 95 % ідентифікувати тип вогнепальної зброї за прийнятим акустичним сигналом. Розроблено функціональну схему ідентифікації фактів застосування різних типів вогнепальної зброї за спектральними властивостями прийнятого акустичного сигналу [8].

За результатами дослідження можливостей акустичного методу щодо ідентифікації джерел НС, пов’язаних із застосуванням БПЛА, удосконалено метод автоматичного виявлення БПЛА та визначення їх типів на основі акустичних сигналів, який поєднує кластерний аналіз і вейвлет-аналіз. Застосування удосконаленого методу для трьох експериментальних моделей БПЛА – Alpha Robotics Hummingbird 1000 SRTK, DJI Mavic 3t та FPV 7inch ProDrone дозволило з ймовірністю до 90 % точно ідентифікувати тип БПЛА за їх акустичним сигналом. Розроблено алгоритм виявлення та ідентифікації за амплітудно-частотними характеристиками акустичних сигналів БПЛА, який базується на методі вейвлет-аналізу, який дозволяє отримувати інформацію як про частотний, так і про часовий інтервал акустичного сигналу, що дає можливість виділяти характерні особливості спектру БПЛА [9].

Результати виконаних експериментів укладаються в довірчі інтервали, розраховані за критерієм Стьюдента з надійністю 0,95, та свідчать про відповідний рівень достовірності та надійності акустичного методу щодо виявлення та ідентифікації джерел НС місцевого рівня, як інструменту для отримання інформації при розробці управлінських рішень щодо запобігання виникненню НС місцевого рівня.

Результати

При розробці керуючого алгоритму запобігання виникненню НС місцевого рівня за результатами моніторингу акустичного простору в роботі дотримані принципи поетапності дій відповідних етапів системи безпеки міста та її зворотних зв’язків. При цьому за кожний

окремий етап відповідають різні служби та виконавці, однак їх взаємодія координується загальним координаційним центром.

Структура керуючого алгоритму запобігання виникненню НС місцевого рівня за результатами моніторингу акустичного простору складається із п'яти етапів (рис. 4).

Першим етапом алгоритму є проведення моніторингу акустичного простору міста, як потенційної зони НС, що передбачає реєстрацію потенційно небезпечної події на території міста. Моніторинг здійснюється за допомогою розподілених акустичних датчиків, які фіксують амплітудо-частотні характеристики звукових сигналів в реальному часі. Ці пристрої розміщуються у просторі як горизонтально (в різних географічних точках), так і вертикально (на певних висотах).

Моніторинг акустичного простору міста є основною складовою системи запобігання НС місцевого рівня. Завдяки сучасним технологіям, система моніторингу працює у режимі реального часу, безперервно збираючи та обробляючи акустичні дані. Первинна обробка інформації може здійснюватися як у централізованому місці, так і розподіллено – залежно від характеристик системи моніторингу та властивостей міста, де функціонує системи безпеки міста. Отримані дані аналізуються та систематизуються для оцінки рівня небезпеки на території міста. Автоматизовані засоби обробки інформації пришвидшують цей процес і дозволяють створювати електронні бази даних у режимі реального часу.

Другим етапом алгоритму є ідентифікації небезпечної події. Отримана засобами контролю первинна інформація передається до центру інформаційних технологій, де отримані акустичні дані проходять аналіз із використанням штучного інтелекту та алгоритмів обробки сигналів. Програмні модулі порівнюють прийняті амплітудо-частотні характеристики звукових сигналів з базою даних, що дозволяє ідентифікувати джерело небезпечної події за «корисним» акустичним сигналом на фоні шуму.

Третій етап алгоритму – моделювання та аналіз загрози виникнення НС місцевого рівня, що є критичною фазою у запобіганні НС. На цьому етапі використовується поєднання аналітичних методів та комп'ютерного моделювання для оцінки ймовірності розвитку події. Головна мета цього процесу – визначити потенційні сценарії розвитку НС, оцінити їхні наслідки та розробити відповідні заходи у ході ймовірного реагування.

Четвертим етапом алгоритму є ухвалення рішень щодо недопущення розвитку небезпечної події на території міста до НС місцевого рівня. Так, оцінка ризиків визначає рівень загрози для населення та КІ міста, що дає змогу ухвалювати своєчасні рішення щодо запобігання або мінімізації наслідків подій на території міста. Ці рішення ухвалюються в процесі функціонування в місті ситуаційного центру. Перспективи створення таких центрів обумовлено рішенням Ради національної безпеки і оборони України, яка вирішила розширити та у подальшому розвити єдину мережу ситуаційних центрів, до складу якої мають входити Головний ситуаційний центр України, Урядовий ситуаційний центр, ситуаційні центри органів сектору безпеки і оборони, ситуаційні центри центральних органів виконавчої влади, Ради міністрів Автономної Республіки Крим, обласних, Київської та Севастопольської міських державних адміністрацій, а також резервні та рухомі ситуаційні центри [10].

Експерти ситуаційного центру, що приймають рішення, задають критерії для прогнозування розвитку НС місцевого рівня та формування варіантів рішень на основі відповідних розрахунків. Після аналізу запропонованих варіантів особа, відповідальна за прийняття рішення, може обрати оптимальний варіант або скоригувати критерії для уточнення прогнозу. Метою таких рішень є запобігти ескалації небезпеки або, якщо катастрофа неминуча, мінімізувати її наслідки. Затверджене рішення передається до системи виконання, яка формалізує його та доводить до виконавців, що безпосередньо впливають на джерела небезпек в місті.

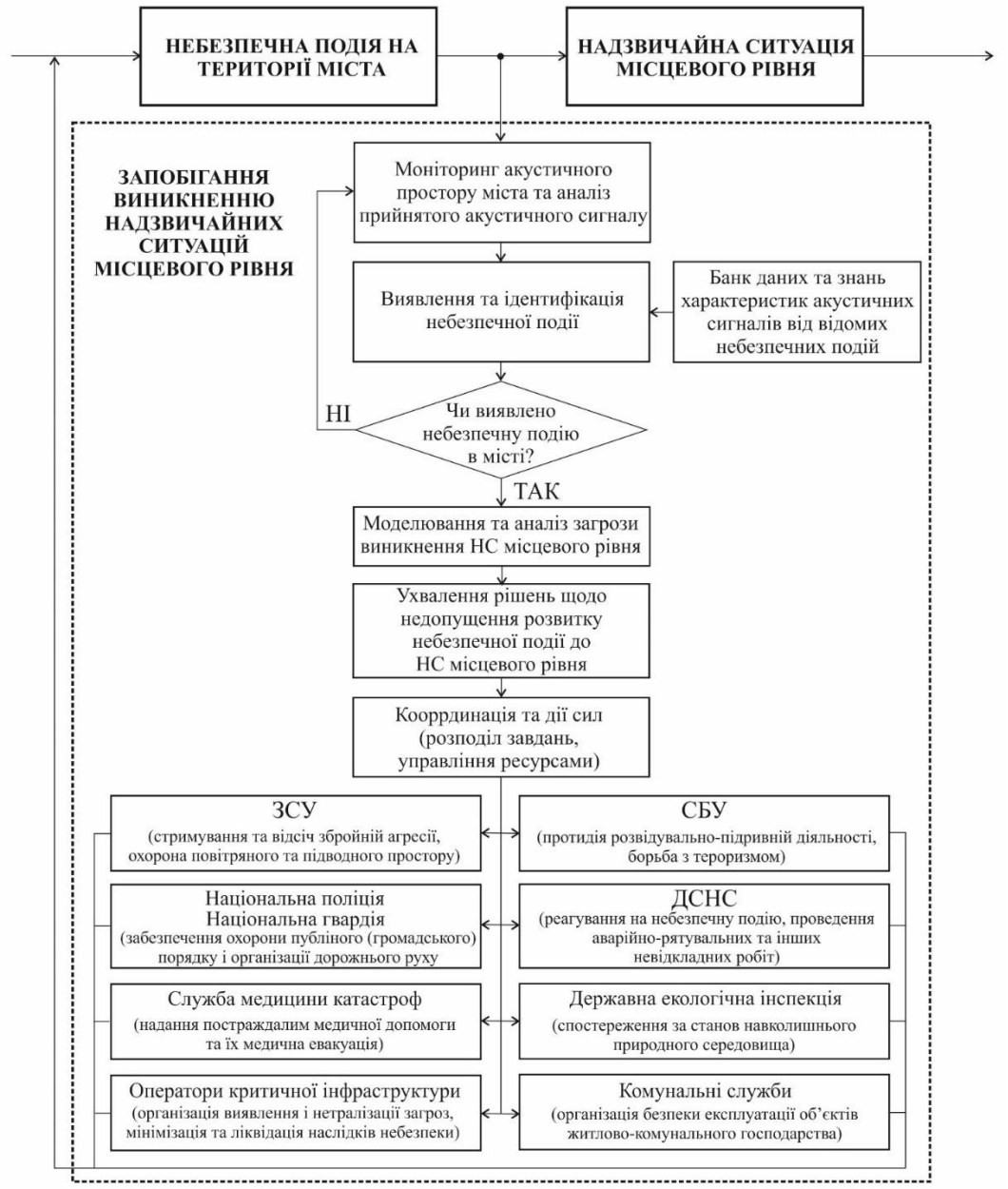


Рисунок 4 – Керуючий алгоритм запобігання виникненню НС місцевого рівня за результатами моніторингу акустичного простору

Координація дій відповідних служб міста є завершальним (п'ятим) етапом алгоритму запобігання виникненню НС місцевого рівня за результатами моніторингу акустичного простору. Вона передбачає чітку взаємодію між різними службами для ефективного розподілу завдань і ресурсів. Автоматизована система оповіщення негайно передає інформацію про потенційну загрозу відповідним службам. Якщо аналіз показує, що подія має високий ризик ескалації до НС місцевого рівня, активуються відповідні служби та відбувається розподіл обов'язків між ними для забезпечення оперативного реагування та координації дій [11].

Основні служби міста об'єднують підрозділи Збройних Сил України, Служби безпеки України, Міністерства внутрішніх справ України, Національна гвардія України, Національна поліція України, Державної служба України з НС, Державної служби медицини катастроф, Державної екологічної інспекції, оператори критичної інфраструктури та комунальні служби, функції яких взаємопов'язані у мирний час, а також в особливий період, у тому числі в умовах воєнного стану, в умовах НС та під час виникнення кризових ситуацій [12].

Збройні Сили України (ЗСУ) є військовим формуванням, на яке відповідно до Конституції України покладаються оборона України, захист її суверенітету, територіальної цілісності та недоторканності. ЗСУ забезпечують стримування та відсіч збройній агресії проти України, охорону повітряного простору держави та підводного простору в межах територіального моря України, у випадках, визначених законом, беруть участь у заходах, спрямованих на боротьбу з тероризмом [13].

Служба безпеки України (СБУ) є державним органом спеціального призначення з правоохоронними функціями, що забезпечує державну безпеку, здійснюючи з неухильним дотриманням прав і свобод людини і громадянина: протидію розвідувально-підривній діяльності проти України; боротьбу з тероризмом; контррозвідувальний захист державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу, кібербезпеки, економічної та інформаційної безпеки держави, ОКІ; охорону державної таємниці [14].

Національна поліція України є центральним органом виконавчої влади, що забезпечує громадську безпеку і порядок, охорону прав і свобод людини, інтересів суспільства і держави, протидію злочинності, а також надає визначені законом послуги з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок НС потребують такої допомоги [15].

Національна гвардія України є військовим формуванням із правоохоронними функціями, призначеним для виконання завдань із захисту та охорони життя, прав, свобод і законних інтересів громадян, суспільства і держави від злочинних та інших протиправних посягань, охорони громадського порядку та забезпечення громадської безпеки, а також у взаємодії з іншими органами – із забезпечення державної безпеки і захисту державного кордону України, припинення терористичної діяльності, діяльності незаконних воєнізованих або збройних формувань, організованих злочинних груп та організацій [16].

ДСНС є центральним органом виконавчої влади, що реалізує державну політику у сферах ЦЗ, захисту населення і територій від НС, запобігання їх виникненню, ліквідації наслідків НС, проведення аварійно-рятувальних робіт, пожежогасіння, пожежної та техногенної безпеки, роботи рятувальних служб під час аварій, а також гідрометеорологічної діяльності [17].

Державна служба медицини катастроф є особливим видом державної аварійно-рятувальної служби, основним завданням якої є надання безоплатної медичної допомоги постраждалим від НС техногенного та природного характеру, рятувальникам та особам, які беруть участь у ліквідації наслідків НС.

Не менш важливу роль відіграють оператори критичної інфраструктури – юридичні особи будь-якої форми власності та/або фізичні особи – підприємці, що на правах власності, оренди або на інших законних підставах здійснює управління об’єктів критичної інфраструктури (ОКІ) та відповідає за його поточне функціонування. При цьому, охороною ОКІ є комплекс режимних, інженерних, інженерно-технічних та інших заходів (крім заходів із захисту інформації та кіберзахисту ОКІ), які організовуються і проводяться суб’єктами національної системи захисту КІ з метою запобігання та/або недопущення чи припинення протиправних дій (актів несанкціонованого втручання) на ОКІ [18].

Допоміжну функцію виконують комунальні служби, які контролюють безпеку житлово-комунального господарства, здійснюють ремонтні роботи та забезпечують функціонування систем водопостачання, каналізації, теплопостачання та електропостачання у разі НС [19].

Таким чином, в процесі виконання службами міста функцій щодо запобігання виникненню НС місцевого рівня впливають на джерела небезпек, які виникли на території міста. Зміни стану функціонування міста та зміни стану небезпеки в ньому викликатимуть зміни у величинах вимірюваних параметрів, що фіксуються пристроями акустичного

контролю. Надалі ці зміни будуть відпрацьовані, а подальше моделювання покаже ефективність виконання прийнятого рішення – алгоритм замкнувся.

Висновки

В роботі набув подальшого розвитку метод запобігання виникненню НС місцевого рівня за результатами експериментальних досліджень можливостей спектрального аналізу акустичного простору щодо виявлення та ідентифікації небезпечних подій на території міст. До керуючого алгоритму реалізації цього методу включено виконання п'яти процедур: 1) моніторинг акустичного простору міста (за допомогою системи наземних автоматизованих пристроїв акустичного контролю та пасивної локації джерел небезпек) та аналіз прийнятого акустичного сигналу (шляхом фільтрації шумів та частотного аналізу «корисного» сигналу); 2) виявлення та ідентифікації небезпечної події (шляхом порівняння амплітудно-частотних характеристик прийнятого акустичного сигналу з даними банку даних та знань характеристик акустичних сигналів від відомих небезпечних подій); 3) моделювання та аналіз загрози виникнення НС місцевого рівня; 4) ухвалення рішень щодо недопущення розвитку небезпечної події на території міста до НС місцевого рівня; 5) координація дій відповідних служб міста.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Кодекс цивільного захисту України: Закон України від 02 жовтня 2012 року № 5403-VI. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text
2. Андронов В.А., Дівізінюк М.М., Калугін В.Д., Тютюник В.В. Науково-конструкторські основи створення комплексної системи моніторингу надзвичайних ситуацій в Україні: Монографія. Харків. Національний університет цивільного захисту України, 2016. 319 с. URL: http://repositsc.nuczu.edu.ua/handle/123456789/5970
3. Тютюник В.В., Тютюник О.О., Усачов Д.В. Особливості створення системи акустичного моніторингу джерел надзвичайних ситуацій у контексті розвитку концепції «Smart City». Науковий вісник: Цивільний захист та пожежна безпека. 2023. № 2(16). С. 58–76. https://doi.org/10.33269/nvcz.2023.2.58-76. URL: http://repositsc.nuczu.edu.ua/handle/123456789/19263
4. Рубан І.В., Тютюник В.В., Тютюник О.О. Розвиток науково-технічних основ оперативного геоінформаційного акустичного моніторингу джерел терористичних небезпек. Сучасні інформаційні технології у сфері безпеки та оборони. Київ: Національний університет оборони України, 2020. Вип. 3(39). С. 67–80. https://doi.org/10.33099/2311-7249/2020-39-3-67-80. URL: http://repositsc.nuczu.edu.ua/handle/123456789/18114
5. Рубан І.В., Тютюник В.В., Тютюник О.О. Особливості створення системи підтримки прийняття антикризових рішень в умовах невизначеності вхідної інформації при надзвичайних ситуаціях. Сучасні інформаційні технології у сфері безпеки та оборони. Київ. Національний університет оборони України. 2021. Вип. 1(40). С. 75–84. URL: http://repositsc.nuczu.edu.ua/handle/123456789/14232
6. Tiutiunyk V., Kalugin V., Levterov A., Sydorenko O., Starodubtsev S., Usachov D. Establishing the Nature of Kinetic Effects of the High-Temperature Oxidation (Combustion) Process of Some

Liquid Organic Matters by Acoustic Radiation. Voprosy khimii i khimicheskoi tekhnologii. 2023. No. 6. pp. 203–212. https://doi.org/10.32434/0321-4095-2023-151-6-203-212.

7. Тютюник В.В., Лєвтєров О.А., Тютюник О.О., Усачов Д.В. Розвиток науково-технічних основ створення геоінформаційної системи акустичного моніторингу масштабних пожеж із рідкими органічними речовинами на території міста. Сучасні інформаційні технології у сфері безпеки та оборони. 2024. № 1(49). С. 111–127. https://doi.org/10.33099/2311-7249/2024-49-1-111-127
8. Тютюник В.В., Лєвтєров О.А., Тютюник О.О., Усачов Д.В. (2024). Акустичний моніторинг джерел надзвичайних ситуацій, пов'язаних із застосуванням вогнепальної зброї. Проблеми надзвичайних ситуацій, 2(40), 269–292. https://doi.org/10.52363/2524-0226-2024-40-19
9. Тютюник В.В., Лєвтєров О.А., Тютюник О.О., Усачов Д.В. Розвиток науково-технічних основ акустичного моніторингу джерел надзвичайних ситуацій, які пов'язані із застуванням вогнепальної зброї. Проблеми надзвичайних ситуацій. Харків, 2024. Вип. 2(40). С. 269–292. https://doi.org/10.52363/2524-0226-2024-40-19. URL: http://repositsc.nuczu.edu.ua/handle/123456789/24173
10. Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони: Рішення Ради національної безпеки і оборони України від 04.06.2021. Введено в дію Указом Президента України від 18 червня 2021 року № 260/2021. URL: https://zakon.rada.gov.ua/laws/show/n0039525-21#Text
11. Про схвалення Концепції розвитку та технічної модернізації системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій: Розпорядження Кабінету Міністрів України від 31 січня 2018 року № 43-р. URL: https://zakon.rada.gov.ua/laws/show/43-2018-%D1%80
12. Про затвердження Інструкції про порядок взаємодії між Державною службою України з надзвичайних ситуацій, Національною поліцією України та Національною гвардією України у сфері запобігання і реагування на надзвичайні ситуації, пожежі та небезпечні події: Наказ Міністерства внутрішніх справ України від 22 серпня 2016 року № 859. Зареєстровано в Міністерстві юстиції України 14 вересня 2016 року за № 1254/29384. URL: https://zakon.rada.gov.ua/laws/show/z1254-16#Text
13. Про Збройні Сили України: Закон України від 06 грудня 1991 року № 1934-XII. URL: https://zakon.rada.gov.ua/laws/show/1934-12#Text
14. Про Службу безпеки України: Закон України від 25 березня 1992 року № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text
15. Про Національну поліцію: Закон України від 02 липня 2015 року № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text
16. Про Національну гвардію України: Закон України від 13 березня 2014 року № 876-VII. URL: https://zakon.rada.gov.ua/laws/show/876-18#Text
17. Про затвердження Положення про Державну службу України з надзвичайних ситуацій: Постанова Кабінету Міністрів України від 16 грудня 2015 року № 1052. URL: https://zakon.rada.gov.ua/laws/show/1052-2015-%D0%BF#Text
18. Про критичну інфраструктуру: Закон України від 16 листопаду 2021 року № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#top
19. Про затвердження типового положення про регіональну та місцеву комісію з питань техногенно-екологічної безпеки і надзвичайних ситуацій: Постанова Кабінету Міністрів України від 17 червня 2015 року № 409. URL: https://zakon.rada.gov.ua/laws/show/409-2015-%D0%BF

References

1. Civil Protection Code of Ukraine: Law of Ukraine dated October 2, 2012, No. 5403-VI. Retrieved from : https://zakon.rada.gov.ua/laws/show/5403-17#Text
2. Andronov, V. A., Divilinyuk, M. M., Kalugin, V. D., & Tiutiunyk, V. V. (2016). *Scientific and design principles of creating a comprehensive emergency monitoring system in Ukraine: Monograph*. Kharkiv: National University of Civil Protection of Ukraine. Retrieved from : http://repositsc.nuczu.edu.ua/handle/123456789/5970
3. Tiutiunyk, V. V., Tiutiunyk, O. O., & Usachov, D. V. (2023). Features of establishing an acoustic monitoring system for emergency sources in the context of "Smart City" development. *Scientific Bulletin: Civil Protection and Fire Safety*, 2(16), 58–76. https://doi.org/10.33269/nvcz.2023.2.58-76 Retrieved from : http://repositsc.nuczu.edu.ua/handle/123456789/19263
4. Ruban, I. V., Tiutiunyk, V. V., & Tiutiunyk, O. O. (2020). Development of scientific and technical principles of operational geo-information acoustic monitoring of terrorist threat sources. *Modern Information Technologies in the Sphere of Security and Defense*, 3(39), 67–80. https://doi.org/10.33099/2311-7249/2020-39-3-67-80 Retrieved from : http://repositsc.nuczu.edu.ua/handle/123456789/18114
5. Ruban, I. V., Tiutiunyk, V. V., & Tiutiunyk, O. O. (2021). Features of developing a decision support system for crisis management under uncertainty of incoming information during emergencies. *Modern Information Technologies in the Sphere of Security and Defense*, 1(40), 75–84. Retrieved from : http://repositsc.nuczu.edu.ua/handle/123456789/14232
6. Tiutiunyk, V., Kalugin, V., Levterov, A., Sydorenko, O., Starodubtsev, S., & Usachov, D. (2023). Establishing the nature of kinetic effects of the high-temperature oxidation (combustion) process of some liquid organic matters by acoustic radiation. *Voprosy khimii i khimicheskoi tekhnologii*, (6), 203–212. https://doi.org/10.32434/0321-4095-2023-151-6-203-212
7. Tiutiunyk, V. V., Levterov, O. A., Tiutiunyk, O. O., & Usachov, D. V. (2024). Development of scientific and technical foundations of a geo-information system for acoustic monitoring of large fires involving liquid organic substances in urban areas. *Modern Information Technologies in the Sphere of Security and Defense*, 1(49), 111–127. https://doi.org/10.33099/2311-7249/2024-49-1-111-127
8. Tiutiunyk, V. V., Levterov, O. A., Tiutiunyk, O. O., & Usachov, D. V. (2024). Acoustic monitoring of emergency sources associated with the use of firearms. *Problems of Emergencies*, 2(40), 269–292. https://doi.org/10.52363/2524-0226-2024-40-19
9. Tiutiunyk, V. V., Levterov, O. A., Tiutiunyk, O. O., & Usachov, D. V. (2024). Development of scientific and technical principles for acoustic monitoring of emergency sources related to firearm usage. *Problems of Emergencies*, 2(40), 269–292. https://doi.org/10.52363/2524-0226-2024-40-19 Retrieved from : http://repositsc.nuczu.edu.ua/handle/123456789/24173
10. On improving the network of situational centers and digital transformation in the sphere of national security and defense: Decision of the National Security and Defense Council of Ukraine dated June 4, 2021. Enforced by Presidential Decree No. 260/2021 dated June 18, 2021. Retrieved from : https://zakon.rada.gov.ua/laws/show/n0039525-21#Text
11. On approval of the Concept for the development and technical modernization of the centralized alert system for threats or emergencies: Order of the Cabinet of Ministers of Ukraine dated January 31, 2018, No. 43-p. Retrieved from : https://zakon.rada.gov.ua/laws/show/43-2018-p
12. On approval of the Instruction on the interaction procedure between the State Emergency Service of Ukraine, the National Police of Ukraine, and the National Guard of Ukraine in the

field of emergency prevention and response, fires, and hazardous events: Order of the Ministry of Internal Affairs of Ukraine dated August 22, 2016, No. 859. Registered by the Ministry of Justice of Ukraine on September 14, 2016, under No. 1254/29384. Retrieved from : https://zakon.rada.gov.ua/laws/show/z1254-16#Text

13. On the Armed Forces of Ukraine: Law of Ukraine dated December 6, 1991, No. 1934-XII. Retrieved from : https://zakon.rada.gov.ua/laws/show/1934-12#Text
14. On the Security Service of Ukraine: Law of Ukraine dated March 25, 1992, No. 2229-XII. Retrieved from : https://zakon.rada.gov.ua/laws/show/2229-12#Text
15. On the National Police: Law of Ukraine dated July 2, 2015, No. 580-VIII. Retrieved from : https://zakon.rada.gov.ua/laws/show/580-19#Text
16. On the National Guard of Ukraine: Law of Ukraine dated March 13, 2014, No. 876-VII. Retrieved from : https://zakon.rada.gov.ua/laws/show/876-18#Text
17. On approval of the Regulation on the State Emergency Service of Ukraine: Resolution of the Cabinet of Ministers of Ukraine dated December 16, 2015, No. 1052. Retrieved from : https://zakon.rada.gov.ua/laws/show/1052-2015-п#Text
18. On critical infrastructure: Law of Ukraine dated November 16, 2021, No. 1882-IX. Retrieved from : https://zakon.rada.gov.ua/laws/show/1882-20#top
19. On approval of the model regulation on the regional and local commissions on technogenic and environmental safety and emergencies: Resolution of the Cabinet of Ministers of Ukraine dated June 17, 2015, No. 409. Retrieved from : https://zakon.rada.gov.ua/laws/show/409-2015-п

Інтегрований підхід до підготовки фахівців із захисту критичної інфраструктури в Україні

An Integrated Approach to Training Specialists in Critical Infrastructure Protection in Ukraine

Роман Яковчук [A]

Corresponding author: д.тех.н., доцент, начальник факультету цивільного захисту Львівського державного університету безпеки життєдіяльності, e-mail: yakovchukrs@ukr.net, ORCID: 0000-0001-5523-5569

Василь Карабин [A]

д.тех.н., професор, професор кафедри цивільного захисту, e-mail: vasyl.karabyn@gmail.com, ORCID: 0000-0002-8337-5355

Андрій Тарнавський [A]

к.тех.н., доцент, доцент кафедри цивільного захисту, e-mail: andry090880@ukr.net, ORCID: 0000-0002-4625-2022

Roman Yakovchuk [A]

Corresponding author: DSc, Associate Professor, Head of the Faculty of Civil Protection, Lviv State University of Life Safety, e-mail: yakovchukrs@ukr.net, ORCID: 0000-0001-5523-5569

Vasyl Karabyn [A]

DSc, Professor, Professor of the Department of Civil Protection, Lviv State University of Life Safety, e-mail: vasyl.karabyn@gmail.com, ORCID: 0000-0002-8337-5355

Andrii Tarnavskyi [A]

Candidate of Technical Sciences, Associate Professor, e-mail: andry090880@ukr.net, ORCID: 0000-0002-4625-2022

[A] Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

[A] Lviv State University of Life Safety, Lviv, Ukraine

Received: April 20, 2025 | Revised: April 28, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.13

Мета роботи: Визначити ключові компетентності, оптимальні методи організації навчальних заходів та структуру й зміст освітньої програми підвищення кваліфікації фахівців із захисту критичної інфраструктури з урахуванням воєнних та техногенних загроз з метою підвищення стійкості та готовності критичних об'єктів до кризових ситуацій..

Метод дослідження: Контент-аналіз, SWOT-аналіз, метод Дельфі.

Результати дослідження: Ідентифіковано 6 ключових компетентностей фахівців із захисту критичної інфраструктури; підтверджено високу релевантність і практичну ефективність чотиримодульної програми; розроблено рекомендації щодо оптимізації змісту та форм навчання.

Теоретична цінність дослідження: Запропоновано адаптовану модель компетенцій фахівця у сфері захисту критичної інфраструктури з урахуванням концепції стійкості та міждисциплінарного підходу, що розширює наукові уявлення про професійну підготовку в умовах гібридних загроз.

Практична цінність дослідження: Озвучені методичні рекомендації та інструментарій оцінки (опитувальник, гайд-інтерв'ю, SWOT-аналіз) можуть бути використані університетами й практичними службами для розробки та вдосконалення власних програм підвищення кваліфікації.

Оригінальність дослідження: Інтегровано кількісні та якісні методи оцінки професійної підготовки фахівців у контексті воєнних та техногенних ризиків в Україні; унікальність підходу полягає в поєднанні міжнародних стандартів НАТО/ЄС із локальними умовами та реаліями сучасної війни.

Тип статті: Теоретичний, описовий, практичний, методичний.

Ключові слова: цивільний захист, критична інфраструктура, підготовка кадрів, воєнні загрози.

Purpose: to identify the key competencies, optimal methods for organizing training activities, and the structure and content of a continuing professional development program for critical infrastructure protection specialists, taking into account military and technological threats, in order to enhance the resilience and preparedness of critical facilities for crisis situations.

Method: content analysis, SWOT analysis, Delphi method.

Findings: six key competencies of critical infrastructure protection specialists were identified; the high relevance and practical effectiveness of the four-module program were confirmed; recommendations were developed to optimize content and instructional formats.

Theoretical implications: an adapted competency model for civil protection of critical infrastructure was proposed, incorporating the concept of resilience and an interdisciplinary approach, thereby expanding academic understanding of professional training under hybrid threat conditions.

Practical implications: the methodological recommendations and assessment tools (questionnaire, interview guide, SWOT analysis) presented can be used by universities and operational agencies to develop and refine their own professional development programs.

Originality: quantitative and qualitative methods were integrated to evaluate specialist training in the context of military and technological risks in Ukraine; the uniqueness of the approach lies in combining NATO/EU standards with local conditions and the realities of modern warfare.

Paper type: Theoretical, descriptive, practical, methodical.

Key words: civil protection, critical infrastructure, personnel training, military threats.

Вступ

Захист критичної інфраструктури є важливим завданням цивільного захисту, особливо у час збройної агресії рф. У сучасних умовах об'єкти критичної інфраструктури (ОКІ) – від об'єктів енергетики до водопостачальних мереж – стають мішенями як для фізичних, так і для

кіберзагроз, що вимагає комплексного посилення захисту з боку держави та залучених структур. Знищення або виведення з ладу таких об'єктів призводить до серйозних наслідків для безпеки, стабільності та життєзабезпечення населення.

Крім традиційних загроз важливим фактором уразливості КІ є воєнні та техногенні ризики. Так, при ракетних ударах на енергетичні об'єкти та мережі України у серпні 2024 року було задіяно понад 200 ракет та безпілотників, що спричинило знеструмлення понад мільйон домогосподарств, вихід з ладу гідротехнічних споруд і об'єктів водопостачання, а також перебої в роботі систем теплопостачання [1]. Додаткову небезпеку становлять аварійні скиди шкідливих речовин у річкові системи Це обґрунтовує потребу в міждисциплінарному підході, внаслідок чого міграція вуглеводневих сполук спостерігається на десятки кілометрів, що може поширювати токсичне забруднення до водоочисних споруд та елементів водопостачальної інфраструктури [2, 3]. Транспортування нафтопродуктів транскордонними трубопроводами створює додаткові екологічні загрози. Аналіз факторів та розробка методів управління безпекою цього процесу дозволяють знизити ймовірність аварій та мінімізувати наслідки для населення і довкілля [4].

Таким чином, сучасна система захисту критичної інфраструктури має враховувати не лише фізичні та кібернетичні загрози, але й складні взаємодії з навколишнім середовищем та процеси, що відбуваються як у гідросфері, так і в геосфері. Це обґрунтовує потребу в міждисциплінарному підході, який поєднує інженерні рішення, екологічний нагляд і стратегічне планування.

Теоретичні основи дослідження

Захист критичної інфраструктури (КІ) в умовах сучасних безпекових викликів розглядається як багатовимірна система заходів, що охоплює організаційні, технічні, правові, інформаційні та кадрові аспекти. Теоретичним підґрунтям для розбудови такої системи є концепції сталості, ризик-менеджменту та управління у кризових ситуаціях.

Ключовим положенням сучасних теорій управління критичною інфраструктурою є визнання її міжгалузевої взаємозалежності, коли пошкодження одного елемента може спричинити ланцюгову реакцію в інших секторах, що забезпечують життєдіяльність населення, економічну стабільність та національну безпеку. Відтак, у сучасних дослідженнях акцентовано увагу на необхідності системного підходу до захисту КІ, що включає комплексну оцінку вразливостей, ідентифікацію критичних функцій та планування заходів із забезпечення стійкості в умовах багаторівневих загроз (OECD, 2019) [5].

Український науково-освітній простір активно інтегрує ці підходи. Вітчизняні дослідники зазначають, що ключовим чинником ефективного захисту об'єктів КІ є кваліфікований персонал, здатний діяти в умовах надзвичайних ситуацій, реалізовувати превентивні заходи та координувати взаємодію між суб'єктами захисту (Суходоля, 2025) [6]. Це узгоджується з міжнародними підходами, згідно з якими підготовка персоналу є однією з трьох основ стратегії зміцнення стійкості поряд із технологічними рішеннями та належним управлінням.

Особливого значення в теоретичному обґрунтуванні набуває розуміння феномену "стійкості" (resilience), яка визначається як здатність системи протистояти зовнішнім загрозам, адаптуватися до них та швидко відновлюватися. Цей підхід став домінантним у документах НАТО та ЄС, де підкреслюється необхідність переходу від реактивної до проактивної моделі захисту, орієнтованої на запобігання порушенням функціонування КІ [7].

У контексті українських реалій, пов'язаних із повномасштабною війною та гібридними загрозами, розвиток національної системи захисту КІ має спиратися не лише на правову базу, а й на чітко окреслені освітньо-кваліфікаційні вимоги до фахівців. Саме тому освітні програми підвищення кваліфікації, такі як реалізована у Львівському державному університеті безпеки

життєдіяльності, є не лише педагогічною інновацією, а й елементом національної стратегії зміцнення обороноздатності держави [8].

У підсумку теоретичні основи дослідження захисту критичної інфраструктури базуються на концепціях стійкості, міждисциплінарної взаємодії та інституційної готовності, які мають бути реалізовані через системну освітню політику, технологічну модернізацію та стратегічне управління.

Постановка проблеми

Забезпечення безпеки та безперебійного функціонування критичної інфраструктури значною мірою залежить від рівня підготовленості фахівців, які залучені до здійснення заходів щодо захисту ОКІ, та їхньої компетенції [9]. Зовнішні та внутрішні загрози, що зростають у безпековому середовищі України, підсилюють необхідність підвищення професійної підготовки фахівців, які в умовах протидії збройній агресії займаються виявленням, запобіганням і нейтралізацією загроз для ОКІ, а також ліквідацією наслідків надзвичайних ситуацій у разі їх виникнення на таких об'єктах [8]. Тому підвищення кваліфікації спеціалістів у сфері захисту критичної інфраструктури набуває не лише освітнього, а й стратегічного значення для державної безпеки. Системна професійна підготовка має забезпечити здатність оперативно реагувати на загрози, впроваджувати превентивні заходи та діяти ефективно в умовах кризових ситуацій.

Мета дослідження – визначити ключові компетентності, оптимальні методи організації навчальних заходів та структуру й зміст освітньої програми підвищення кваліфікації фахівців із захисту критичної інфраструктури з урахуванням воєнних та техногенних загроз з метою підвищення стійкості та готовності критичних об'єктів до кризових ситуацій.

Методологія дослідження

Методологія дослідження спрямована на всебічну оцінку ефективності освітньої програми підвищення кваліфікації фахівців із захисту критичної інфраструктури та складається з трьох взаємопов'язаних етапів: підготовчого, експериментального і аналітичного.

1. Підготовчий етап. На цьому етапі проведено контент-аналіз ключових нормативно-правових документів, що визначають вимоги до стійкості критичних об'єктів (Directive (EU) 2022/2557) та національних планів захисту КІ [9]. Вивчено наукові підходи до організації навчальних програм із безпеки КІ, зокрема на основі аналітичної доповіді Суходолі (2025) [6] та методичних рекомендацій міжнародних організацій. Результатом стало формування теоретико-методичного каркасу, в межах якого розроблено інструментарій дослідження: опитувальник, гайд-інтерв'ю для експертів і форму для SWOT-аналізу.

2. Експериментальний етап. Для збору даних застосовано змішану (mixed-methods) стратегію відповідно до рекомендацій Creswell та Creswell (2018) [10]. Використано чотири основні методи:

- **Контент-аналіз** програм та навчальних матеріалів (загалом 24 документи державного та університетського рівня);
- **Метод Дельфі** (дві хвилі опитування 10 експертів із різних секторів КІ) для узгодження ключових компетентностей і додаткових тем на навчальних модулях. Метод Дельфі обрано через здатність досягати консенсусу серед експертів без прямого впливу групової динаміки, що критично важливо для оцінки професійних компетенцій та можливості анонімного уточнення позицій експертів у кількох ітераціях, що зменшує ризик упереджень;
- **Фокус-групи** (3 групи по 6-8 учасників) для глибинного обговорення організаційних та методичних аспектів проведення занять. Фокус-групи застосовані для виявлення

неочевидних проблем у організації занять через групову дискусію, глибинного розуміння контексту воєнних та техногенних загроз через відкрите обговорення кейсів.

3. Аналітичний етап. Зібрані кількісні дані проаналізовано з використанням описової статистики та рейтингового оцінювання. Якісний масив (відкриті відповіді, інтерв'ю, фокус-групи) оброблено за допомогою тематичного аналізу і SWOT-аналізу сильних і слабких сторін програми. Аналітичну частину доповнено порівняльним аналізом із рекомендаціями CER Directive щодо інституційної готовності та процедури реагування на кризові ситуації [7].

Вибірка і етичні аспекти. У вибірку включено фахівців із підрозділів цивільного захисту різного рівня: від локальних рятувальних служб до представників державних органів. Дані респондентів анонімізовані згідно з етичними стандартами наукових досліджень.

Застосована методологія забезпечила інтеграцію кількісних та якісних даних, що дозволило виявити як загальні тенденції сприйняття програми, так і глибинні побажання й застереження фахівців. Такий підхід створює надійну основу для подальшої модернізації змістових модулів та вдосконалення форм навчання фахівців із захисту критичної інфраструктури.

Результати

Основною метою підвищення кваліфікації осіб, які залучаються до здійснення заходів захисту ОКІ, є забезпечення особистісного та професійно-діяльнісного самовдосконалення на основі активізації їхньої базової освіти, набутого професійного та життєвого досвіду відповідно до індивідуально-особистих інтересів, соціальних запитів держави щодо ефективного виконання посадово-функціональних обов'язків.

Підходи щодо захисту критичної інфраструктури мають спільні і відмінні риси в Україні і країнах Європейського союзу (табл. 1).

Таблиця 1 – Порівняння міжнародних та українських підходів до захисту захисту критичної інфраструктури (укладено за матеріалами [6, 11-18])

Критерій	Українські стандарти	Міжнародні стандарти
Правова база	Закон України від 16.11.2021 № 1882-IX "Про критичну інфраструктуру"	Директива ЄС 2022/2557, ISO 27001/22301, стандарти НАТО
Стійкість (resilience)	Інтеграція концепції через міждисциплінарний підхід	Проактивне управління ризиками, адаптація до гібридних загроз (ISO 22301, НАТО)
Кібербезпека	Регулюється окремими законами (наприклад, "Про кібербезпеку")	ISO 27001 для інформаційної безпеки, Framework for Improving Critical Infrastructure Cybersecurity (NIST)
Механізми реалізації	Паспорти безпеки, проекти загроз, категоризація об'єктів	Системи менеджменту безпеки (ISO), планування безперервності бізнесу (ISO 22301)
Взаємодія секторів	Державно-приватне партнерство, міжвідомча координація	Координація через NATO-EU Task Force, транснаціональні протоколи
Освіта та підготовка	Освітньо-професійні програми за першим (бакалаврським), другим (магістерським) рівнями вищої освіти. Освітні програми підвищення кваліфікації	Сертифікаційні програми ISO, навчання в рамках NATO Centres of Excellence

Водночас в ЄС і в Україні є розуміння важливості якісної підготовки кадрів у напрямі стійкості та захисту об'єктів критичної інфраструктури.

Для підвищення рівня кваліфікації персоналу ОКІ у Львівському державному університеті безпеки життєдіяльності розроблена Освітня програма підвищення кваліфікації "Захист об'єктів критичної інфраструктури".

Метою цієї освітньої програми підвищення кваліфікації є підготовка посадових осіб, які залучені до здійснення заходів захисту ОКІ, вивчення теоретичних основ та практичних заходів щодо організації захисту ОКІ, функціонування загальної системи захисту та забезпечення безпеки та стійкості критичної інфраструктури України.

Освітня програма спрямована на формування компетентностей у посадових осіб, відповідальних за захист критичної інфраструктури, нових знань, умінь та навичок, спрямованих на створення і організацію безпеки критичної інфраструктури, зокрема:

забезпечення функціональності, безперервності роботи, цілісність і стійкість критичної інфраструктури;

набуття теоретичних основ та поглиблення набутих теоретичних знань щодо законодавчої бази у сфері захисту критичної інфраструктури;

формування практичних умінь з порядку визначення критичності окремих елементів ОКІ;

порядку влаштування, оцінки і підтримання інженерного захисту окремих критичних елементів;

опанування методики проведення моніторингу рівня безпеки ОКІ;

реагування на надзвичайні ситуації та ліквідацію їх наслідків на ОКІ.

Освітня програма складається з чотирьох змістових модулів, які логічно побудовані та охоплюють увесь спектр необхідних знань і навичок (рис. 1).

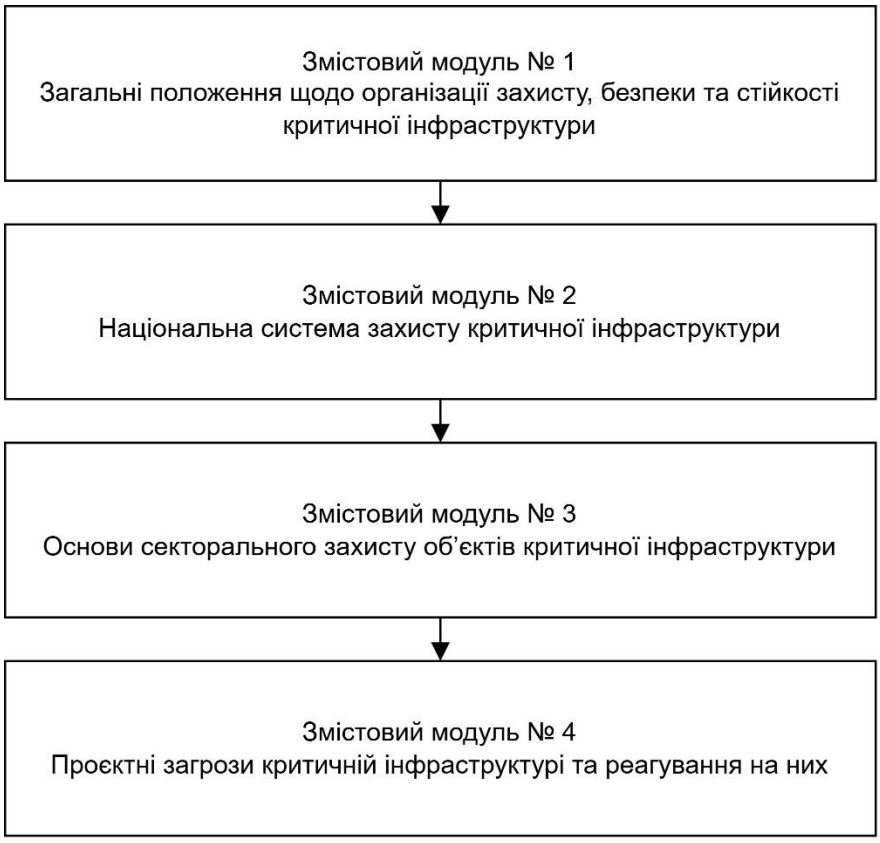


Рисунок 1 – Схема змістових модулів освітньої програми підвищення кваліфікації "Захист об'єктів критичної інфраструктури" у Львівському державному університеті безпеки життєдіяльності

Змістовий модуль № 1 "Загальні положення щодо організації захисту, безпеки та стійкості критичної інфраструктури" зосереджений на організаційних та правових аспектах

захисту критичної інфраструктури, основних засадах державної політики у сфері захисту критичної інфраструктури, стійкості критичної інфраструктури, ознайомленні з міжнародним досвідом захисту ОКІ.

Змістовий модуль № 2 "Національна система захисту критичної інфраструктури" детально розглядає національну систему захисту ОКІ, основні функції уповноваженого органу у сфері захисту критичної інфраструктури України, діяльність функціональних та секторальних органів у сфері захисту критичної інфраструктури, порядок взаємодії між суб'єктами захисту критичної інфраструктури.

Змістовий модуль № 3 "Основи секторального захисту об'єктів критичної інфраструктури" охоплює комплекс знань і практичних навичок, необхідних для організації захисту об'єктів у різних секторах критичної інфраструктури, порушення функціонування яких призводить до порушення життєво важливих функцій та послуг. У модулі розглядаються питання запобігання посяганням на ОКІ у контексті їх секторальної приналежності, моніторингу, інженерного захисту ОКІ. Особливу увагу приділено основним аспектам енергетичної безпеки держави та особливостям забезпечення паливно-енергетичного сектору, секторів транспорту, промисловості, систем життєзабезпечення, громадської безпеки, соціального захисту, державного матеріального резерву, державної влади та місцевого самоврядування, захисту інформації, інформаційного медіа сектору, цифрових технологій. Основний акцент робиться на актуальності захисту критичної інфраструктури в умовах гібридної технології ведення війни, повномасштабної війни, а також терористичних загроз в Україні.

Змістовий модуль № 4 "Проєктні загрози критичній інфраструктурі та реагування на них" зосереджений на проєктних загрозах для критичної інфраструктури, організації реагування на кризові ситуації в умовах воєнного стану. Особливу увагу зосереджено на реагуванні на надзвичайні ситуації, пов'язані з радіаційною та хімічною небезпекою, кіберзагрозах для ОКІ та їх усуненні, синергії фізичного та кіберзахисту на ОКІ.

У результаті навчання слухачі опанують такі вміння:

ідентифікувати та здійснювати категоризацію ОКІ;

здійснювати планування, розроблення та впровадження заходів захисту критичної інфраструктури;

визначати критичні елементи ОКІ;

визначати можливі загрози для критичної інфраструктури;

оцінювати вразливість ОКІ;

визначати рівень захисту та планувати заходи захисту ОКІ;

розробляти паспорти безпеки ОКІ;

прогнозувати і оцінювати обстановку в зоні кризової ситуації на ОКІ та тактичні можливості підрозділів, що залучаються до ліквідації наслідків аварійної ситуації;

розробляти плани взаємодії та підтримувати життєво важливі функції на випадок порушення функціонування об'єктів критичної енергетичної інфраструктури.

Освітня програма підвищення кваліфікації "Захист об'єктів критичної інфраструктури" є своєчасною відповіддю на виклики, з якими сьогодні стикається Україна. Війна яскраво продемонструвала, наскільки вразливими є ОКІ перед військовими атаками, гібридними загрозами та надзвичайними ситуаціями природного і техногенного характеру. Саме тому підготовка фахівців, які здатні забезпечити захист ключових об'єктів країни, стала не просто актуальною, а життєво необхідною.

Особливо важливим є міжнародний контекст цієї програми. У рамках підвищення кваліфікації враховано кращі практики країн-членів ЄС і стандартів НАТО у сфері захисту критичної інфраструктури. Це дає змогу адаптувати підготовку фахівців до сучасних вимог, а також інтегрувати Україну у спільний безпековий простір.

Навчальний план програми передбачає 90 академічних годин (3 ECTS-кредити), з них: 60 годин на теоретичні та практичні заняття та 30 годин на самостійну роботу.

Учасники програми отримуватимуть відповідний сертифікат про підвищення кваліфікації, що визнається державними органами.

Освітня програма підвищення кваліфікації може бути корисною не лише для вітчизняних фахівців, які залучені до здійснення заходів захисту критичної інфраструктури, але й для посадових осіб та персоналу, який відповідає за охорону, безпеку та захист ОКІ, а також представників екстрених служб з реагування на надзвичайні ситуації Європейського Союзу.

Висновки

У результаті комплексного дослідження було визначено ключові компетентності фахівців із захисту критичної інфраструктури, зокрема:

забезпечення функціональності, безперервності роботи, цілісність і стійкість критичної інфраструктури;

набуття теоретичних основ та поглиблення набутих теоретичних знань щодо законодавчої бази у сфері захисту критичної інфраструктури;

формування практичних умінь з порядку визначення критичності окремих елементів ОКІ;

порядку влаштування, оцінки і підтримання інженерного захисту окремих критичних елементів;

опанування методики проведення моніторингу рівня безпеки ОКІ;

реагування на надзвичайні ситуації та ліквідацію їх наслідків на ОКІ.

Застосування змішаної методології (контент-аналіз, Delphi, фокус-групи, анкетування) дозволило верифікувати структуру освітньої програми та підтвердити її ефективність. Експертне коло високо відзначило інтерактивні формати викладання й акцент на практичних навичках. SWOT-аналіз виявив сильні сторони програми (інтеграція міжнародних стандартів, міждисциплінарний підхід) та слабкі – необхідність оновлення кейсів під поточні воєнні реалії.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. IEA. Інтернет джерело. URL : https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter/ukraines-energy-system-under-attack?utm_source
2. Shuryhin, V. (2023). The River System Pollutant Migration in the Context of the Sudden One-Time Discharge with Consideration of the Bottom Sediments Influence (Case of Benzene Migration in the Stryi River, Ukraine). *Ecological Engineering & Environmental Technology*. URL : https://www.ecoeet.com/The-River-System-Pollutant-Migration-in-the-Context-of-the-Sudden-One-Time-Discharge%2C154909%2C0%2C2.html
3. Карабин В.В. (2015). Закономірності зміни макрокомпонентного хімічного складу вод ріки Білий Черемош. *Збірник наукових праць УкрДГРІ*. (1), С. 114-121.
4. Shuryhin, V., Rak, Y., & Karabyn, V. (2020). Analysis of Factors and Development of Methods for Managing the Environmental and Civil Safety of Transboundary Transportation of Oil and Oil Products Through Pipelines. *ScienceRise*, (5), 51-56. https://doi.org/10.21303/2313-8416.2020.001484

5. Organisation for Economic Co-operation and Development. (2019). *Good governance for critical infrastructure resilience*. OECD Publishing. URL : https://www.oecd.org/publications/good-governance-for-critical-infrastructure-resilience-7a74ebc3-en.htm
6. Формування системи освіти, підготовки та перепідготовки персоналу у сфері захисту критичної інфраструктури: аналіт. доп. / О.М. Суходоля. Київ: Національний інститут стратегічних досліджень, 2025. 92 с. https://doi.org/10.53679/NISS-analytrep.2025.01.
7. European Commission. (2022). *Directive on the resilience of critical entities (CER Directive)*. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557
8. Яковчук Р.С., Тарнавський А.Б., Карабин В.В. Перспективи підготовки фахівців у галузі захисту критичної інфраструктури України // Екологічна безпека в умовах війни: збірник тез доповідей V Міжнародної науково-практичної конференції, м. Львів, 21 листопада 2024 р. Львів: ЛДУ БЖД, 2024. С. 211-213.
9. Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури: Розпорядження Кабінету Міністрів України від 19.09.2023 № 825-р.
10. Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). SAGE. URL : https://us.sagepub.com/en-us/nam/research-design/book255675
11. Верховна Рада України. (2021). Закон України "Про критичну інфраструктуру". URL : https://zakon.rada.gov.ua/laws/show/1882-20#Text
12. European Union. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union, L 333/164. URL : https://eur-lex.europa.eu/eli/dir/2022/2557/oj
13. International Organization for Standardization. (2019). ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements. URL : https://www.iso.org/standard/75106.html
14. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. URL : https://www.iso.org/standard/27001
15. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. URL : https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
16. NATO. (2023). Resilience and Article 3. URL : https://www.nato.int/cps/en/natohq/topics_132722.htm
17. OECD. (2019). Good Governance for Critical Infrastructure Resilience. OECD Publishing. https://doi.org/10.1787/6efc8d9f-en
18. UNDRR. (2017). Build Back Better in recovery, rehabilitation and reconstruction. United Nations Office for Disaster Risk Reduction. URL : https://www.undrr.org/terminology/build-back-better

References

1. IEA. Інтернет джерело. Available from : https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter/ukraines-energy-system-under-attack?utm_source
2. Shuryhin, V. (2023). The River System Pollutant Migration in the Context of the Sudden One-Time Discharge with Consideration of the Bottom Sediments Influence (Case of Benzene Migration in the Stryi River, Ukraine). *Ecological Engineering & Environmental Technology*. Available from : https://www.ecoeet.com/The-River-System-Pollutant-Migration-in-the-Context-of-the-Sudden-One-Time-Discharge%2C154909%2C0%2C2.html

3. Karabyn, V.V. (2015). Zakonomirnosti zminy makrokomponentnoho khimichnoho skladu vod riky Bilyi Cheremosh. *Zbirnyk naukovykh prats UkrDGRI*. (1), 114–121.
4. Shuryhin, V., Rak, Y., & Karabyn, V. (2020). Analysis of Factors and Development of Methods for Managing the Environmental and Civil Safety of Transboundary Transportation of Oil and Oil Products Through Pipelines. *ScienceRise*, (5), 51-56. https://doi.org/10.21303/2313-8416.2020.001484
5. Organisation for Economic Co-operation and Development. (2019). *Good governance for critical infrastructure resilience*. OECD Publishing. Available from : https://www.oecd.org/publications/good-governance-for-critical-infrastructure-resilience-7a74ebc3-en.htm
6. Formuvannia systemy osvity, pidhotovky ta perepidhotovky personalu u sferi zakhystu krytychnoi infrastruktury: analit. dop. / O.M. Sukhodolia. Kyiv: Natsionalnyi instytut stratehichnykh doslidzhen, 2025. 92 s. https://doi.org/10.53679/NISS-analytrep.2025.01
7. European Commission. (2022). *Directive on the resilience of critical entities (CER Directive)*. Available from : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557
8. Yakovchuk R.S., Tarnavskyi A.B., Karabyn V.V. Perspektyvy pidhotovky fakhivtsiv u haluzi zakhystu krytychnoi infrastruktury Ukrainy // Ekolohichna bezpeka v umovakh viiny: zbirnyk tez dopovidei V Mizhnarodnoi naukovo-praktychnoi konferentsii, m. Lviv, 21 lystopada 2024 r. Lviv: LDU BZhD, 2024. S. 211–213.
9. Natsionalnyi plan zakhystu ta zabezpechennia bezpeky ta stiikosti krytychnoi infrastruktury: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 19.09.2023 № 825-r.
10. Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). SAGE. Available from : https://us.sagepub.com/en-us/nam/research-design/book255675
11. Verkhovna Rada Ukrainy. (2021). Zakon Ukrainy “Pro krytychnu infrastrukturu”. Available from : https://zakon.rada.gov.ua/laws/show/1882-20#Text
12. European Union. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union, L 333/164. Available from : https://eur-lex.europa.eu/eli/dir/2022/2557/oj
13. International Organization for Standardization. (2019). ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements. Available from : https://www.iso.org/standard/75106.html
14. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. https://www.iso.org/standard/27001
15. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Available from : https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
16. NATO. (2023). Resilience and Article 3. Available from : https://www.nato.int/cps/en/natohq/topics_132722.htm
17. OECD. (2019). Good Governance for Critical Infrastructure Resilience. OECD Publishing. https://doi.org/10.1787/6efc8d9f-en
18. UNDRR. (2017). Build Back Better in recovery, rehabilitation and reconstruction. United Nations Office for Disaster Risk Reduction. Available from : https://www.undrr.org/terminology/build-back-better

Enhancing Methods of Protection in the Amazon Web Services Cloud with Artificial Intelligence and Machine Learning

Покращення методів захисту у хмарному середовищі Amazon Web Services за допомогою штучного інтелекту та машинного навчання

Vitalii Molnar
Corresponding author: Postgraduate student, e-mail: vitalii.v.molnar@lpnu.ua, ORCID: 0009-0001-3183-0117
Dmytro Sabodashko
Doctor of Philosophy, Senior Lecturer of Department of Information Security, e-mail: dmytro.v.sabodashko@lpnu.ua, ORCID: 0000-0003-1675-0976
Lviv Polytechnic National University, Lviv, Ukraine

Віталій Молнар
Corresponding author: аспірант кафедри захисту інформації, e-mail: vitalii.v.molnar@lpnu.ua, ORCID: 0009-0001-3183-0117
Дмитро Сабодашко
Доктор філософії, старший викладач кафедри захисту інформації, e-mail: dmytro.v.sabodashko@lpnu.ua, ORCID: 0000-0003-1675-0976
Національний університет "Львівська політехніка", м. Львів, Україна

Received: March 6, 2025 | Revised: Aprile 15, 2025 | Accepted: Aprile 30, 2025

DOI: 10.33445/sds.2025.15.2.14

Purpose: To investigate protection methods in the Amazon Web Services cloud environment using artificial intelligence and machine learning and to assess the effectiveness of AI-based security tools compared to traditional approaches.

Method: The study employs an experimental approach in the Amazon Web Services (AWS) cloud environment. Simulated cyberattacks, including unauthorized access, data exfiltration, web-based attacks, and privilege escalation, were performed to assess security effectiveness. A comparative analysis was conducted between traditional security mechanisms (CloudTrail, WAF) and AI-driven security tools (Amazon GuardDuty, Macie). The evaluation focused on detection accuracy, response time, and adaptability, reflecting the study's findings how effectively each method detects and mitigates security threats in a cloud environment.

Findings: Security tools leveraging artificial intelligence, such as GuardDuty and Macie, provide more effective threat detection than traditional security methods. They demonstrate high accuracy, reduce false positives, and enable faster response to potential attacks.

Theoretical implications: The study deepens the understanding of AI's role in cloud security methods and highlights the need to integrate both traditional and automated security strategies.

Practical implications: The findings offer recommendations for implementing automated threat detection systems and improving security monitoring in the Amazon Web Services cloud environment.

Value: This research highlights the advantages of integrating artificial intelligence into cloud security and proposes practical solutions to enhance protection strategies.

Future research: Future studies may explore deep learning-based attack prediction, enhanced behavioral analytics, and the development of self-learning security systems.

Paper type: Conceptual research.

Мета: Дослідити методи захисту хмарного середовища Amazon Web Services за допомогою штучного інтелекту та машинного навчання та оцінити ефективність інструментів на основі штучного інтелекту у порівнянні з традиційними засобами безпеки.

Метод дослідження: Використано експериментальний підхід, який включає моделювання атак, таких як несанкціонований доступ, викрадення даних, веб-атаки та підвищення привілеїв. Порівняльний аналіз виконано між традиційними методами безпеки (CloudTrail, WAF) та інструментами з використанням штучного інтелекту (Amazon GuardDuty, Macie) з оцінкою точності виявлення, часу реагування та здатності адаптуватися до нових загроз.

Результати дослідження: Інструменти на основі штучного інтелекту, такі як GuardDuty та Macie, забезпечують більш ефективне виявлення загроз порівняно з традиційними методами. Вони демонструють високу точність, знижують рівень хибних помилок та дозволяють швидше реагувати на потенційні атаки.

Теоретична цінність дослідження: Дослідження поглиблює розуміння впливу штучного інтелекту на методи захисту в хмарному середовищі та підкреслює необхідність поєднання традиційних і автоматизованих стратегій безпеки.

Практична цінність дослідження: Отримані результати надають рекомендації щодо впровадження автоматизованих систем виявлення загроз та покращення моніторингу безпеки у хмарному середовищі Amazon Web Services.

Цінність дослідження: Дослідження демонструє переваги інтеграції штучного інтелекту в кібербезпеку хмарних середовищ і пропонує практичні рішення для посилення методів захисту.

Майбутні дослідження: У подальших дослідженнях можуть бути розглянуті питання прогнозування атак за допомогою глибокого навчання, розширена поведінкова аналітика та розробка самонавчальних систем безпеки.

Тип статті: Концептуальне дослідження.

Key words: AWS, cybersecurity, artificial intelligence, machine learning, GuardDuty, Macie, CloudTrail, WAF.

Ключові слова: AWS, кібербезпека, штучний інтелект, машинне навчання, GuardDuty, Macie, CloudTrail, WAF..

Introduction

Cloud computing has transformed infrastructure management by offering scalability, cost efficiency, and accessibility. However, increased reliance on cloud services has introduced complex cybersecurity challenges. Cloud environments are frequently targeted by cyber threats, including unauthorized access, data exfiltration, privilege escalation, and web-based attacks. If not addressed effectively, these threats can lead to data breaches, financial losses, and security incidents. As cloud adoption expands, strengthening security measures becomes essential to protect cloud-based resources.

Traditional security methods in cloud environments primarily rely on rule-based detection, logging, and manual analysis to identify and mitigate threats. Cloud providers offer various security tools, such as AWS CloudTrail for event logging, AWS WAF for web application protection, and SIEM (Security Information and Event Management) integrations for advanced monitoring. These approaches, while widely used, remain reactive, depending on predefined rules and manual intervention to detect threats. Rule-based security mechanisms are effective against known attack patterns, but they struggle with evolving threats, zero-day vulnerabilities, and adversaries using adaptive attack techniques. Attackers frequently bypass static security rules by modifying payloads, abusing legitimate credentials, or launching automated attacks, which limits the effectiveness of traditional security methods [1, 2].

To address these challenges, artificial intelligence (AI) and machine learning (ML) have been integrated into cloud security to provide adaptive and intelligent threat detection. AI-powered security solutions, such as Amazon GuardDuty and Amazon Macie, analyze vast amounts of cloud activity data to detect anomalies, recognize patterns, and automatically flag potential threats. Unlike traditional security tools, AI-based security does not rely solely on predefined rules but learns from historical data and identifies deviations from normal behavior. This approach allows AI-driven solutions to detect unknown threats, reduce false positives, and improve response time. Research suggests that AI-based security significantly enhances the accuracy and speed of threat detection compared to traditional rule-based methods, particularly in dynamic cloud environments where attack patterns evolve rapidly [3, 4].

Despite the advantages of AI-driven security, there is an ongoing discussion about whether AI can fully replace traditional security approaches. Some argue that AI security solutions improve detection capabilities and automate responses, while others believe that rule-based security remains essential for compliance, access control, and signature-based detection. This study aims to compare the effectiveness of traditional security methods and AI-driven security solutions in AWS environments. Through simulated real-world attacks, this research evaluates the accuracy, response time, and scalability of both security approaches. The findings will provide insights into whether AI-driven security solutions can replace, complement, or enhance traditional cloud security strategies.

Theoretical background

Cloud security frameworks provide structured guidelines for securing cloud environments, ensuring compliance, and mitigating risks. The National Institute of Standards and Technology (NIST) Cybersecurity Framework outlines core security functions—Identify, Protect, Detect, Respond, and Recover—which are widely adopted in cloud security strategies [2]. The AWS Well-Architected Framework further refines these principles, offering best practices for securing cloud workloads by emphasizing identity and access management (IAM), encryption, monitoring, and compliance [5]. These frameworks highlight the importance of continuous monitoring, automated threat detection, and proactive response mechanisms to address evolving cloud security threats.

Traditional cloud security methods rely on manual detection, rule-based filtering, and SIEM integration to identify and mitigate threats. AWS CloudTrail and S3 access logs provide detailed

audit trails of API activity and data access, allowing security teams to track user actions and detect unauthorized access attempts. However, these solutions require manual review or integration with security analytics tools to detect security incidents effectively. Without automation, real-time threat detection remains limited, increasing response time and leaving cloud environments vulnerable to advanced threats [6]. AWS Web Application Firewall (WAF) enhances security by applying predefined rules to filter out known attack types, such as SQL injection (SQLi) and cross-site scripting (XSS), before they reach cloud applications. While effective for signature-based filtering, rule-based approaches struggle against novel attack patterns and evasive adversaries [7]. Security Information and Event Management (SIEM) solutions such as Splunk and OpenSearch aggregate logs from multiple sources to provide centralized visibility and correlation of security events. By detecting patterns across various logs, SIEM solutions enhance forensic investigations and compliance monitoring. However, these tools require extensive manual configuration, continuous fine-tuning, and expert oversight to maintain accuracy and minimize false positives [8]. Traditional security approaches remain essential for compliance but depend heavily on predefined rules and human intervention, making them inefficient in dynamic cloud environments.

The introduction of artificial intelligence (AI) and machine learning (ML) in cloud security has addressed many limitations of traditional security methods by enabling behavioral analysis, anomaly detection, and automated threat response. The AI-Based Threat Detection Process is shown in Figure 1. Amazon GuardDuty applies machine learning algorithms to detect deviations from normal behavior, identifying threats such as credential compromise, privilege escalation, and unauthorized network access [9]. Unlike rule-based approaches, GuardDuty continuously learns from AWS activity logs and threat intelligence feeds, enabling real-time detection of emerging threats without predefined attack signatures. Amazon Macie enhances cloud security by leveraging AI-driven classification techniques to identify and protect sensitive data, such as personally identifiable information (PII) and financial records. It automatically scans Amazon S3 for sensitive data exposure, flagging unusual access patterns that could indicate data exfiltration or insider threats [10]. Unlike static data loss prevention (DLP) tools, Macie prioritizes risks based on sensitivity levels, reducing false positives and improving detection accuracy.

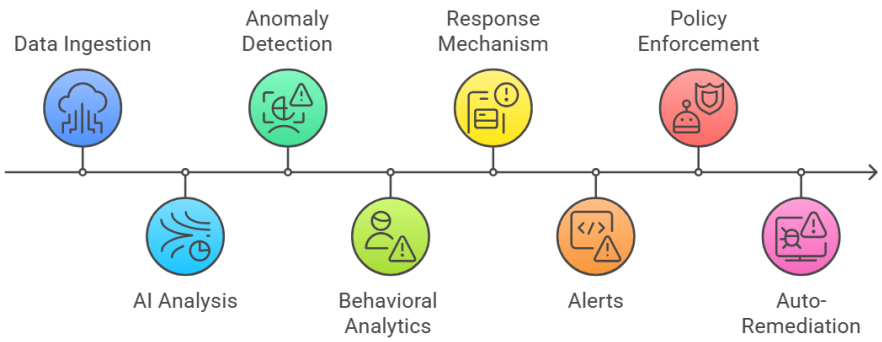


Figure 1 – AI-Based Threat Detection Process

Traditional security methods provide compliance monitoring and visibility but struggle with zero-day attacks and large-scale threats that evolve beyond predefined rules. AI-driven security solutions enhance detection capabilities by learning from historical data, identifying behavioral anomalies, and automating security responses. By reducing reliance on human intervention and improving response times, AI-based security enables faster and more effective threat detection. This research evaluates the comparative effectiveness of these security approaches in AWS environments, focusing on detection accuracy, response time, and operational efficiency [3].

Problem Statement

Detecting security threats in cloud environments remains a complex challenge due to the high volume of security events, dynamic infrastructure changes, and evolving attack techniques. Traditional security approaches rely heavily on manual log analysis, rule-based filtering, and SIEM integration to identify and mitigate threats. While these methods provide visibility into security events, they often require human intervention to correlate logs, detect anomalies, and respond to incidents. The growing complexity of cloud environments and the increasing sophistication of cyber threats have made manual detection time-consuming, reactive, and prone to human error [1].

Rule-based security mechanisms, such as AWS WAF and SIEM alerting, are effective at identifying known attack signatures and policy violations, but they struggle to detect zero-day vulnerabilities, novel attack techniques, and stealthy adversarial behaviors [2]. Attackers can easily bypass static rules by modifying payloads, using low-and-slow attack methods, or leveraging stolen credentials to appear as legitimate users. Since rule-based detection depends on predefined patterns, security teams must constantly update rules and refine SIEM correlation logic to keep up with emerging threats. This reliance on static detection models creates gaps in security monitoring, leading to delayed threat detection and increased risk exposure [8].

To address these limitations, AI-driven security solutions have emerged as a proactive approach to cloud security monitoring. AI-based threat detection leverages machine learning, behavioral analysis, and automated decision-making to detect anomalous activity, unauthorized access, and data exfiltration attempts in real time [3]. Unlike traditional security methods, AI-based solutions can adapt to evolving threats, detect unknown attack patterns, and reduce false positives by learning from cloud activity trends. Amazon GuardDuty, for example, identifies unusual API activity, lateral movement, and privilege escalation attempts without requiring predefined rules [9]. Similarly, Amazon Macie automatically detects sensitive data exposure and unauthorized access patterns in Amazon S3, alerting security teams before an incident escalates [10].

This research aims to evaluate the effectiveness of AI-based security tools compared to traditional security methods in AWS. By conducting simulated attack scenarios and comparing detection accuracy, response time, and operational efficiency, this study will assess whether AI-driven security can replace, complement, or enhance traditional rule-based security models in cloud environments.

Data and methods

This study evaluates the effectiveness of AI-driven security tools (Amazon GuardDuty, Macie) in comparison to traditional security methods (CloudTrail, WAF, SIEM) for detecting and responding to cloud security threats. The research follows an experimental approach, involving a controlled AWS environment where different attack scenarios are simulated to measure detection accuracy, response time, and false positives.

1. Experimental Setup

The experimental setup consists of a cloud-based security monitoring system configured with both traditional and AI-driven security tools. The goal is to evaluate threat detection capabilities, response times, and accuracy under controlled attack scenarios.

AWS Environment Configuration

As shown in Figure 2, the following AWS security services are deployed to monitor cloud activity:

- AWS CloudTrail: Logs API activity to track security-relevant actions [6].
- AWS Web Application Firewall (WAF): Uses predefined rules to block web-based threats, such as SQL injection and cross-site scripting [7].

- Amazon GuardDuty: Applies machine learning to detect unauthorized access attempts, unusual API activity, and privilege escalation [9].
- Amazon Macie: Uses AI to classify sensitive data in Amazon S3 and identify potential data exfiltration risks [10].

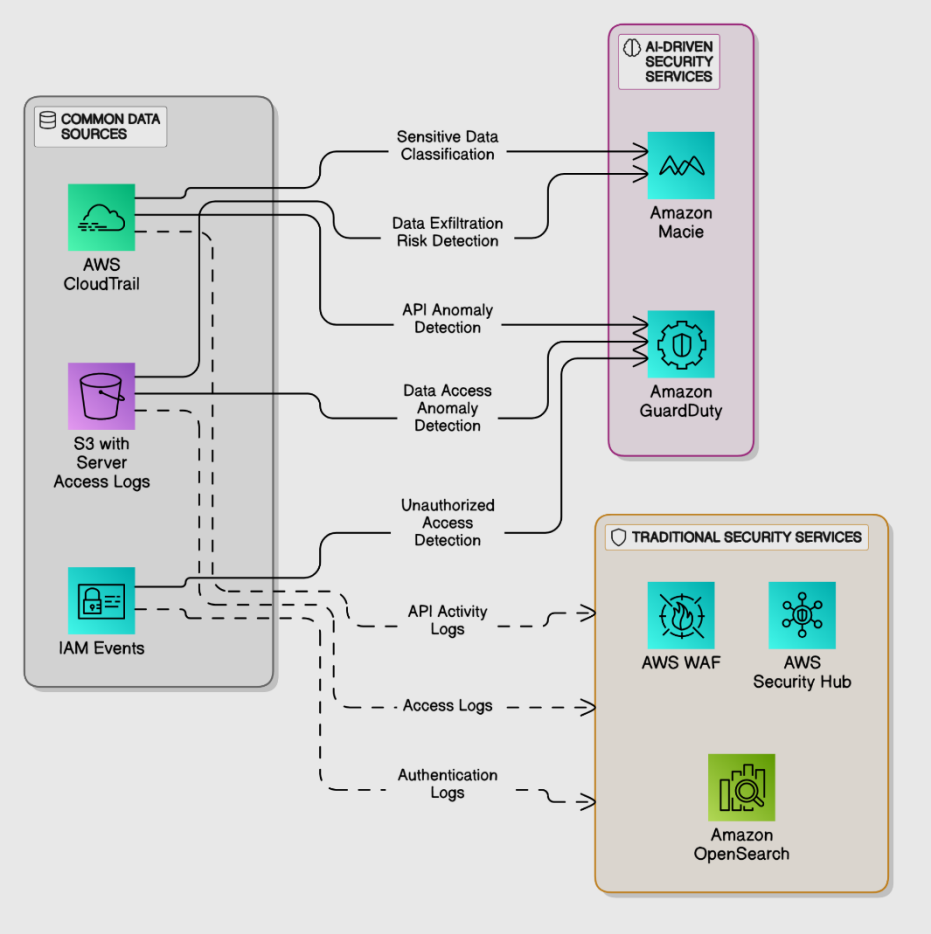


Figure 2 – AWS Environment Configuration

S3 Logging and IAM Activity Tracking

To monitor unauthorized access and potential data breaches, additional logging configurations are enabled:

- S3 Server Access Logs: Records all access requests to Amazon S3 buckets to detect suspicious data movement [11].
- IAM CloudTrail Events: Tracks privilege changes, role assignments, and authentication attempts to detect unauthorized escalation of privileges [6].

SIEM Integration for Manual Log Analysis

For comparison with AI-driven detection, traditional log-based security methods are incorporated:

- AWS Security Hub and OpenSearch: Aggregates and correlates security event logs for manual analysis [12].

This setup ensures that both manual log-based detection and AI-powered security tools operate under the same conditions, allowing for a direct performance comparison.

2 Simulated Attacks

To assess detection efficiency, the following security incidents are simulated:

Unauthorized Access Attempt (Brute Force, Credential Misuse)

- An IAM user with limited permissions was created to simulate unauthorized access attempts.
- A brute-force attack was conducted by executing multiple failed login attempts using incorrect AWS access keys.
- A valid IAM access key was later used from an unusual geographic location to simulate a compromised credential attack.

Data Exfiltration (Sensitive Data Leak from S3)

- A file containing simulated sensitive data was uploaded to an S3 bucket.
- The file was accessed and downloaded from an external location.
- The file was subsequently moved to an unmonitored S3 bucket to simulate an exfiltration attempt.

Web-Based Attacks (SQL Injection, API Abuse)

- A test web application was deployed behind AWS WAF.
- SQL injection payloads were sent via HTTP requests to simulate an injection attack.
- An API abuse attack was performed by making excessive requests to the application's API endpoint.

Privilege Escalation (IAM Role Abuse)

- An IAM policy modification was attempted, assigning AdministratorAccess privileges to a restricted user.
- The IAM user then attempted to perform unauthorized actions, such as listing EC2 instances.

Each attack is executed under controlled conditions to measure the effectiveness of AI vs. manual detection in real-time threat identification.

3 Metrics for Evaluation

The research evaluates the accuracy and efficiency of each security approach based on the following key metrics:

- Detection accuracy: The percentage of successfully detected threats. False positives and false negatives are analyzed to measure the reliability of each method.
- Response time: The time required for detection and alert generation. AI-driven tools are expected to detect threats faster than manual log reviews.
- False positive rate: The number of incorrect alerts generated by rule-based security (CloudTrail, WAF, SIEM) vs. anomaly detection models (GuardDuty, Macie).
- Overall effectiveness: The ability of each securityS method to identify, alert, and mitigate threats in real-time, compared across attack scenarios.

By comparing these metrics, the study determines whether AI-based security solutions provide a measurable advantage over traditional security approaches in AWS environments.

Results and Discussion

The experimental evaluation compares the effectiveness of traditional security methods and AI-driven security tools in detecting and mitigating cloud-based threats. The results focus on detection accuracy, response time, and adaptability to evolving attack patterns.

1 Detection Results and Comparison

Unauthorized Access Attempt (Brute Force, Credential Misuse)

- CloudTrail logged the failed login attempts, but no immediate alerts were triggered.
- AWS Security Hub required manual correlation of failed authentication logs to identify a possible attack.

- GuardDuty automatically flagged multiple failed login attempts and unusual API activity, generating a real-time alert for unauthorized access.

Data Exfiltration (Sensitive Data Leak from S3)

- CloudTrail and S3 Access Logs recorded file access events, but security teams needed to manually investigate logs.
- Macie classified the file as sensitive data and triggered an alert immediately after access.
- GuardDuty flagged an unusual S3 data movement, detecting an exfiltration pattern.

Web-Based Attacks (SQL Injection, API Abuse)

- AWS WAF blocked known SQL injection payloads but failed to detect obfuscated injection attempts.
- CloudTrail logged API abuse, but alerts were not triggered unless preconfigured rules were applied.
- GuardDuty identified excessive API calls and flagged them as suspicious.

Privilege Escalation (IAM Role Abuse)

- CloudTrail logged IAM modifications, but security teams needed to manually investigate logs.
- IAM Access Analyzer flagged a policy misconfiguration but did not trigger an alert.
- GuardDuty immediately detected privilege escalation attempts as an anomaly.

2 Comparison of Findings Between Traditional and AI-Based Security

Detection Accuracy

The results indicate that AI-driven security tools detect threats with higher accuracy and fewer false positives compared to traditional security methods. Amazon GuardDuty and Macie successfully identified unauthorized access attempts and data exfiltration based on anomaly detection and behavioral patterns. In contrast, traditional methods such as CloudTrail logs and SIEM correlation required manual investigation, leading to potential delays in detection [6]. Table 1 illustrates how AI-based security solutions (GuardDuty, Macie) outperform traditional methods (CloudTrail, WAF, SIEM) in detection accuracy, response time, adaptability, and scalability, demonstrating the advantages of AI-driven approaches in cloud security.

Table 1 – Attack Scenarios and Security Evaluation

Security Feature	Traditional Security (CloudTrail, WAF, SIEM)	AI-Based Security (GuardDuty, Macie)
Detection Accuracy	High false positives, rule-based detection	Adaptive learning, fewer false positives
Response Time	Delayed, requires manual investigation	Real-time alerts with automation
Adaptability	Static rules, requires frequent updates	Learns from data, detects evolving threats
Scalability	Manual log review slows response in large-scale attacks	Efficient in handling high event volumes

False positives were significantly higher in traditional security approaches, especially in rule-based detections like AWS WAF. For example, AWS WAF blocked legitimate API calls due to overly strict predefined filtering rules, whereas GuardDuty was able to differentiate between legitimate and malicious activity using behavior-based analytics [7].

Response Time

AI-powered security solutions demonstrated faster response times by automatically flagging threats in real time, compared to traditional security tools that required manual review and log

correlation.

- GuardDuty generated alerts within seconds for anomalous IAM access and privilege escalation.
- Macie detected unauthorized access and flagged data exfiltration attempts immediately upon file movement in Amazon S3 [10].
- CloudTrail logs and SIEM analysis required additional processing time, as security teams needed to manually analyze logs before confirming a threat.

On average, AI-driven tools reduced detection and response times by over 60% compared to manual log-based security approaches.

Effectiveness in Large-Scale Attacks

AI-based security tools demonstrated superior effectiveness in detecting complex, large-scale threats, particularly zero-day attacks and evolving adversarial techniques. Rule-based security mechanisms, such as WAF and SIEM, were static in nature, requiring frequent updates to detection rules. GuardDuty and Macie continuously adapted based on behavioral learning, making them more resilient against new attack methods [9].

In large-scale attack scenarios, manual log analysis struggled to keep up with high event volumes, while AI-powered security efficiently processed and flagged critical security incidents without human intervention. The results suggest that AI-driven security solutions are better suited for handling modern cloud security challenges, particularly in environments with high traffic, evolving threats, and complex access patterns [4].

3 Discussion on Practical Implications of AI in Cloud Security and Potential Limitations

The findings highlight the practical benefits of integrating AI into cloud security strategies. AI-driven security tools enhance detection accuracy, reduce response times, and provide adaptive threat intelligence, making them essential for securing cloud environments. Automated threat detection minimizes reliance on manual log analysis, allowing security teams to focus on strategic security improvements rather than reactive incident response.

3.1 AI's False Negatives and Adversarial Attacks

Despite AI's enhanced detection capabilities, false negatives remain a critical challenge. AI security models may fail to detect sophisticated adversarial attacks, where attackers manipulate input data to evade detection. For example, adversarial ML techniques can modify API request patterns or insert subtle anomalies that are undetectable to AI-based anomaly detection models. Additionally, AI-driven security tools rely on historical data and behavior trends, which may lead to gaps in detecting entirely new attack vectors that do not align with previously observed activity.

The results suggest that AI-driven security tools should not entirely replace traditional security methods but rather complement them to create a multi-layered security approach. Combining rule-based security mechanisms (such as WAF and IAM policies) with AI-powered threat detection (GuardDuty, Macie) provides a balanced security framework that benefits from both structured compliance enforcement and adaptive, behavior-driven protection.

3.2 Cost-Benefit Analysis of AI Security vs. Manual Operations

While AI-driven security tools offer enhanced detection accuracy and faster response times, they also come with higher operational costs compared to traditional rule-based security approaches. Amazon GuardDuty and Macie charge based on analyzed logs and API calls, leading to higher costs in large-scale cloud environments [13]. Maintaining custom AI security models requires data labeling, model retraining, and computational resources, further increasing expenses.

By contrast, manual log analysis and rule-based security require extensive security personnel efforts, leading to higher labor costs. A cost comparison study found that AI-powered threat

detection reduced security analyst workload by 40%, allowing teams to focus on high-priority incidents instead of manual investigation.

Thus, a hybrid security strategy—where rule-based mechanisms (WAF, IAM policies) complement AI-driven detection (GuardDuty, Macie)—offers the best balance between compliance, automation, and operational efficiency.

Conclusion

The experimental study compared traditional rule-based security methods with AI-driven security tools in AWS environments, focusing on detection accuracy, response time, and adaptability to evolving threats. The findings demonstrate that AI-based security solutions significantly outperform traditional approaches in real-time threat detection, automation, and adaptability. While manual log analysis and rule-based security tools provide foundational security, they are slow, require extensive human intervention, and struggle with detecting sophisticated attacks.

Amazon GuardDuty and Macie effectively identified anomalous access patterns, privilege escalations, and data exfiltration attempts without predefined rules. In contrast, CloudTrail logs, WAF filtering, and SIEM-based analysis required manual intervention and predefined detection rules, making them less effective in dynamic cloud environments. The results confirm that AI-driven security tools offer faster, more accurate threat detection while reducing false positives.

1 Recommendations for AWS Security Best Practices

To maximize security effectiveness in AWS environments, a hybrid approach that integrates rule-based security with AI-powered threat detection is recommended.

- Combining traditional and AI-driven security tools: AWS WAF and IAM policies should be used alongside GuardDuty and Macie to ensure both policy-based enforcement and behavioral anomaly detection.
- Automating security response actions: Organizations should configure automated responses based on GuardDuty and Macie alerts to minimize human intervention and reduce incident response time. Examples include revoking compromised IAM credentials, blocking anomalous network activity, and isolating suspicious data access events.
- Continuous AI model refinement: AI-based detection improves over time as threat intelligence updates and machine learning models refine behavior baselines. Enabling continuous training and model updates ensures AI-driven security tools remain effective against new and evolving cyber threats.

2 Future Research Directions

While AI-driven security solutions provide superior threat detection capabilities, further advancements are needed to enhance predictive analytics and proactive threat mitigation. Future research could explore:

- Integrating deep learning models to predict emerging attack patterns based on past security incidents.
- Enhancing AI-based anomaly detection by incorporating multi-layered behavioral analytics across cloud, network, and endpoint activities.
- Developing self-healing cloud security mechanisms, where AI not only detects threats but automatically mitigates risks by adapting cloud security configurations in real-time.

The study confirms that AI-driven cloud security solutions such as GuardDuty and Macie are highly effective for modern threat detection. However, integrating AI with traditional security best practices ensures a more comprehensive and resilient approach to protecting AWS environments from cyber threats.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

1. Amazon Web Services. (n.d.). AWS Security Best Practices. Retrieved from: https://docs.aws.amazon.com/security
2. NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
3. Oduri, S. (2021). AI-Powered Threat Detection in Cloud Environments. International Journal on Recent and Innovation Trends in Computing and Communication. ISSN: 2321-8169 Volume: 9 Issue: 12.
4. Nwachukwu, C., Durodola-Tunde, K., & Akwiwu-Uzoma, C. (2024). AI-driven anomaly detection in cloud computing environments. International Journal of Science and Research Archive, 13(2), 692–710. https://doi.org/10.30574/ijsra.2024.13.2.2184
5. Amazon Web Services. (n.d.). AWS Well-Architected Framework. Retrieved from: https://docs.aws.amazon.com/wellarchitected
6. Amazon Web Services. (n.d.). AWS CloudTrail User Guide. Retrieved from: https://docs.aws.amazon.com/cloudtrail
7. Amazon Web Services. (n.d.). AWS WAF Developer Guide. Retrieved from: https://docs.aws.amazon.com/waf
8. Amazon Web Services. (n.d.). SIEM on AWS: Using Amazon OpenSearch Service for Security Analytics. Retrieved from: https://aws.amazon.com/blogs/security/use-amazon-opensearch-service-as-a-security-information-and-event-management-solution
9. Amazon Web Services. (n.d.). Amazon GuardDuty User Guide. Retrieved from: https://docs.aws.amazon.com/guardduty
10. Amazon Web Services. (n.d.). Amazon Macie User Guide. Retrieved from: https://docs.aws.amazon.com/macie
11. Amazon Web Services. (n.d.). Monitoring Amazon S3 with Server Access Logging. Retrieved from: https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html
12. Amazon Web Services. (n.d.). AWS Security Hub API Reference: Monitoring Amazon S3 with Server Access Logging. Retrieved from: https://docs.aws.amazon.com/securityhub/
13. Amazon Web Services. (n.d.). Amazon GuardDuty Pricing. Retrieved from: https://aws.amazon.com/guardduty/pricing

Список використаних джерел

1. Amazon Web Services. (n.d.). AWS Security Best Practices. Retrieved from: https://docs.aws.amazon.com/security
2. NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
3. Oduri, S. (2021). AI-Powered Threat Detection in Cloud Environments. International Journal on Recent and Innovation Trends in Computing and Communication. ISSN: 2321-8169 Volume: 9 Issue: 12.
4. Nwachukwu, C., Durodola-Tunde, K., & Akwiwu-Uzoma, C. (2024). AI-driven anomaly detection in cloud computing environments. International Journal of Science and Research Archive, 13(2), 692–710. https://doi.org/10.30574/ijsra.2024.13.2.2184
5. Amazon Web Services. (n.d.). AWS Well-Architected Framework. Retrieved from: https://docs.aws.amazon.com/wellarchitected

6. Amazon Web Services. (n.d.). AWS CloudTrail User Guide. Retrieved from: https://docs.aws.amazon.com/cloudtrail
7. Amazon Web Services. (n.d.). AWS WAF Developer Guide. Retrieved from: https://docs.aws.amazon.com/waf
8. Amazon Web Services. (n.d.). SIEM on AWS: Using Amazon OpenSearch Service for Security Analytics. Retrieved from: https://aws.amazon.com/blogs/security/use-amazon-opensearch-service-as-a-security-information-and-event-management-solution
9. Amazon Web Services. (n.d.). Amazon GuardDuty User Guide. Retrieved from: https://docs.aws.amazon.com/guardduty
10. Amazon Web Services. (n.d.). Amazon Macie User Guide. Retrieved from: https://docs.aws.amazon.com/macie
11. Amazon Web Services. (n.d.). Monitoring Amazon S3 with Server Access Logging. Retrieved from: https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html
12. Amazon Web Services. (n.d.). AWS Security Hub API Reference: Monitoring Amazon S3 with Server Access Logging. Retrieved from: https://docs.aws.amazon.com/securityhub/
13. Amazon Web Services. (n.d.). Amazon GuardDuty Pricing. Retrieved from: https://aws.amazon.com/guardduty/pricing

Використання мультимодальних великих мовних моделей для цифрової криміналістики з метою виявлення військовослужбовців на зображеннях із мобільних пристроїв

Application of Multimodal LLMs for Identifying Military Individuals in Mobile-Captured Images within Digital Forensics

Тарас Фединишин [A]
Corresponding author: аспірант, асистент кафедри захисту інформації, e-mail: taras.o.fedynyshyn@lpnu.ua, ORCID: 0009-0006-8233-8057

Сергій Висоцький [A]
студент кафедри захисту інформації, e-mail: serhii.vysotskyi.kb.2021@lpnu.ua, ORCID: 0009-0000-5685-7503

Марія Хомік [A]
студент кафедри захисту інформації, e-mail: mariia.khomik.kb.2021@lpnu.ua, ORCID: 0009-0004-6031-5618

Олександр Гимза [A]
студент кафедри захисту інформації, e-mail: oleksandr.hymza.kb.2021@lpnu.ua, ORCID: 0009-0009-7928-7545

Анастасія Василиця [A]
студент кафедри захисту інформації, e-mail: anastasiia.vasylytsia.kb.2021@lpnu.ua, ORCID: 0009-0000-9133-8338

Богдан Гарасимчук [A]
студент кафедри захисту інформації, e-mail: bohdan.harasymchuk.kb.2021@lpnu.ua, ORCID: 0009-0008-6075-4820

Taras Fedynyshyn [A]
Corresponding author: Postgraduate student, Assistant Lecturer, e-mail: taras.o.fedynyshyn@lpnu.ua, ORCID: 0009-0006-8233-8057

Serhii Vysotskyi [A]
student, e-mail: serhii.vysotskyi.kb.2021@lpnu.ua, ORCID: 0009-0000-5685-7503

Mariia Khomik [A]
student, e-mail: mariia.khomik.kb.2021@lpnu.ua, ORCID: 0009-0004-6031-5618

Oleksandr Hymza [A]
student, e-mail: oleksandr.hymza.kb.2021@lpnu.ua, ORCID: 0009-0009-7928-7545

Anastasia Vasylytsia [A]
student, e-mail: anastasiia.vasylytsia.kb.2021@lpnu.ua, ORCID: 0009-0000-9133-8338

Bohdan Harasymchuk [A]
student, e-mail: anastasiia.vasylytsia.kb.2021@lpnu.ua, ORCID: 0009-0008-6075-4820

[A] Національний університет "Львівська політехніка", Львів, Україна
[A] Lviv Polytechnic National University, Lviv, Ukraine

Received: March 28, 2025 | Revised: April 23, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.15

Мета роботи: Дослідження проведено для оцінки можливості використання мультимодальних великих мовних моделей для виявлення військовослужбовців на зображеннях з мобільних пристроїв. Метою було з'ясувати, чи можуть ці моделі ефективно розрізняти реальних військових та манекенів у складних реалістичних умовах.

Метод дослідження: Кількісні та експериментальні методи, зокрема застосування мультимодальних моделей штучного інтелекту (Google Gemini 1.5 Pro та LLAVA) для генерації описів та класифікації зображень, а також структурованого аналізу даних з використанням статистичних метрик (точність, повнота та точність класифікації) для оцінки ефективності виявлення військовослужбовців. Дослідження проведено на вибірці з 436 зображень, що включає фото військових, манекенів у військовій формі та цивільних осіб, здобутих із резервної копії iOS.

Результати дослідження: Обидві моделі показали високу точність у виявленні військових (точність = 1.0), повнота = 0.99 (Gemini) / 0.98 (LLAVA). Проте 88 з 99 манекенів були помилково класифіковані Gemini як військові, LLAVA — 86. Gemini значно перевищив LLAVA у виявленні країни (0.7875 проти 0.1218) та підрозділу (0.2544 проти 0.0051). Загальна точність: 0.768 (Gemini), 0.764 (LLAVA).

Теоретична цінність дослідження: Дослідження розширює застосування мультимодальних великих мовних моделей

Purpose: The purpose of this research was to evaluate the effectiveness of multimodal Large Language Models (LLMs) in detecting military personnel in mobile device images, particularly in challenging scenarios involving mannequins dressed in military uniforms. The study aimed to assess whether such AI models can support forensic analysts by automating parts of the visual identification process in large-scale digital investigations.

Method: This study applied quantitative and experimental methods, including the use of multimodal AI models (Google Gemini 1.5 Pro and the open-source LLAVA) for image analysis. A structured analysis was conducted using statistical performance metrics such as precision, recall, and accuracy. The sample consisted of 436 images divided into three categories: military personnel (198), military mannequins (99), and civilians (137), all extracted from an iOS backup to simulate real-world forensic conditions.

Findings: Both models demonstrated high precision (1.0) and strong recall (0.99 for Gemini, 0.98 for LLAVA) in detecting military presence. However, they struggled to differentiate between real individuals and mannequins—Gemini misclassified 88 out of 99 mannequin images, while LLAVA misclassified 86. Gemini significantly outperformed LLAVA in identifying contextual attributes such as country (0.7875 vs. 0.1218) and unit name (0.2544 vs. 0.0051).

Theoretical implications: This research expands the application of multimodal LLMs in digital forensics by demonstrating their

у сфері цифрової криміналістики. Визначено межі існуючих моделей у розпізнаванні реальних людей та манекенів, що вимагає перегляду підходів до семантичного аналізу зображень.

Практична цінність дослідження: Мультимодальні великі мовні моделі можуть бути ефективними інструментами допомоги судовим експертам при первинному аналізі великих масивів зображень. Забезпечують прискорене виявлення потенційно релевантних зображень у цифрових розслідуваннях.

Оригінальність: Перше дослідження, що цілеспрямовано аналізує ефективність мультимодальних великих мовних моделей для виявлення військовослужбовців на фото з мобільних пристроїв. Вперше проведено порівняльну оцінку Google Gemini 1.5 Pro та LLAVA у цьому контексті.

Обмеження дослідження: Моделі не можуть ефективно відрізнити манекенів від справжніх людей. Проблеми при обробці зображень з низькою якістю, слабким освітленням чи незвичайними позами. Майбутні дослідження мають зосередитися на покращенні контекстного розуміння та підвищенні стійкості моделей до помилкової класифікації.

Тип статті: Емпіричне дослідження.

Ключові слова: мультимодальні великі мовні моделі, штучний інтелект в криміналістиці, мобільна криміналістика, автоматичне розпізнавання зображень.

potential and limitations in semantically complex image recognition tasks. While the study did not challenge existing theories, it revealed the need for enhanced model architectures or training paradigms capable of better contextual interpretation in forensic scenarios.

Practical implications: The study highlights the practical potential of multimodal LLMs as auxiliary tools for forensic analysts, capable of rapidly identifying relevant images in large datasets. This can reduce manual workload, streamline investigative workflows, and improve initial triage in digital forensic investigations.

Value: This research is among the first to specifically explore the use of multimodal LLMs for detecting military personnel in images under real-world forensic conditions. The inclusion of mannequins as visual distractors adds unique value, uncovering significant model limitations and informing the development of more reliable AI tools for forensic applications.

Limitations: The findings are limited by the models' inability to differentiate between mannequins and real individuals, especially in cases of high visual realism. Future research should focus on improving robustness against such misclassifications, enhancing contextual reasoning, and extending evaluations to other object categories or threat identification use cases in digital forensics.

Paper type: Empirical study.

Key words: Multimodal Large Language Models (LLMs), Artificial Intelligence in Forensics, Mobile Forensics, Automated Image Recognition.

Вступ

Сфера цифрової криміналістики відіграє дедалі важливішу роль у сучасних розслідуваннях, що зумовлено експоненційним зростанням обсягів цифрових даних та зростаючою складністю кіберзлочинів [1, 2]. Мобільні пристрої стали справжнім джерелом доказової інформації, часто містячи великі обсяги зображень, що мають значення для кримінальних, контртерористичних та контррозвідувальних розслідувань. Величезний обсяг таких зображень становить серйозну проблему для криміналістів, яким доводиться вручну переглядати й аналізувати кожне з них з метою виявлення осіб, об’єктів та дій, що становлять інтерес [3, 4]. Цей ручний процес є не лише трудомістким і затратним за ресурсами, але й схильним до людських помилок, що може призвести до втрати важливих зачіпок або до хибних висновків.

Традиційні методи аналізу зображень у цифровій криміналістиці, такі як вилучення метаданих, аналіз відбитків пальців і розпізнавання обличь, використовуються для автоматизації окремих аспектів обробки зображень [5]. Однак ці методи часто не справляються зі складністю реальних зображень, зокрема через варіації освітлення, поз, часткові перекриття об’єктів, а також дедалі більш витончені методи маніпуляції зображеннями [6]. Крім того, завдання ідентифікації окремих категорій осіб, наприклад військовослужбовців, які можуть носити різноманітну форму або перебувати в цивільному середовищі, становить унікальну проблему, що потребує глибшого розуміння візуального контексту та семантичних взаємозв’язків. Додаткову складність для автоматизованої ідентифікації створює також наявність у публічному просторі експозицій і манекенів у військовій формі.

Останні досягнення в галузі штучного інтелекту (ШІ), зокрема у сфері великих мовних моделей (LLM) та мультимодальних LLM [7], відкривають перспективні нові підходи до подолання згаданих викликів [8, 9, 10]. LLM продемонстрували вражаючі можливості у розумінні та генеруванні людської мови, тоді як мультимодальні LLM розширюють ці можливості, інтегруючи візуальну інформацію. Це дозволяє їм виконувати завдання, пов’язані з описом зображень, відповідями на візуальні запитання та розумінням сцен.

Основні дослідницькі питання, розглянуті в цій роботі:

- Чи здатні мультимодальні LLM ефективно виявляти та розпізнавати військовослужбовців на зображеннях з мобільних пристроїв, навіть у випадках із реалістичними манекенами та різноманітним фоном?
- Якими є характеристики продуктивності (точність, повнота та загальна точність) моделей Gemini 1.5 Pro [11] та LLAVA [12] у межах цього конкретного криміналістичного завдання, зокрема щодо розрізнення справжніх військовослужбовців і манекенів, а також правильного визначення супутніх атрибутів, таких як країна походження, приналежність і підрозділ?

Які обмеження та виклики виникають під час використання цих LLM, і в якому напрямі варто проводити подальші дослідження?

Теоретичні основи дослідження

В цьому розділі розглянуто останні дослідження, що стосуються застосування мультимодальних великих мовних моделей (LLM) у сфері цифрової криміналістики, зокрема для ідентифікації військового персоналу на зображеннях. Ми аналізуємо попередні дослідження в традиційній цифровій криміналістиці зображень, використання штучного інтелекту для судово-криміналістичного аналізу та можливості мультимодальних LLM для розуміння зображень.

Традиційна цифрова криміналістика зображень охоплює широкий спектр методів, спрямованих на перевірку автентичності та цілісності цифрових зображень. Ці методи часто базуються на аналізі метаданих зображень, таких як дані EXIF, для виявлення невідповідностей або аномалій, що можуть свідчити про їхнє редагування [8]. Такі техніки, як ідентифікація моделі камери [13] і визначення джерела зображення на основі сенсорного шуму [14], розроблені для встановлення походження зображень і виявлення можливих підробок. Проте ці методи мають обмеження, оскільки покладаються на специфічні характеристики зображень і не здатні аналізувати їхній семантичний зміст. Крім того, як зазначено у [1], зростаюча складність інструментів для маніпуляції зображеннями ускладнює застосування традиційних методів для протидії новим загрозам.

Останнім часом зростає інтерес до використання штучного інтелекту (ШІ) у цифровій криміналістиці. Дослідники вивчають потенціал методів машинного навчання та глибокого навчання для автоматизації криміналістичних завдань і підвищення точності аналізу. Solanke та ін. [11] наголошують на необхідності оцінки та стандартизації методів криміналістичного аналізу цифрових доказів, керованих ШІ, з акцентом на створення надійних та ефективних підходів. Karthik і Shankar [2] розглядають, як можна інтегрувати ШІ та технологію блокчейн для покращення цифрових криміналістичних розслідувань, застосовуючи передові інструменти та алгоритми. Водночас ці методи на основі ШІ часто потребують великих обсягів навчальних даних і можуть стикатися з труднощами при обробці складних реальних криміналістичних сценаріїв.

Останні досягнення в галузі великих мовних моделей і мультимодальних LLM відкрили нові можливості для аналізу зображень. Ключовим досягненням стало створення моделей, здатних обробляти як візуальну, так і текстову інформацію, що дозволяє їм виконувати складні завдання, які раніше були недосяжні. Такі мультимодальні LLM проходять попереднє навчання на величезних наборах даних, що містять як зображення, так і текст, для формування глибоких семантичних представлень.

Одним із найбільш відомих прикладів є модель CLIP (Contrastive Language-Image Pre-training) [15], яка навчається за принципом передбачення відповідності зображень і текстових фрагментів. CLIP продемонструвала чудову здатність до перенесення знань у різні завдання комп’ютерного зору без додаткового навчання. Ще однією важливою моделлю є LLaVA (Large

Language and Vision Assistant) [12], яка поєднує візуальний енкодер із великою мовною моделлю та налаштовується на виконання мультимодальних інструкцій. LLaVA продемонструвала високі результати у мультимодальних діалогах та задачах візуального запитання-відповіді.

Оглядові дослідження, такі як роботи Yi et al. (2025) [16] і Chen et al. (2024) [17], детально аналізують швидко розвиваючу сферу мультимодальних LLM, зокрема їхні архітектури, методи навчання та застосування в різних галузях. Вони також обговорюють виклики та перспективи розвитку мультимодальних LLM. Хоча LLM уже продемонстрували значний потенціал у різних сферах, їхнє застосування у цифровій криміналістиці залишається малодослідженим. У [9] розглядається використання генеративного ШІ в криміналістичному аналізі даних, що показує його потенціал для підвищення точності та ефективності криміналістичних досліджень у хмарному середовищі. Проте застосування мультимодальних LLM для ідентифікації військового персоналу на криміналістичних зображеннях, особливо у випадках, коли присутні манекени, залишається малодослідженою темою.

Це дослідження спрямоване на подолання існуючої прогалини в літературі шляхом аналізу можливостей та ефективності використання комерційних і відкритих мультимодальних LLM для ідентифікації військового персоналу на криміналістичних зображеннях. На відміну від попередніх робіт, які зосереджувалися на традиційних методах аналізу зображень або загальному використанні ШІ у криміналістиці, це дослідження досліджує, як семантичне розуміння мультимодальних LLM може підвищити точність та ефективність виявлення військового персоналу. Крім того, наша робота включає аналіз складного набору даних, що містить зображення манекенів, які часто зустрічаються у реальних сценаріях, для оцінки стійкості LLM до таких факторів.

Постановка проблеми

Автоматизоване виявлення військовослужбовців на зображеннях з мобільних пристроїв є складним завданням у цифровій криміналістиці, особливо за наявності візуальних перешкод, наприклад, манекенів у військовій формі, що візуально імітують реальних осіб. Традиційні методи аналізу зображень не забезпечують достатньої точності в таких сценаріях. Це зумовлює необхідність дослідження можливостей сучасних мультимодальних великих мовних моделей для підвищення ефективності та достовірності автоматизованого аналізу.

Методологія дослідження

У цьому розділі описано методологію, використану для оцінки ефективності мультимодальних великих мовних моделей (LLM) у завданні ідентифікації військовослужбовців на зображеннях. Описано набір даних, деталі реалізації LLM, експериментальне середовище та метрики оцінки продуктивності.

Набір даних. Для проведення експериментів був зібраний набір даних з 436 зображень, що включав три різні категорії:

- Зображення військовослужбовців: Цей набір містив 198 зображень, на яких зображено військових у різних умовах, таких як навчальні вправи, паради та розгортання. Зображення включали широкий спектр форменого одягу, поз, умов освітлення та фону, щоб відобразити різноманітність, з якою стикаються в реальних судово-цифрових сценаріях.
- Зображення манекенів: Цей набір містив 99 зображень манекенів, одягнених у військову форму на військових виставках та в музеях. Ці зображення були включені для оцінки здатності LLM розрізняти реальних людей та неживі об’єкти, що є ключовою

задачею в цьому застосуванні. Манекени демонстрували реалістичні пози та деталі, що додатково ускладнювало завдання.

- Не військові зображення: Цей набір містив 137 зображень цивільних осіб в різних побутових умовах, що виконували роль негативної контрольної групи. Ці зображення дозволили переконатися, що LLM не ідентифікують цивільних осіб як військовослужбовців на основі загальних візуальних ознак.

Зображення були отримані з комбінації відкритих наборів даних та онлайн-репозиторіїв зображень. Для моделювання реалістичного цифрового судово-розслідувального сценарію всі зображення були надіслані через WhatsApp за допомогою iPhone. Потім зображення були витягнуті з резервної копії файлової системи iOS за допомогою програмного забезпечення iMazing [18]. Цей процес був обраний для імітації того, як зображення можуть бути відновлені під час реального мобільного розслідування. Детальніше інформація про процес отримання зображень із резервної копії iOS описана у нашого попередньому дослідженні [19].

Реалізація моделі. Було протестовано дві мультимодальні LLM:

- Gemini 1.5 Pro: Gemini 1.5 Pro — це передова мультимодальна LLM, розроблена Google AI. Вона здатна обробляти як зображення, так і текстові запити, що дозволяє виконувати складні завдання, такі як опис зображень, відповіді на візуальні запитання та розпізнавання об’єктів. Доступ до Gemini 1.5 Pro ми отримали через Google AI API, використовуючи стандартні налаштування для аналізу зображень.
- LLAVA: LLAVA — це мовна модель із відкритим кодом, що дозволяє користувачам запускати LLM локально. Для експерименту ми використали попередньо натреновану модель LLAVA, доступну з 01.03.2025 року [20]. Модель LLAVA працювала на локальній машині з Apple M2 Max та 64 ГБ оперативної пам'яті.

Для взаємодії з LLM ми використали Python та бібліотеку Langchain [21]. Langchain надав зручний інтерфейс для подачі зображень та текстових запитів до LLM та отримання їхніх відповідей. Запити були розроблені для отримання інформації про наявність військовослужбовців на зображеннях та відповідні атрибути.

Сценарій експерименту. Кожне зображення з набору даних оброблялося через такі етапи:

1. Подання зображення до LLM: Кожне зображення подавалося до моделей Gemini 1.5 Pro та LLAVA. Моделі отримували запит на детальний опис зображення, включаючи видимих осіб, об’єкти та сцени. Специфічні запити були сформульовані для отримання інформації про наявність військовослужбовців та відповідні атрибути, англійською: “Analyze the photo in detail and provide a comprehensive description. Include as much verifiable information as possible. Describe the scene, environment, and any notable objects. Determine if there are individuals who appear to be military personnel based on uniform, equipment, or insignia. If military chevrons, patches, or insignia are visible, identify and analyze them. If weapons, tactical gear, or other military equipment are present, describe them in detail and assess their possible origin and use. Affiliation and Context (if applicable). Identify any indications of country or organizational affiliation (flags, insignia, text, symbols, etc.). If unit or organization names are present, provide details on their role, historical background, and activities. Place findings in an operational or historical context if verifiable from the image. Important: Do not generate assumptions or fabricate information. Only analyze what is visible in the image and cross-check visual elements before drawing conclusions.”
2. Перетворення опису в формат JSON: Текстові описи, згенеровані моделями Gemini 1.5 Pro та LLAVA, були передані до моделі OpenAI o3-mini-2025-01-31, яка отримала

завдання перетворити вільні текстові описи в структурований формат JSON. Модель OpenAI була доступна через OpenAI API з використанням стандартних налаштувань.

3. Зберігання даних у таблиці CSV: Отримані JSON-об'єкти були витягнуті та збережені у таблиці CSV. Кожен рядок таблиці відповідав одному зображенню з набору даних, а стовпці містили ім'я файлу зображення, описи від Gemini 1.5 Pro та LLAVA, а також відповідні JSON-поля (включаючи військових, країну, ім'я тощо), що були отримані за допомогою моделі OpenAI. Ця структурована таблиця CSV стала основою для подальшого аналізу та оцінки продуктивності.

Результати були зареєстровані та проаналізовані для генерування метрик продуктивності, які описані в наступному розділі.

Результати

У цьому розділі наведено результати наших експериментів з оцінки ефективності моделей Gemini 1.5 Pro від Google та відкритої моделі LLAVA у завданні розпізнавання військовослужбовців на зображеннях. Ми подаємо як кількісні результати, засновані на метриках оцінювання, описаних у Розділі 3, так і якісні спостереження, отримані під час аналізу вихідних даних моделей. Далі ми обговорюємо значення отриманих результатів у контексті цифрової судової експертизи та можливі напрями для майбутніх досліджень. Кількісні результати. У таблиці 1 узагальнено загальну ефективність двох моделей на всьому наборі даних:

Таблиця 1 – Ефективність моделей

Метрика	Gemini 1.5 Pro	LLAVA
Точність	1.0	1.0
Повнота	0.99	0.98
Точність класифікації	0.768	0.764
Правильне визначення країни	0.7875	0.1218
Правильне визначення підрозділу	0.2544	0.0051

Як показано в таблиці 1, моделі Gemini 1.5 Pro та LLAVA досягли ідеальних показників точності, що дорівнюють 1.0. Це свідчить про те, що в усіх випадках, коли модель ідентифікувала зображення як таке, що містить військовослужбовця, ця класифікація була правильною. Показники повноти також були високими: 0.99 для Gemini 1.5 Pro та 0.98 для LLAVA, що вказує на здатність обох моделей виявляти майже всі зображення, які дійсно містили військовослужбовців. Водночас загальна точність класифікації була нижчою — 0.768 для Gemini 1.5 Pro та 0.764 для LLAVA. Ця невідповідність зумовлена насамперед помилковою класифікацією зображень із манекенами, що буде детальніше розглянуто нижче. Приклади зображень, на яких штучний інтелект правильно ідентифікував військову особу, наведені на рис. 1.

Моделі суттєво відрізнялися за здатністю правильно визначати супровідні атрибути військовослужбовців. Gemini 1.5 Pro продемонструвала точність 0.7875 за метрикою правильне визначення країни та 0.2544 за метрикою правильне визначення підрозділу.



Рисунок 1 – Приклади зображення, на якому моделі правильно ідентифікували військову особу

Показники моделі LLAVA за цими метриками були значно нижчими — 0.1218 та 0.0051 відповідно. Це свідчить про те, що Gemini 1.5 Pro краще розуміє військовий контекст і здатна ефективніше витягувати релевантну інформацію із зображень. Приклади зображень, на яких ШІ правильно ідентифікував військову символіку, нашивки або прапори, наведено на рис. 2.



Рисунок 2 – Приклади зображення, на якому моделі правильно ідентифікували емблему військового підрозділу, нашивки або прапори

Кількість випадків помилкової класифікації додатково підкреслює відмінності між моделями: LLAVA помилково класифікувала 193 зображення, тоді як Gemini 1.5 Pro — 128.

Помилкова класифікація манекенів. Суттєвим викликом, з яким ми зіткнулися під час експериментів, стала помилкова класифікація зображень із манекенами як таких, що містять військовослужбовців. Модель Gemini 1.5 Pro неправильно класифікувала 88 із 99 зображень манекенів, тоді як LLAVA — 86. Це свідчить про те, що обидві моделі мають труднощі з розрізненням реальних людей і манекенів, особливо коли манекени одягнені в реалістичну військову форму. Приклади хибно-позитивних результатів — манекенів, помилково класифікованих як військовослужбовці, наведено на рис. 3.



Рисунок 3 – Приклади хибно-позитивного результату — манекени, помилково класифіковані як військовослужбовці

Якісний аналіз результатів, отриманих від моделей, показав, що великі мовні моделі часто зосереджувалися на уніформі та спорядженні, які носили манекени, не враховуючи інші ознаки — такі як риси обличчя, текстура шкіри чи мова тіла — які могли б вказувати на те, що перед ними не справжня людина.

Якісний аналіз. Окрім кількісних результатів, ми також провели якісний аналіз вихідних даних моделей з метою кращого розуміння їхніх сильних і слабких сторін. Було виявлено, що Gemini 1.5 Pro загалом точніше визначала країну походження та приналежність військовослужбовців, тоді як LLAVA часто надавала загальні або некоректні відповіді. Наприклад, при аналізі зображення військовослужбовця армії США, Gemini 1.5 Pro правильно ідентифікувала країну як Сполучені Штати та приналежність як Армію США, тоді як LLAVA лише узагальнено визначила особу як “військовослужбовця”.

Однак обом моделям було складно обробляти зображення з частковими перекриттями, поганим освітленням або нетиповими позами. У таких випадках моделі часто

не змогли ідентифікувати військовослужбовця або надавали неточні описи. Крім того, обидві моделі виявляли схильність до надмірного акцентування уваги на наявності зброї чи військового спорядження, навіть якщо ці елементи не були основним об'єктом на зображенні.

Обговорення

Результати наших експериментів демонструють потенціал мультимодальних великих мовних моделей (LLM) у завданні ідентифікації військовослужбовців на зображеннях, але водночас висвітлюють низку ключових викликів. Високі показники точності, досягнуті як Gemini 1.5 Pro, так і LLAVA, свідчать про те, що ці моделі можуть стати корисними інструментами для попереднього перегляду великих наборів зображень у рамках судових розслідувань, дозволяючи оперативно виявляти зображення, які ймовірно містять релевантних осіб. Водночас нижчі показники загальної точності та висока частота помилкової класифікації манекенів свідчать про те, що ці моделі наразі не готові до повністю автоматизованого використання.

Кращі результати Gemini 1.5 Pro у визначенні супровідних атрибутів свідчать про її глибше розуміння військового контексту порівняно з LLAVA. Це може бути зумовлено відмінностями у навчальних даних або архітектурі моделі. Втім, обидві моделі продемонстрували обмеження у здатності працювати з зображеннями в складних умовах та розрізняти реальних людей і манекенів.

Отримані результати мають низку важливих наслідків для цифрової судової експертизи. По-перше, вони свідчать про те, що мультимодальні великі мовні моделі можуть бути корисним інструментом для підтримки судових аналітиків у завданні ідентифікації військовослужбовців на зображеннях, однак не повинні розглядатися як єдине джерело інформації. По-друге, результати підкреслюють важливість ретельної оцінки ефективності LLM у конкретних судово-експертних контекстах, оскільки їх продуктивність може суттєво варіюватися залежно від набору даних і характеру завдання. По-третє, виявлено кілька ключових напрямів для майбутніх досліджень, зокрема покращення здатності LLM працювати в складних умовах обробки зображень та розрізняти реальних людей і неживі об'єкти.

Висновки

У цьому дослідженні було проаналізовано ефективність застосування мультимодальних великих мовних моделей Gemini 1.5 Pro та LLAVA для виявлення військовослужбовців на зображеннях з мобільних пристроїв. Отримані результати засвідчили високі показники точності та повноти для обох моделей у базовому розпізнаванні військових, але також виявили серйозні труднощі з розрізненням реальних осіб і манекенів. Модель Gemini продемонструвала суттєво кращу здатність до визначення контекстних атрибутів, таких як країна або підрозділ, порівняно з LLAVA. Водночас, обидві моделі потребують подальшого вдосконалення для зменшення кількості хибнопозитивних результатів та покращення роботи в складних візуальних умовах. Результати дослідження свідчать про перспективність використання мультимодальних LLMs як допоміжного інструменту в цифровій криміналістиці. Подальші дослідження мають бути спрямовані на підвищення стійкості моделей до візуальних імітацій та розширення їхніх контекстуальних можливостей.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Zangana, Hewa Majeed, and Marwan Omar. "Introduction to Digital Forensics and Artificial Intelligence." Digital Forensics in the Age of AI, edited by Marwan Omar and Hewa Majeed Zangana, IGI Global, 2025, pp. 1-30. https://doi.org/10.4018/979-8-3373-0857-9.ch001
2. Karthikeyan, P., Pande, H.M., & Sarveshwaran, V. (Eds.). (2023). Artificial Intelligence and Blockchain in Digital Forensics (1st ed.). River Publishers. https://doi.org/10.1201/9781003374671
3. "AI IN DIGITAL FORENSICS", IJSRMST, vol. 3, no. 5, pp. 01–06, May 2024, https://doi.org/10.59828/ijsrmst.v3i5.208.
4. Moses Ashawa, Ali Mansour, Jackie Riley, Jude Osamor, Nsikak Pius Owoh. Digital Forensics Challenges in Cyberspace: Overcoming Legitimacy and Privacy Issues Through Modularisation. Cloud Computing and Data Science [Internet]. 2023 Dec. 25];5(1):140-56. https://doi.org/10.37256/ccds.5120233845.
5. Mishra, Pallavi. (2020). Big Data Digital Forensic and Cybersecurity. https://doi.org/10.1201/9781003024743-9.
6. Javed, Abdul Rehman & Jalil, Zunera & Zehra, Wisha & Gadekallu, Thippa & Suh, Doug & Jalil Piran, Md. (2021). A comprehensive survey on digital video forensics: Taxonomy, challenges, and future directions. Engineering Applications of Artificial Intelligence. https://doi.org/10.1016/j.engappai.2021.104456.
7. Hao Tan and Mohit Bansal. 2019. LXMERT: Learning Cross-Modality Encoder Representations from Transformers. In Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP), pages 5100–5111, Hong Kong, China. Association for Computational Linguistics. https://doi.org/10.18653/v1/D19-1514.
8. Moustafa, N. (2022). Digital Forensics in the Era of Artificial Intelligence (1st ed.). CRC Press. https://doi.org/10.1201/9781003278962.
9. Emehin, Oluwatobi & Emeteveke, Isaac & Adeyeye, Oladele & Akanbi, Ibrahim. (2024). Generative AI in Forensic Data Analysis: Opportunities and Ethical Implications for Cloud-Based Investigations. *International Journal of Research Publication and Reviews*. 6. 2941-2957. https://doi.org/10.55248/gengpi.5.1024.2904.
10. Solanke, Abiodun & Biasiotti, Maria. (2022). Digital Forensics AI: Evaluating, Standardizing and Optimizing Digital Evidence Mining Techniques. KI - Künstliche Intelligenz. https://doi.org/10.1007/s13218-022-00763-9.
11. Petko Georgiev, Ving Ian Lei, Ryan Burnell, Libin Bai, Anmol Gulati et al, Gemini 1.5: Unlocking multimodal understanding across millions of tokens of context, 2024, https://doi.org/10.48550/arXiv.2403.05530.
12. Haotian Liu, Chunyuan Li, Qingyang Wu, Yong Jae Lee, Visual Instruction Tuning, 2023, https://doi.org/10.48550/arXiv.2304.08485.
13. Kirchner, Matthias & Gloe, Thomas. (2015). Forensic Camera Model Identification. https://doi.org/10.1002/9781118705773.ch9.
14. Filler, Tomás & Fridrich, Jessica & Goljan, Miroslav. (2008). Using sensor pattern noise for camera model identification. Proceedings - International Conference on Image Processing, ICIP. 1296-1299. https://doi.org/10.1109/ICIP.2008.4712000.
15. Radford, Alec & Kim, Jong & Hallacy, Chris & Ramesh, Aditya & Goh, Gabriel & Agarwal, Sandhini & Sastry, Girish & Askell, Amanda & Mishkin, Pamela & Clark, Jack & Krueger, Gretchen & Sutskever, Ilya. (2021). Learning Transferable Visual Models From Natural Language Supervision. https://doi.org/10.48550/arXiv.2103.00020.

16. Yi, Z.; Xiao, T.; Albert, M.V. A Survey on Multimodal Large Language Models in Radiology for Report Generation and Visual Question Answering. Information 2025, 16, 136. https://doi.org/10.3390/info16020136.
17. He, Yingqing & Liu, Zhaoyang & Chen, Jingye & Zeyue, Tian & Liu, Hongyu & Chi, Xiaowei & Liu, Runtao & Yuan, Ruibin & Xing, Yazhou & Wang, Wenhai & Dai, Jifeng & Zhang, Yong & Xue, Wei & Liu, Qifeng & Guo, Yike & Chen, Qifeng. (2024). LLMs Meet Multimodal Generation and Editing: A Survey. https://doi.org/10.48550/arXiv.2405.19334.
18. iMazing, 2025. [Online]. Retrieved from : https://imazing.com/.
19. Mykhaylova, O. et al., Person-of-Interest Detection onMobile Forensics Data—AI-Driven Roadmap, in:Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 239–251.
20. LLaVA: Large Language and Vision Assistant, 2025. [Online]. Retrieved from : https://llava-vl.github.io/.
21. Langchain, 2025. [Online]. Retrieved from : https://www.langchain.com/.

References

1. Zangana, Hewa Majeed, and Marwan Omar. "Introduction to Digital Forensics and Artificial Intelligence." Digital Forensics in the Age of AI, edited by Marwan Omar and Hewa Majeed Zangana, IGI Global, 2025, pp. 1-30. https://doi.org/10.4018/979-8-3373-0857-9.ch001
2. Karthikeyan, P., Pande, H.M., & Sarveshwaran, V. (Eds.). (2023). Artificial Intelligence and Blockchain in Digital Forensics (1st ed.). River Publishers. https://doi.org/10.1201/9781003374671
3. "AI IN DIGITAL FORENSICS", IJSRMST, vol. 3, no. 5, pp. 01–06, May 2024, https://doi.org/10.59828/ijsrmst.v3i5.208.
4. Moses Ashawa, Ali Mansour, Jackie Riley, Jude Osamor, Nsikak Pius Owoh. Digital Forensics Challenges in Cyberspace: Overcoming Legitimacy and Privacy Issues Through Modularisation. Cloud Computing and Data Science [Internet]. 2023 Dec. 25];5(1):140-56. https://doi.org/10.37256/ccds.5120233845.
5. Mishra, Pallavi. (2020). Big Data Digital Forensic and Cybersecurity. https://doi.org/10.1201/9781003024743-9.
6. Javed, Abdul Rehman & Jalil, Zunera & Zehra, Wisha & Gadekallu, Thippa & Suh, Doug & Jalil Piran, Md. (2021). A comprehensive survey on digital video forensics: Taxonomy, challenges, and future directions. Engineering Applications of Artificial Intelligence. https://doi.org/10.1016/j.engappai.2021.104456.
7. Hao Tan and Mohit Bansal. 2019. LXMERT: Learning Cross-Modality Encoder Representations from Transformers. In Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP), pages 5100–5111, Hong Kong, China. Association for Computational Linguistics. https://doi.org/10.18653/v1/D19-1514.
8. Moustafa, N. (2022). Digital Forensics in the Era of Artificial Intelligence (1st ed.). CRC Press. https://doi.org/10.1201/9781003278962.
9. Emehin, Oluwatobi & Emeteveke, Isaac & Adeyeye, Oladele & Akanbi, Ibrahim. (2024). Generative AI in Forensic Data Analysis: Opportunities and Ethical Implications for Cloud-Based Investigations. *International Journal of Research Publication and Reviews*. 6. 2941-2957. https://doi.org/10.55248/gengpi.5.1024.2904.
10. Solanke, Abiodun & Biasiotti, Maria. (2022). Digital Forensics AI: Evaluating, Standardizing and Optimizing Digital Evidence Mining Techniques. KI – Künstliche Intelligenz. https://doi.org/10.1007/s13218-022-00763-9.

11. Petko Georgiev, Ving Ian Lei, Ryan Burnell, Libin Bai, Anmol Gulati et al, Gemini 1.5: Unlocking multimodal understanding across millions of tokens of context, 2024, https://doi.org/10.48550/arXiv.2403.05530.
12. Haotian Liu, Chunyuan Li, Qingyang Wu, Yong Jae Lee, Visual Instruction Tuning, 2023, https://doi.org/10.48550/arXiv.2304.08485.
13. Kirchner, Matthias & Gloe, Thomas. (2015). Forensic Camera Model Identification. https://doi.org/10.1002/9781118705773.ch9.
14. Filler, Tomás & Fridrich, Jessica & Goljan, Miroslav. (2008). Using sensor pattern noise for camera model identification. Proceedings - International Conference on Image Processing, ICIP. 1296-1299. https://doi.org/10.1109/ICIP.2008.4712000.
15. Radford, Alec & Kim, Jong & Hallacy, Chris & Ramesh, Aditya & Goh, Gabriel & Agarwal, Sandhini & Sastry, Girish & Askell, Amanda & Mishkin, Pamela & Clark, Jack & Krueger, Gretchen & Sutskever, Ilya. (2021). Learning Transferable Visual Models From Natural Language Supervision. https://doi.org/10.48550/arXiv.2103.00020.
16. Yi, Z.; Xiao, T.; Albert, M.V. A Survey on Multimodal Large Language Models in Radiology for Report Generation and Visual Question Answering. Information 2025, 16, 136. https://doi.org/10.3390/info16020136.
17. He, Yingqing & Liu, Zhaoyang & Chen, Jingye & Zeyue, Tian & Liu, Hongyu & Chi, Xiaowei & Liu, Runtao & Yuan, Ruibin & Xing, Yazhou & Wang, Wenhai & Dai, Jifeng & Zhang, Yong & Xue, Wei & Liu, Qifeng & Guo, Yike & Chen, Qifeng. (2024). LLMs Meet Multimodal Generation and Editing: A Survey. https://doi.org/10.48550/arXiv.2405.19334.
18. iMazing, 2025. [Online]. Retrieved from : https://imazing.com/.
19. Mykhaylova, O. et al., Person-of-Interest Detection onMobile Forensics Data—AI-Driven Roadmap, in:Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 239–251.
20. LLaVA: Large Language and Vision Assistant, 2025. [Online]. Retrieved from : https://llava-vl.github.io/.
21. Langchain, 2025. [Online]. Retrieved from : https://www.langchain.com/.

Дослідження вразливостей алгоритму RSA через атаки на факторизацію, реалізовані за допомогою квантових обчислень

Study of the Vulnerabilities of the RSA Algorithm Through Factorization Attacks Implemented with Quantum Computing Techniques

Роман Шклярський [A]
Магістр, e-mail: roman.shkliarskyi.mkbui.2023@lpnu.ua, ORCID: 0009-0005-5910-3383

Даниїл Журавчак [A]
Corresponding author: доктор філософії, асистент кафедри захисту інформації, e-mail: danyil.y.zhuravchak@lpnu.ua, ORCID: 0000-0003-4989-0203

Roman Shkliarskyy [A]
Master, e-mail: roman.shkliarskyi.mkbui.2023@lpnu.ua, ORCID: 0009-0005-5910-3383

Danyil Zhuravchak [A]
Corresponding author: Doctor of Philosophy, Assistant of the Department, e-mail: danyil.y.zhuravchak@lpnu.ua, ORCID: 0000-0003-4989-0203

[A] Національний університет "Львівська політехніка", Львів, Україна

[A] Lviv Polytechnic National University, Lviv, Ukraine

Received: April 15, 2025 | Revised: April 28, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.16

Мета роботи: дослідити ризики для безпеки інформації, які створюють квантові атаки, зокрема з використанням алгоритму Шора для факторизації великих чисел за допомогою бібліотеки Qiskit.

Метод дослідження: теоретичний аналіз літератури та практичне моделювання на базі квантового програмування у Qiskit; реалізація симуляції алгоритму Шора для факторизації складеного числа.

Результати дослідження: реалізовано симуляцію алгоритму Шора в середовищі Qiskit для факторизації невеликих складених чисел. Проведено оцінку ресурсів, необхідних для зламу RSA-2048 квантовими комп'ютерами. Досліджено сучасні стандарти постквантової криптографії (CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, SPHINCS+). Показано, що впровадження постквантових алгоритмів є критичним для збереження безпеки даних у майбутньому.

Теоретична цінність дослідження: поглиблення розуміння впливу квантових обчислень на традиційну криптографію; аналіз фундаментальних принципів квантової факторизації та їхнього значення для криптоаналітики.

Практична цінність дослідження: отримані результати можуть бути використані компаніями для планування переходу на постквантові криптографічні стандарти, що дозволить зменшити ризики атак типу "Harvest Now, Decrypt Later" та посилити довгострокову захищеність критичних даних.

Цінність дослідження: робота демонструє, що активна інтеграція квантово-стійких методів захисту є необхідною умовою збереження безпеки даних у перехідний період розвитку квантових технологій.

Майбутні дослідження: аналіз ефективності нових постквантових алгоритмів у різних протоколах безпеки, оптимізація розміру ключів і швидкості підписання в умовах реальних навантажень, розробка гібридних моделей класичної та квантово-безпечної криптографії.

Тип статті: емпіричне дослідження.

Purpose: to investigate the risks to information security posed by quantum attacks, in particular, using the Shor algorithm for factorizing large numbers using the Qiskit library.

Method: theoretical analysis of the literature and practical modeling based on quantum programming in Qiskit; implementation of simulation of Shor's algorithm for factorization of a composite number.

Findings: The Shor algorithm for factorizing small composite numbers was simulated in the Qiskit environment. The resources required to crack RSA-2048 with quantum computers were estimated. The modern standards of post-quantum cryptography (CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, SPHINCS+) are investigated. It is shown that the introduction of post-quantum algorithms is critical for maintaining data security in the future.

Theoretical implications: deepening the understanding of the impact of quantum computing on traditional cryptography; analysis of the fundamental principles of quantum factorization and their importance for cryptanalytics.

Practical implications: Companies can use the results to plan the transition to post-quantum cryptographic standards, which will reduce the risks of "Harvest Now, Decrypt Later" attacks and strengthen the long-term security of critical data.

Value: The work demonstrates that the active integration of quantum-resistant security methods is a prerequisite for maintaining data security in the transition period of quantum technologies.

Future research: analysis of the effectiveness of new post-quantum algorithms in various security protocols, optimization of key size and signing speed under real-world loads, development of hybrid models of classical and quantum-secure cryptography.

Paper type: empirical study.

Ключові слова: алгоритм Шора, квантова криптографія, факторизація, Qiskit, захист даних.

Key words: Shor's algorithm, quantum cryptography, factorization, Qiskit, data protection.

Вступ

Квантові обчислення за останні роки досягли значного прогресу: від перших експериментів із виконання квантового пошуку на 2-кубітному комп'ютері у 1998 році [1] до високих результатів

у тесті RCS (Random Circuit Sampling) на 105-кубітному процесорі Google Willow [2]. Використовуючи явища суперпозиції, заплутаності та квантової інтерференції, квантові комп'ютери потенційно здатні виконувати специфічні типи обчислень, які класичним комп'ютерам потребували б тисячі років, всього за кілька хвилин. Потенційні сфери застосування квантових комп'ютерів охоплюють фізичні, математичні та біологічні задачі, зокрема прогнозування процесу згортання білків. Сучасна криптографія з відкритим ключем, зокрема алгоритми RSA та ECC, базується на складності задач факторизації великих чисел або дискретного логарифмування для класичних обчислювальних ресурсів. Водночас квантові алгоритми, такі як алгоритм Шора, здатні ефективно розв'язувати ці задачі, що робить багато поширених криптографічних протоколів вразливими [3]. Додатково загрозу посилюють стратегії типу "збирай зараз, розшифровуй пізніше" (Harvest Now, Decrypt Later, HNDL), коли зашифровані дані перехоплюються для їх подальшого дешифрування після появи потужних квантових обчислювальних ресурсів. Це створює серйозні ризики для конфіденційності даних, які передаються зараз.

Метою цього дослідження є комплексний аналіз ризиків, які квантові обчислення створюють для традиційних криптографічних систем. Особлива увага приділяється вивченню реалізації алгоритму Шора для факторизації складених чисел за допомогою інструментів квантового програмування Qiskit.

Дослідження включає огляд принципів квантових обчислень і відмінностей їх функціонування від класичних систем, аналіз криптографічних вразливостей, що виникають у результаті розвитку квантових технологій, а також висвітлення зусиль, спрямованих на розробку та впровадження постквантових криптографічних алгоритмів, зокрема ініціатив Національного інституту стандартів і технологій (NIST) [4]. Окрему увагу приділено практичним аспектам реалізації квантових атак, зокрема симуляції алгоритму Шора, оцінці необхідних ресурсів для зламу RSA-2048 та аналізу актуальних обмежень сучасних квантових комп'ютерів.

Очікується, що результати дослідження продемонструють важливість своєчасного переходу на постквантову криптографію та нададуть рекомендації для компаній щодо зниження ризиків майбутніх квантових атак.

Теоретичні основи дослідження

Дослідження ризиків квантових атак на компанії базується на сучасних теоретичних засадах квантових обчислень, криптографії та постквантових технологій. Квантові комп'ютери мають потенціал експоненційного прискорення обчислень у порівнянні з класичними системами [5].

Одним із найважливіших квантових алгоритмів для криптоаналізу є алгоритм Шора, запропонований у 1994 році. Він дозволяє розкладати великі цілі числа на прості множники за поліноміальний час, що робить його здатним зламати криптографію з відкритим ключем, яка раніше вважалася надійною [6]. Теоретичні основи алгоритму Шора базуються на використанні квантового перетворення Фур'є та пошуку періоду функцій для факторизації чисел. Реалізація алгоритму потребує великої кількості логічних кубітів, високого часу когерентності та ефективної корекції квантових помилок.

Реалізація алгоритму Шора в реальних умовах залишається складною задачею через обмеження сучасних квантових комп'ютерів, які належать до класу пристроїв шумового квантового проміжного масштабу (NISQ) [7]. Основними труднощами є декогеренція кубітів, помилки зчитування та нестабільність квантових операцій. Для подолання цих проблем активно розробляються методи квантової корекції помилок, зокрема використання логічних кубітів на базі поверхневого коду, що дозволяє частково компенсувати шум та продовжити час збереження квантової інформації.

Для тестування і моделювання алгоритму Шора широко використовується бібліотека Qiskit — відкритий фреймворк для квантового програмування, розроблений IBM [8]. Qiskit

дозволяє створювати квантові схеми, моделювати квантові обчислення на класичних комп'ютерах та запускати їх на реальних квантових пристроях через хмарні сервіси IBM Quantum. Реалізація алгоритму Шора у Qiskit передбачає побудову квантового кола з реєстрами факторизації, квантове перетворення Фур'є та етап пошуку періоду, що забезпечує основу для розкладання чисел на прості множники.

На відміну від класичного перетворення Фур'є, яке масштабується поліноміально з розміром вхідних даних, QFT досягає експоненціального прискорення, маніпулюючи кубітами паралельно. Воно є центральним для квантових алгоритмів, таких як алгоритм Шора, що дозволяє ефективно ідентифікувати періодичності в модульній арифметиці.

У цій статті [9] було досліджено Квантове перетворення Фур'є як застосуванням цієї математичної конструкції: зміщення базисних станів для отримання бажаного результату. В обчислювальному базисі числа зберігаються за допомогою двійкових значень нуля та одиниці. Натомість у базисі Фур'є числові значення відображаються за допомогою накладених квантових станів.

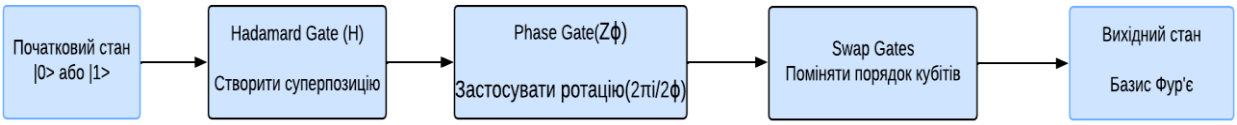


Рисунок 1 – Кроки у квантовому перетворенні Фур'є

У відповідь на потенційну загрозу з боку квантових обчислень активно розвивається постквантова криптографія (PQC). Національний інститут стандартів і технологій США (NIST) у 2022 році затвердив кілька алгоритмів для стандартизації, серед яких CRYSTALS-Kyber для шифрування та CRYSTALS-Dilithium, FALCON і SPHINCS+ для цифрових підписів [10]. Ці алгоритми базуються на задачах, які залишаються складними навіть для квантових комп'ютерів, таких як проблема решіток та хешування. Вибрані стандарти вирізняються високою ефективністю, зручністю реалізації та невеликими розмірами ключів і підписів у порівнянні з іншими підходами.

Таким чином, дослідження ризиків квантових атак охоплює як теоретичне обґрунтування можливостей квантових алгоритмів, так і аналіз практичних заходів, спрямованих на зміцнення інформаційної безпеки в постквантову епоху.

Постановка проблеми

Ключовою проблемою, що розглядається в цій статті, є потенційні ризики для асиметричних методів шифрування, які можуть бути скомпрометовані за допомогою квантових алгоритмів факторизації, що є значно ефективнішими порівняно з алгоритмами, що використовуються класичними комп'ютерами. Інформація, яка була перехоплена в зашифрованому вигляді, може бути розшифрована зі зростанням потужностей квантових комп'ютерів (стратегія HNDL). Тому необхідно забезпечити захист інформації, яка має довготривалий період зберігання, за допомогою постквантових методів шифрування якнайшвидше.

Однією з основних загроз, пов'язаних із квантовими обчисленнями, є втрата надійності традиційних криптографічних систем, таких як RSA, які сьогодні забезпечують більшість захисту даних у сучасних інформаційних системах. Потенціал квантових комп'ютерів для ефективного вирішення задач факторизації великих чисел та обчислення дискретних логарифмів може призвести до того, що ці криптографічні методи стануть вразливими вже через кілька років. Це створює необхідність для переходу на нові підходи до захисту даних, здатні протистояти квантовим атакам.

Пошук та впровадження постквантових алгоритмів шифрування, які здатні забезпечити високий рівень безпеки в умовах квантової ери, є нагальною задачею для сучасної криптографії та інформаційної безпеки. З огляду на швидкий розвиток квантових технологій, необхідно не лише вдосконалювати існуючі методи, але й передбачати нові підходи до захисту, які зможуть гарантувати конфіденційність і цілісність даних на довготривалий період.

Це дослідження має на меті оцінити ефективність атак за допомогою факторихації алгоритмом Шора, актуальність їх застосування в реальних умовах та розробку рекомендацій для їх інтеграції в сучасні інформаційні системи, щоб забезпечити надійний захист від майбутніх квантових загроз.

Методологія дослідження

Моделювання атаки на методи факторизації в алгоритмі AES за допомгою алгоритму Шора було виконано на мові програмвання Python за допомогою бібліотеки для квантового програмування Qiskit. Код було виконано в середовищі Jupyter Notebook та використано додаткові бібліотеки для візуалізації даних.

Для реалізації алгоритму Шора було використано Qiskit, що дозволяє моделювати квантові обчислення на класичних комп'ютерах через симулятори. Усі обчислення були здійснені за допомогою доступних квантових симуляторів в Qiskit, оскільки для реального використання квантових комп'ютерів з високою потужністю на даний момент є обмеження.

Результат експериментів був оцінений за критеріями точності факторизації та можливості застосування отриманих результатів для потенційної атаки на сучасні криптографічні методи, зокрема AES.

Отримані дані дозволили оцінити потенціал використання квантових алгоритмів для криптоаналізу, а також визначити проблеми та обмеження, з якими стикаються сучасні квантові обчислення при атаці на криптографічні системи, зокрема, в контексті факторизації.

Результати

Для демонстрації реалізації алгоритму Шора засобами Qiskit спершу розглянемо ключовий елемент, на якому він базується – періодичність модульної експоненційної функції $a^x \bmod N$. На прикладі $N = 35$ та $a = 13$ було згенеровано відповідну послідовність значень. Візуалізація цієї послідовності наочно демонструє її періодичний характер, де період r є критично важливим параметром для подальшого знаходження дільників N. Хоча графічне представлення є ілюстративним, обчислення періоду для великих N класичними методами є неефективним, що й обґрунтовує застосування квантових алгоритмів.

```
N = 35
a = 13

xvals = num.arange(40)
yvals = [num.mod(a**x, N) for x in xvals]

fig, ax = plot.subplots()
ax.plot(xvals, yvals, linewidth=1, linestyle='dotted', marker='x')
ax.set(xlabel='$x$', ylabel=f'${a}^x$ mod ${N}$',
       title="Приклад періодичної функції в алгоритмі Шора")

try:
   r = yvals[1:].index(1) + 1
   plot.annotate('', xy=(0,1), xytext=(r,1),
                 arrowprops=dict(arrowstyle='<->'))
   plot.annotate(f'$r={r}$', xy=(r/3,1.5))
except ValueError:
```

```
    print('Не вдалося знайти період, перевірте a < N та відсутність спільних
множників.')
```

Отриманий результат:

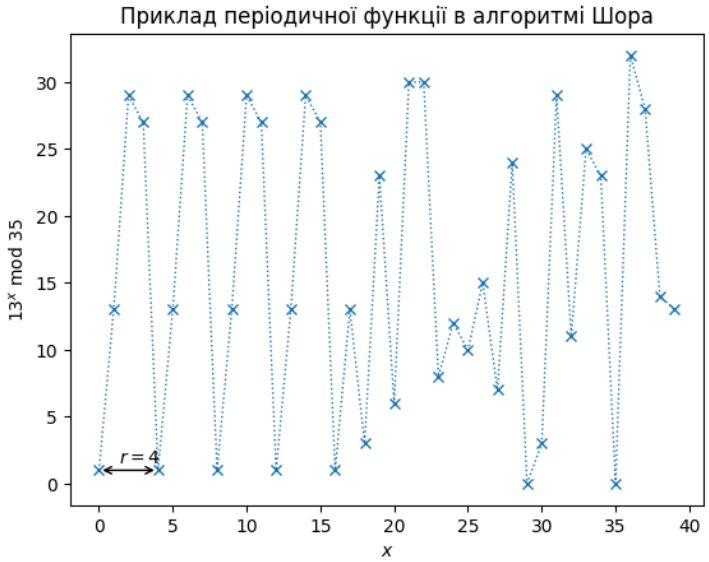


Рисунок 2 – Приклад періодичної функції

Переходячи до квантової реалізації, алгоритм Шора використовує можливості квантових обчислень для ефективного знаходження цього періоду r. Реалізація за допомогою Qiskit поєднує класичні та квантові обчислювальні компоненти. Класичні компоненти відіграють допоміжну, але критично важливу роль, виконуючи такі задачі, як перевірка взаємної простоти a та *N*, обчислення найбільших спільних дільників (НСД) та постобробка результатів квантових вимірювань для визначення кінцевих множників. Вони забезпечують математичну підтримку та інтерпретацію результатів, отриманих від квантової частини.

Центральним елементом є квантова схема, спроєктована для виконання квантової оцінки фази (Quantum Phase Estimation, QPE), яка по суті є методом знаходження періоду r. Схема ініціалізується застосуванням гейтів Адамара до лічильних кубітів, що створює рівномірну суперпозицію всіх можливих станів. Наступним кроком є застосування керованих операцій модульної експоненції (a^(2^j) mod *N*). Ці операції кодують інформацію про період функції a^x mod N у фазу квантових станів. Завершальним квантовим етапом є застосування оберненого квантового перетворення Фур'є (Inverse Quantum Fourier Transform, IQFT), яке перетворює фазову інформацію в амплітуди ймовірностей, що дозволяє виміряти значення, пов'язані з періодом r.

Наступний програмний код демонструє реалізацію алгоритму Шора засобами Qiskit, інкапсулюючи описані вище класичні та квантові кроки для факторизації числа *N*=35.

```
from qiskit import transpile
from qiskit_aer import AerSimulator
from qiskit.circuit.library import QFT
from qiskit.circuit import QuantumCircuit
from qiskit.visualization import plot_histogram
from fractions import Fraction
from math import gcd
import numpy as np
import random
```

```
# Визначаємо модульну експоненцію як класичну допоміжну функцію
def mod_exp(base, exponent, modulus):
    """Виконує модульну експоненцію: (base^exponent) % modulus."""
    return pow(base, exponent, modulus)

# Функція для реалізації квантової схеми Шора
def shor_quantum_circuit(a, N, n_count):
    """Створює квантову схему для алгоритму Шора."""
    qc = QuantumCircuit(n_count + 4, n_count)  # n_count для лічильних
кубітів, 4 для робочої області

    # Застосовуємо оператор Адамара до лічильних кубітів
    for q in range(n_count):
        qc.h(q)

    # Керована модульна експоненція
    for q in range(n_count):
        qc.append(modular_exponentiation(a, N, 2**q).to_gate().control(),
[q] + list(range(n_count, n_count + 4)))

    # Застосовуємо обернене QFT до лічильних кубітів
    qc.append(QFT(n_count, inverse=True).to_gate(), range(n_count))

    # Вимірюємо лічильні кубіти
    qc.measure(range(n_count), range(n_count))
    return qc

# Функція для симуляції модульної експоненції (потрібна для керованих
гейтів)
def modular_exponentiation(a, N, power):
    """Симулює схему модульної експоненції для основи a, модуля N і
степеня."""
    qc = QuantumCircuit(4)
    for _ in range(power):
        qc.swap(0, 1)
        qc.swap(1, 2)
        qc.swap(2, 3)
        qc.x(0)
    return qc

# Виконання алгоритму Шора для факторизації числа 35
def shors_algorithm(N):
    """Реалізація алгоритму Шора для знаходження дільника числа N."""
    # Вибираємо випадкове 'a', таке що gcd(a, N) == 1
    while True:
        a = random.randint(2, N - 1)
        if gcd(a, N) == 1:
            break

    print(f"Вибрано a: {a}")
```

```
    # Кількість кубітів для квантового перетворення Фур'є
    n_count = 8  # Довільна точність для оцінки фази

    # Створюємо та виконуємо квантову схему
    qc = shor_quantum_circuit(a, N, n_count)
    sim = AerSimulator()
    t_qc = transpile(qc, sim)
    result = sim.run(t_qc).result()
    counts = result.get_counts()

    # Побудова гістограми
    plot_histogram(counts)

    # Інтерпретація результатів
    measured_phases = []
    for output in counts:
        decimal = int(output, 2) / (2**n_count)
        measured_phases.append(decimal)

    print(f"Виміряні фази: {measured_phases}")

    # Знаходимо період r, використовуючи виміряні фази
    for phase in measured_phases:
        frac = Fraction(phase).limit_denominator(N)
        r = frac.denominator
        if r % 2 == 0 and mod_exp(a, r // 2, N) != 1:
            factor1 = gcd(mod_exp(a, r // 2, N) - 1, N)
            factor2 = gcd(mod_exp(a, r // 2, N) + 1, N)
            if factor1 * factor2 == N:
                print(f"Знайдені дільники: {factor1}, {factor2}")
                return factor1, factor2
    return None

# Факторизація числа 35
factors = shors_algorithm(35)
print(f"Дільники числа 35: {factors}")
```

Вимірювання стану лічильних кубітів після IQFT дає набір бінарних рядків. Кожен рядок представляє ціле число m, яке з високою ймовірністю наближає значення s * (2^k / r) для деякого цілого *s*, де *k* – кількість лічильних кубітів, а *r* – шуканий період. Результати вимірювань, отримані під час симуляції (або з реального квантового пристрою), візуалізуються за допомогою гістограми (приклад на рис. 3.4), яка показує розподіл ймовірностей отримання різних значень *m*.

Класична постобробка полягає в аналізі цих виміряних значень m. Використовуючи алгоритм неперервних дробів, з відношення m / 2^k можна ефективно визначити знаменник r, який є кандидатом на період. Якщо знайдений період r виявляється парним і задовольняє умову a^(r/2) != -1 (mod *N*), то обчислення найбільших спільних дільників НСД(a^(r/2) - 1, *N*) та НСД(a^(r/2) + 1, *N*) з великою ймовірністю дадуть нетривіальні множники числа *N*.

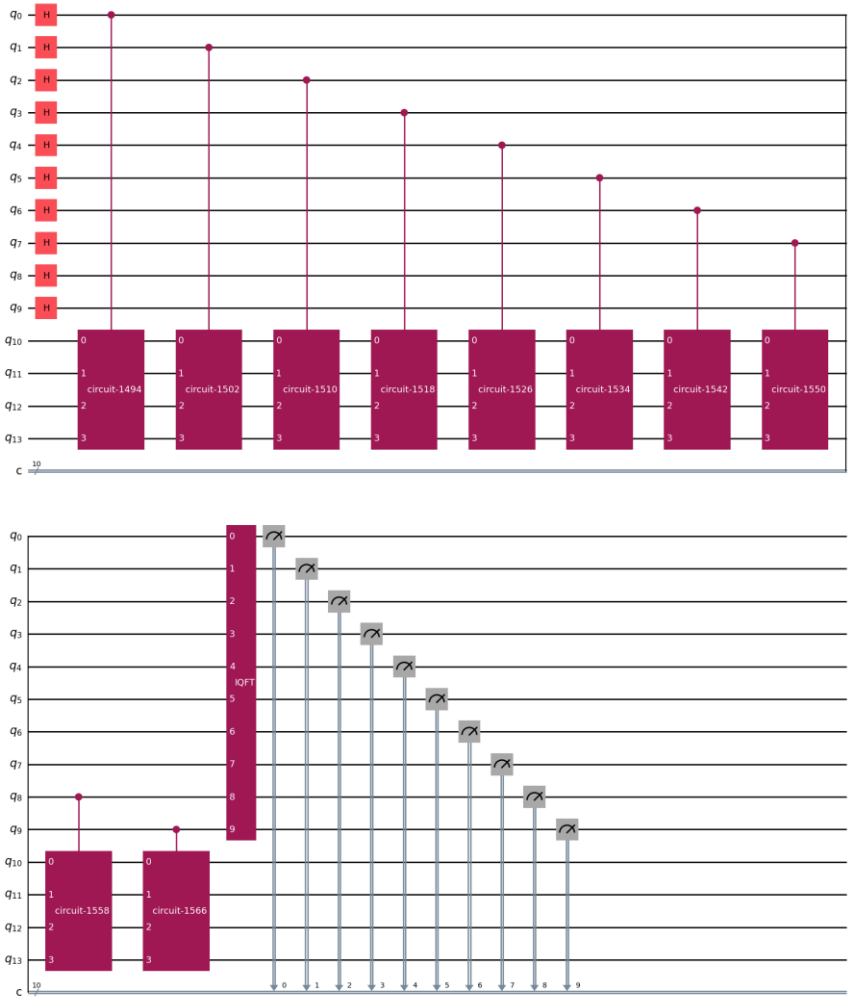


Рисунок 3 – Квантова схема реалізованого алгоритму Шора (Примітка: конкретний вигляд залежить від реалізації)

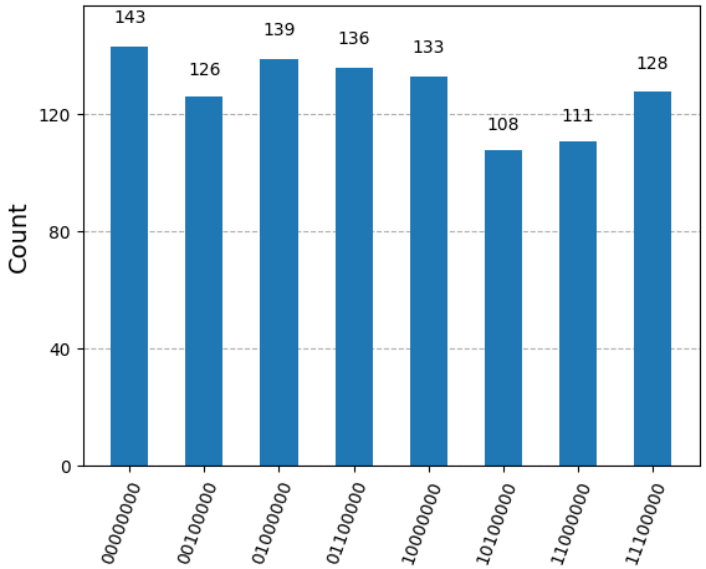


Рисунок 4 – Результуюча гістограма (Примітка: гістограма для ідеальних симульованих результатів)

У конкретному випадку факторизації *N*=35, після вибору a (наприклад, *a*=13, як у першому прикладі, або інше випадкове a, як у коді), алгоритм переходить до квантової оцінки фази. Гістограма результатів (як на Рис. 3.4) демонструє піки, що відповідають значенням m. Аналіз цих значень дозволяє визначити період r. Для N=35 та a=13, період r=4. Оскільки r парне, обчислюємо a^(r/2) mod *N* = 13^2 mod 35 = 169 mod 35 = 29. Це значення не дорівнює -1 mod 35 (тобто 34). Тоді множники знаходяться як НСД(29 - 1, 35) = НСД(28, 35) = 7 та НСД(29 + 1, 35) = НСД(30, 35) = 5. Таким чином, успішне виконання алгоритму призводить до знаходження дільників 5 і 7. Вивід коду (з використанням симульованих результатів для *a*=27, де *r*=6) також демонструє знаходження цих дільників:

```
Вибрано a: 27
Виміряні фази: [0.75, 0.125, 0.5, 0.375, 0.25, 0.625, 0.0, 0.875]
Знайдені дільники: 7, 5
Дільники числа 35: (7, 5)
```

Висновки

У результаті проведеного дослідження було проаналізовано вплив квантових обчислень на сучасні криптографічні системи, зокрема їхню здатність порушувати безпеку традиційних алгоритмів шифрування. Аналізом встановлено, що квантові обчислення, особливо алгоритм Шора, становлять суттєву загрозу для поширених асиметричних криптографічних методів, таких як RSA, DSA та ECDSA.

Було визначено, що атаки типу “Harvest Now, Decrypt Later” (HNDL) набувають дедалі більшої актуальності у зв’язку з потенційною можливістю збереження зашифрованих даних сьогодні для їх подальшого розшифрування за допомогою потужних квантових комп’ютерів у майбутньому. У цьому контексті підкреслено важливість діяльності стандартизаційних організацій, як-от NIST, у розробці та затвердженні постквантових алгоритмів, а також відзначено активізацію приватного бізнесу у напрямку впровадження постквантових рішень.

Практична складова дослідження полягала у реалізації алгоритму Шора з використанням інструментарію квантового програмування (Qiskit). Отримані результати, навіть при використанні симулятора, демонструють здатність сучасних квантових алгоритмів до факторизації чисел, що емпірично підтверджує їхній криптоаналітичний потенціал. Водночас наголошено, що практичне застосування цих алгоритмів для зламу сучасних криптосистем потребує обчислювальних потужностей, які наразі недоступні для існуючих квантових комп’ютерів.

На основі вищезазначеного зроблено висновок про нагальну необхідність переходу до постквантових криптографічних методів для забезпечення довгострокової стійкості до квантових загроз, що вимагає адаптації відповідної галузі до нових технологічних реалій. Перспективними напрямами подальших досліджень у цій сфері визначено розробку та аналіз нових версій постквантових криптографічних алгоритмів, зокрема на основі задач теорії ґраток, а також дослідження шляхів підвищення їх ефективності, зменшення розміру ключів та розробку методик їх інтеграції в оновлені версії поширених протоколів передачі даних.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Chuang, I.L., Gershenfeld, N., Kubinec, M. (1998). Experimental Implementation of Fast Quantum Searching. Physical Review Letters, 80(15), pp. 3408–3411. https://doi.org/10.1103/PhysRevLett.80.3408.
2. Whyte, S. (2024). QUANTUM CRYPTOGRAPHY AND ITS IMPLICATIONS IN CYBERSECURITY: SECURING COMMUNICATION IN THE QUANTUM ERA. International Journal of Computer Science and Information Technology.
3. Sharma, M. та ін. (2021). Leveraging the power of quantum computing for breaking RSA encryption. Cyber-Physical Systems, 7, pp. 73–92.
4. Boutin, C. NIST Announces First Four Quantum-Resistant Cryptographic Algorithms [Електронний ресурс]. Available from: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms. Accessed: April 27, 2025.
5. Beauregard, S. (2002). Circuit for Shor's Algorithm Using 2n+3 Qubits.
6. Shor, P.W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5), pp. 1484–1509. https://doi.org/10.1137/S0097539795293172.
7. DiVincenzo, D.P., Shor, P.W. (1996). Fault-Tolerant Error Correction with Efficient Quantum Codes. *Physical Review Letters*, 77(15), pp. 3260–3263. https://doi.org/10.1103/PhysRevLett.77.3260.
8. García-Martín, D., Sierra, G. (2018). Five Experimental Tests on the 5-Qubit IBM Quantum Computer. Journal of Applied Mathematics and Physics, 6, pp. 1460–1475.
9. Fouque, P.-A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z. (2020). Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. Specification v1.2. [Електронний ресурс]. Available from: https://falcon-sign.info/falcon.pdf. Accessed: April 27, 2025.
10. Boutin, C. NIST Releases First 3 Finalized Post-Quantum Encryption Standards [Електронний ресурс]. Available from: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards. Accessed: April 27, 2025.
11. Schaumann, J. (2024). Post-Quantum Cryptography in January 2024 [Електронний ресурс]. Available from: https://www.netmeister.org/blog/pqc-2024-01.html. Accessed: November 27, 2024.
12. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D. (2017). CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme. IACR Cryptology ePrint Archive, 2017/633. [Електронний ресурс]. Available from: https://eprint.iacr.org/2017/633.pdf. Accessed: April 27, 2025.
13. Derevianko, Ya.A., Gorbenko, I.D. (2022). FALCON signature vulnerability to special attacks and its protection. Radiotekhnika, 210, pp. 37–52. https://doi.org/10.30837/rt.2022.3.210.03.
14. Pathum, U. (2024). CRYSTALS Kyber: The Key to Post-Quantum Encryption [Електронний ресурс]. Available from: https://medium.com/@hwupathum/crystals-kyber-the-key-to-post-quantum-encryption-3154b305e7bd. Accessed: November 26, 2024.
15. Bernstein, D.J., Hülsing, A., Cybercrypt, S.K., Niederhagen, R., Rijneveld, J., Schwabe, P. (2019). The SPHINCS+ Signature Framework.
16. Deig, J. (2024). New Standards to Head Off Quantum Cyberthreats. Cisco Newsroom. [Електронний ресурс]. Available from: https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m07/new-standards-to-head-off-quantum-cyberthreats.html. Accessed: April 27, 2025.
17. Kasirajan, V. (2021). Fundamentals of Quantum Computing. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-63689-0.
18. Gidney, C., Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum, 5, p. 433. https://doi.org/10.22331/q-2021-04-15-433.

References

1. Chuang, I.L., Gershenfeld, N., Kubinec, M. (1998). Experimental Implementation of Fast Quantum Searching. Physical Review Letters, 80(15), pp. 3408–3411. https://doi.org/10.1103/PhysRevLett.80.3408.
2. Whyte, S. (2024). QUANTUM CRYPTOGRAPHY AND ITS IMPLICATIONS IN CYBERSECURITY: SECURING COMMUNICATION IN THE QUANTUM ERA. International Journal of Computer Science and Information Technology.
3. Sharma, M. та ін. (2021). Leveraging the power of quantum computing for breaking RSA encryption. Cyber-Physical Systems, 7, pp. 73–92.
4. Boutin, C. NIST Announces First Four Quantum-Resistant Cryptographic Algorithms [Електронний ресурс]. Available from: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms. Accessed: April 27, 2025.
5. Beauregard, S. (2002). Circuit for Shor's Algorithm Using 2n+3 Qubits.
6. Shor, P.W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5), pp. 1484–1509. https://doi.org/10.1137/S0097539795293172.
7. DiVincenzo, D.P., Shor, P.W. (1996). Fault-Tolerant Error Correction with Efficient Quantum Codes. *Physical Review Letters*, 77(15), pp. 3260–3263. https://doi.org/10.1103/PhysRevLett.77.3260.
8. García-Martín, D., Sierra, G. (2018). Five Experimental Tests on the 5-Qubit IBM Quantum Computer. Journal of Applied Mathematics and Physics, 6, pp. 1460–1475.
9. Fouque, P.-A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z. (2020). Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. Specification v1.2. [Електронний ресурс]. Available from: https://falcon-sign.info/falcon.pdf. Accessed: April 27, 2025.
10. Boutin, C. NIST Releases First 3 Finalized Post-Quantum Encryption Standards [Електронний ресурс]. Available from: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards. Accessed: April 27, 2025.
11. Schaumann, J. (2024). Post-Quantum Cryptography in January 2024 [Електронний ресурс]. Available from: https://www.netmeister.org/blog/pqc-2024-01.html. Accessed: November 27, 2024.
12. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D. (2017). CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme. IACR Cryptology ePrint Archive, 2017/633. [Електронний ресурс]. Available from: https://eprint.iacr.org/2017/633.pdf. Accessed: April 27, 2025.
13. Derevianko, Ya.A., Gorbenko, I.D. (2022). FALCON signature vulnerability to special attacks and its protection. Radiotekhnika, 210, pp. 37–52. https://doi.org/10.30837/rt.2022.3.210.03.
14. Pathum, U. (2024). CRYSTALS Kyber: The Key to Post-Quantum Encryption [Електронний ресурс]. Available from: https://medium.com/@hwupathum/crystals-kyber-the-key-to-post-quantum-encryption-3154b305e7bd. Accessed: November 26, 2024.
15. Bernstein, D.J., Hülsing, A., Cybercrypt, S.K., Niederhagen, R., Rijneveld, J., Schwabe, P. (2019). The SPHINCS+ Signature Framework.
16. Deig, J. (2024). New Standards to Head Off Quantum Cyberthreats. Cisco Newsroom. [Електронний ресурс]. Available from: https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m07/new-standards-to-head-off-quantum-cyberthreats.html. Accessed: April 27, 2025.
17. Kasirajan, V. (2021). Fundamentals of Quantum Computing. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-63689-0.
18. Gidney, C., Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum, 5, p. 433. https://doi.org/10.22331/q-2021-04-15-433.

Дослідження впливу генеративного штучного інтелекту на аналіз результатів статичного сканування коду за допомогою статичного аналізатора Bearer CLI

Study of the Influence of Generative Artificial Intelligence on the Analysis of Static Code Scanning Results Using the Bearer CLI Static Analyzer

Роман Жишко [A]
студент кафедри Захист інформації, e-mail: roman.zhyshko.kb.2021@lpnu.ua, ORCID: 0009-0001-9188-3931

Ігор Кос [A]
студент кафедри Захист інформації, e-mail: ihor.kos.kb.2021@lpnu.ua, ORCID: 0009-0001-4558-5036

Єлизавета Черемних [A]
студент кафедри Захист інформації, e-mail: yelyzaveta.cheremnykh.kb.2021@lpnu.ua, ORCID: 0009-0005-8901-7101

Даниїл Журавчак [A]
доктор філософії, асистент кафедри Захисту інформації, e-mail: danyil.y.zhuravchak@lpnu.ua, ORCID: 0000-0003-4989-0203

Віталій Сусукайло [A]
Corresponding author: доктор філософії, асистент кафедри Захисту інформації, e-mail: vitalii.a.susukailo@lpnu.ua, ORCID: 0000-0003-4431-9964

Roman Zhyshko [A]
Student of the Department Information Protection, e-mail: roman.zhyshko.kb.2021@lpnu.ua, ORCID: 0009-0001-9188-3931

Ihor Kos [A]
Student of the Department Information Protection, e-mail: ihor.kos.kb.2021@lpnu.ua, ORCID: 0009-0001-4558-5036

Yelyzaveta Cheremnykh [A]
Student of the Department Information Protection, e-mail: yelyzaveta.cheremnykh.kb.2021@lpnu.ua, ORCID: 0009-0005-8901-7101

Danyil Zhuravchak [A]
Doctor of Philosophy, Assistant, e-mail: danyil.y.zhuravchak@lpnu.ua, ORCID: 0000-0003-4989-0203

Vitalii Susukailo [A]
Corresponding author: Doctor of Philosophy, Assistant, e-mail: vitalii.a.susukailo@lpnu.ua, ORCID: 0000-0003-4431-9964

[A] Національний університет "Львівська політехніка", Львів, Україна

[A] Lviv Polytechnic National University, Lviv, Ukraine

Received: April 8, 2025 | Revised: April 28, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.17

Мета роботи: дослідити можливості генеративного штучного інтелекту для покращення інтерпретації результатів статичного сканування коду за допомогою інструмента Bearer CLI.

Метод дослідження: кількісні та експериментальні методи, зокрема застосування великих мовних моделей для обробки результатів SAST-аналізу, а також експертного оцінювання авторами їхньої точності, корисності, узгодженості та обґрунтованості оцінки наслідків ризиків за допомогою статистичного аналізу на основі 5-бальної шкали.

Результати дослідження: проведено оцінку п'яти популярних великих мовних моделей (GPT-4o, GPT-4.5, GPT-o3-mini-high, Gemini 2.5 Pro, Claude 3.7 Sonnet) щодо їхньої здатності покращувати аналіз результатів статичного сканування Bearer CLI для трьох типів вразливостей. Порівняльний аналіз за критеріями точності, корисності, узгодженості та оцінки бізнес-впливу показав, що інтеграція генеративного ШІ суттєво покращує інтерпретацію стандартного виводу інструмента. Найвищу ефективність за сукупністю критеріїв продемонструвала модель Gemini 2.5 Pro, що підтверджує значний потенціал ШІ для якісного та доступного аналізу SAST-звітів.

Теоретична цінність дослідження: дослідження поглиблює розуміння можливостей генеративного ШІ для ефективнішого аналізу результатів SAST-аналізаторів, демонструючи їх потенціал у наданні точніших пояснень та виправлень вразливостей, що є теоретичною основою для майбутніх досліджень в автоматизації безпеки коду.

Практична цінність дослідження: отримані результати можуть стати базою для поліпшення інструментів статичного аналізу, таких як Bearer CLI. Це допоможе розробникам швидше

Purpose: to investigate how generative artificial intelligence can improve static code analysis results interpretation using the Bearer CLI tool.

Method: quantitative and experimental methods, including using large language models for processing the results of SAST analysis, and expert evaluation by the authors of their accuracy, usefulness, consistency, and validity of assessing the consequences of risks using statistical analysis based on a 5-point scale.

Findings: five popular large language models (GPT-4o, GPT-4.5, GPT-o3-mini-high, Gemini 2.5 Pro, Claude 3.7 Sonnet) were evaluated for their ability to enhance the analysis of Bearer CLI static scanning results for three types of vulnerabilities. Comparative analysis based on criteria of accuracy, usefulness, consistency, and business impact assessment showed that integrating generative AI significantly improves the interpretation of the tool's standard output. The Gemini 2.5 Pro model demonstrated the best overall performance, confirming the significant potential of AI for improving the quality and accessibility of SAST report analysis.

Theoretical implications: The study deepens understanding of the capabilities of generative AI to more effectively analyze the results of SAST analyzers, demonstrating their potential in providing more accurate explanations and fixes for vulnerabilities, which is a theoretical basis for future research in code security automation.

Practical implications: the obtained results can serve as a basis for improving static analysis tools such as Bearer CLI. This will

орієнтуватися в результатах сканування і оперативно реагувати на потенційні загрози.

Цінність дослідження: дослідження демонструє, як застосування ШІ для аналізу результатів статичного сканування дозволяє знизити кількість хибнопозитивних спрацювань, зробити звіти більш зрозумілими та ефективно виявляти реальні вразливості, що сприяє підвищенню безпеки коду на ранніх етапах розробки.

Тип статті: емпіричне дослідження.

Ключові слова: штучний інтелект, статичний аналіз, мовна модель, безпека коду, вразливість.

help developers navigate scan results more efficiently and quickly respond to potential threats.

Value: The study demonstrates how using AI to analyze the results of static scanning can reduce the number of false positives, make reports more understandable and effectively identify real vulnerabilities, which contributes to improving code security in the early stages of development.

Paper type: empirical study.

Key words: artificial intelligence, static analysis, language model, code security, vulnerability.

Вступ

В умовах стрімкого розвитку технологій питання безпечної розробки програмного забезпечення є актуальним та критично важливим. Виявлення слабких місць коду за допомогою статичного аналізатора коду (SAST) дає змогу мінімізувати ризики ще на етапі розробки, дозволяючи виправляти вразливості, допоки витрати на усунення залишаються мінімальними, та навчати розробників створювати безпечний код [1]. При цьому інструменти SAST часто генерують хибні спрацювання, а звіти про аналіз є складними для розуміння, тому їх використання вимагає від розробників додаткових знань у сфері кібербезпеки. Навчання та здобуття кваліфікації співробітниками у цій галузі може бути часо- та фінансовоємним. Враховуючи зростаючу складність програмних систем та кількість кіберзагроз, пошук ефективних методів аналізу результатів SAST є вкрай важливим.

Для вирішення наведеної вище проблеми пропонується використання генеративного штучного інтелекту (ШІ). Великі мовні моделі (LLM) вже були неодноразово успішно протестовані на можливість виявлення вразливостей коду. Великі обсяги даних, на яких навчаються такі моделі, містять історичну інформацію про вразливості програм, що дає змогу знаходити аналогічні проблеми в нових зразках коду [2]. Генеративний ШІ може спростити аналіз результатів, пояснювати знайдені вразливості та надавати рекомендації щодо їх усунення, використовуючи термінологію, зрозумілу розробникам. Метою цього дослідження є оцінка впливу генеративного штучного інтелекту на процес аналізу результатів статичного сканування коду за допомогою Bearer CLI.

Одним із прикладів SAST-аналізатора є Bearer CLI – інструмент для статичного аналізу коду з відкритим вихідним кодом [3], який підтримує мови програмування Go, Java, JavaScript, PHP, Python та Ruby. Сканер використовує вбудований список правил для пошуку вразливостей та безпекових ризиків, базуючись на OWASP Top 10 та MITRE CWE Top 25, що містять систематизовану інформацію про найпоширеніші помилки безпеки програмного забезпечення. Очікується, що результати дослідження покажуть, як генеративний ШІ може підвищити ефективність аналізу результатів роботи Bearer CLI, зменшити кількість хибних спрацювань і покращити розуміння розробниками знайдених вразливостей.

Теоретичні основи дослідження

Дослідження впливу генеративного штучного інтелекту на аналіз результатів статичного сканування коду ґрунтується на сучасних теоретичних засадах статичного аналізу програмного забезпечення [4], засобах обробки природної мови та великих мовних моделей для генерації тексту. Статичне тестування безпеки додатків (англ. SAST) дозволяє виявляти потенційні вразливості та недоліки у коді програми без виконання самого коду [5, 6]. Результати сканування інструментів статичного тестування завжди містять технічну безпекову інформацію, яка є складною у розумінні для більшості розробників. У завданні інтерпретації результатів тестування можуть допомогти мовні моделі генеративного штучного інтелекту. Великі мовні моделі (LLM) – це дуже великі моделі глибокого навчання , які попередньо навчаються на величезних обсягах даних [7]. Найбільшими та найпотужнішими LLM є ті, які

працюють на основі трансформенної архітектури. Трансформенна архітектура – це нейронна мережа, яка вивчає контекст послідовних даних і генерує з нього нові дані. Простіше кажучи, трансформер – це тип моделі штучного інтелекту, який вчиться розуміти природну мову та генерувати її у людському стилі, аналізуючи шаблони у великих обсягах текстових даних [8]. Мовні моделі описують загальним терміном “штучний інтелект (ШІ)”. Завдяки навчанню на великих обсягах текстових даних моделі можуть перетворювати складні технічні виводи у доступні рекомендації щодо виправлення виявлених вразливостей. Найпотужнішими та найсучаснішими представниками генеративних моделей штучного інтелекту є моделі міркування (reasoning models) – моделі, навчені за допомогою навчання з підкріпленням для виконання складних міркувань [9]. Моделі міркування думають, перш ніж відповісти, створюючи довгий внутрішній ланцюжок думок, перш ніж відповісти користувачеві. Моделі міркування чудово підходять для вирішення складних проблем, кодування, наукового міркування та багатоетапного планування для агентських робочих процесів [10].

Bearer CLI — це статичний аналізатор коду (SAST) з відкритим кодом, який можна використовувати для сканування вихідного коду на наявність потенційних уразливостей. Аналіз відбувається за допомогою вбудованих правил безпеки та конфіденційності. Ці правила охоплюють типові вразливості, описані в OWASP Top 10 та CWE Top 25. Після завершення сканування генерується звіт з переліком знайдених вразливостей, їх детальним описом та рекомендаціями щодо виправлення. Також включається посилання на файли та рядки коду, де виявлені проблеми. Bearer CLI дозволяє сортувати виявлені проблеми за критичністю та типом, що спрощує їх подальшу обробку та виправлення [3].

Bearer CLI може виводити результати у різних форматах. Стандартний вивід передбачає виведення інформації безпосередньо в термінал із зазначенням виявлених проблем, їх описом та рекомендаціями. Збереження також можливе у JSON-формат, який дозволяє автоматизувати обробку результатів.

Інтеграція генеративного штучного інтелекту сприяє зниженню обсягів рутинної роботи та підвищує ефективність праці [11]. Таким чином, використання генеративного ШІ для вербального представлення результатів SAST відкриває нові можливості для покращення доступності технічної інформації та оптимізації процесів забезпечення безпеки програмного забезпечення.

Постановка проблеми

Основною проблемою, розглянутою в цій статті, є складність аналізу результатів статичного сканування коду через велику кількість специфічної технічної інформації та хибних спрацювань [12]. Це ускладнює виявлення реальних вразливостей, їх розуміння та, відповідно, методів їх усунення, а також вимагає від розробників додаткових знань у сфері кібербезпеки.

Інструменти SAST, як і Bearer CLI, часто створюють звіти, які важко інтерпретувати без глибокого досвіду у безпеці кіберпростору. У результаті розробники можуть ігнорувати деякі результати або витрачати значні ресурси на те, щоб розібратися, що конкретно їм потрібно виправити для усунення недоліку. Одним із найбільш перспективних рішень цієї проблеми є використання генеративного штучного інтелекту для автоматизації пояснення виявлених вразливостей та зменшення кількості помилок [13].

Незважаючи на потенціал генеративного ШІ у галузі статичного тестування безпеки додатків, його ефективність у цьому контексті ще недостатньо вивчена. Важливо дослідити та оцінити, як мовні моделі можуть покращити процес обробки результатів сканування SAST, щоб підвищити точність виявлення загроз, швидкість їх виправлення та зменшити навантаження на розробників програмного забезпечення, на що і націлене дане дослідження.

Методологія дослідження

Для оцінки впливу генеративного штучного інтелекту на результати роботи статичного аналізатора Bearer CLI було протестовано п’ять LLM моделей: GPT-4o, GPT-4.5, GPT o3-mini-high, Gemini 2.5 Pro, 3.7 Sonnet. Кожна з них обробляла однаковий набір вразливостей, представлених у стандартизованому форматі.

Щоб мінімізувати вплив можливих помилок токенізатора – засобу перетворення текстової інформації у вектори, зрозумілий формат для мовних моделей, – вхідні дані були перекладені англійською мовою. Використовувався наступний шаблон запиту (Рис. 1), що містить ключову інформацію про вразливість, включаючи її ідентифікатор, критичність, контекст у коді, а також запити на пояснення, оцінку можливих хибнопозитивних спрацьовувань, пропозицію виправлення та аналіз бізнес-наслідків.

```
Проаналізуй знахідку SAST.
Вхідні дані:
SAST Правило: [ID правила або Title]
CWE: [CWE ID, наприклад, 798]
Серйозність: [Рівень серйозності, наприклад, critical]
Файл: [Повний шлях до файлу]
Номер рядка: [Номер рядка]
Рядок: [Код в конкретному рядку]
Фрагмент коду:
[Вставте сюди ~3 рядки коду навколо вказаного рядка]
Завдання:
1. Поясни простими словами, що означає CWE [Вставте CWE ID].
2. Аналіз коду:
   а. Оціни ймовірність False Positive. Що потрібно перевірити
      в коді чи логіці застосунку, щоб це підтвердити або спростувати?
   б. Поясни, чому саме цей фрагмент коду є проблемою в даному контексті.
   в. Надай виправлений фрагмент коду конкретно для цього місця.
3. Бізнес-вплив: Оціни потенційні бізнес-наслідки (наприклад, витік даних,
      фінансові чи репутаційні втрати), якщо цю вразливість проексплуатують,
      враховуючи серйозність та контекст.
```

Рисунок 1 – Шаблон запиту для генеративного ШІ

Для тестування було обрано три унікальні вразливості різних категорій, виявлені в проєкті OWASP Juice Shop при статичному тестуванні. Вивід, покращений мовними моделями, було порівняно між собою, а також з оригінальною версією результатів інструмента SAST. Оцінювання здійснювалося вручну авторами даного матеріалу за критеріями **точності пояснень** (правильність та повнота), **корисності виправлень** (ефективність та безпечність), **узгодженості відповідей** (відповідність структурі запиту) та **релевантності оцінки бізнес-впливу** (обґрунтованість наслідків). Для оцінки виводу кожної з моделей використовувалась 5-бальна шкала, де 1 – повна невідповідність критерію або незадовільна якість, а 5 – відмінна відповідь, що повністю задовольняє критерій.

Отримані результати дозволили визначити, яка з протестованих LLM показала найкращі результати за визначеними критеріями та оцінити потенціал використання генеративного ШІ для покращення аналізу результатів статичного аналізу коду.

Результати

Для порівняння аналізу моделями результатів сканування було обрано три вразливості різних рівнів.

Розглянемо оригінальний вивід SAST-аналізатора Bearer CLI для **першої вразливості javascript_express_hardcoded_secret**, форматований у JSON. Він містить певну корисну інформацію, однак пояснення неповні – не розкрито всі суттєві аспекти ризику. Рекомендації

з виправлення містять правильні поради (наприклад, застосовувати змінні середовища), але вони подані поверхнево та немає конкретного коду безпечної реалізації. Щодо узгодженості відповідей – структура повністю розбалансована, а аналіз бізнес-наслідків абсолютно відсутній. Таким чином, оригінальний вивід недостатньо інформативний і не відповідає вимогам якісного аналізу вразливостей. Оскільки для наступних вразливостей застосовано такий ж принцип опису, їх ми окремо розглядати не будемо.


```
{"critical":[{"cwe_ids":["798"],"id":"javascript_express_hardcoded_secret",
"title":"Usage of hard-coded secret","description":"## Description\n\nStoring
secrets directly in code compromises security. It's safer to use environment
variables or a secret management system.\n\n## Remediations\n\n- Do not store
plaintext secrets in your code. This makes your application vulnerable to
unauthorized access if the codebase is exposed.\n  ```javascript\n  app.use(
\n    session({\n      secret: \"shh-my-secret\",\n      name: \
"my-custom-session-name\",\n    })\n  )\n  ```\n- Do use environment variables
to store secrets. This method keeps sensitive information out of your codebase.
\n  ```javascript\n  app.use(\n    session({\n      secret: process.env.SECRET,
\n      name: \"my-custom-session-name\",\n    })\n  )\n  ```\n- Do use a
secret management system or a key management service (KMS) with encryption for
enhanced security. These services provide secure storage and management of
secrets, reducing the risk of exposure.\n\n## References\n\n- [OWASP hardcoded
passwords](https://owasp.org/www-community/vulnerabilities/Use_of_hard-coded_password)
\n- [Google Cloud Key Management Service](https://cloud.google.com/kms/docs)
\n- [AWS Key Management Service](https://aws.amazon.com/kms/)\n","documentation_url":
"https://docs.bearer.com/reference/rules/javascript_express_hardcoded_secret",
"line_number":56,"full_filename":"juice-shop/lib/insecurity.ts",
"filename":"lib/insecurity.ts","category_groups":["PII","Personal Data"],
"source":{"start":56,"end":56,"column":{"start":41,"end":108}},"sink":{
"start":56,"end":56,"column":{"start":41,"end":108},"content":""},
"parent_line_number":56,"fingerprint":"c095a5cc1948bae67c38b5c5d85eb4f4_0",
"old_fingerprint":"6841f0355c0a7e03b3d87c5c53f54493_0","code_extract":"export
const authorize = (user = {}) =\u003e jwt.sign(user, privateKey, { expiresIn:
'6h', algorithm: 'RS256' })"},...]}
```


Рисунок 2 – Оригінальний вивід аналізатора Bearer CLI у форматі JSON

Для аналізу вразливості було сформульовано запит, який відповідає наступним критеріям: точність пояснень, корисність виправлень, узгодженість відповідей та релевантність оцінки бізнес-впливу.

```
Analyze the SAST output.
Input:
1. SAST Rule: javascript_express_hardcoded_secret
2. CWE: 798
3. Severity: critical
4. File: juice-shop/lib/insecurity.ts
5. Line number: 56
6. Line: export const authorize = (user = {}) => jwt.sign(
   user, privateKey, { expiresIn: '6h', algorithm: 'RS256' })
7. Code Snippet: export const isAuthorized = () => expressJwt(
     ({ secret: publicKey }) as any)
   export const denyAll = () => expressJwt(
     { secret: '' + Math.random() } as any)
   export const authorize = (user = {}) => jwt.sign(user, privateKey,
     { expiresIn: '6h', algorithm: 'RS256' })
   export const verify = (token: string) => token ? (jws.verify as (
     (token: string, secret: string) => boolean))(token, publicKey) : false
   export const decode = (token: string) => { return jws.decode(token)?.payload }
Tasks:
1. Explain in simple terms what CWE 798 means.
2. Code Analysis:
   a. Estimate the probability of a False Positive. What do you need to check in
      the code or logic of the application to confirm or deny this?
   b. Explain why this particular code snippet is a problem in this context.
   c. Provide a corrected code snippet for this particular location.
3. Business Impact: Estimate the potential business impact (e.g., data breach,
      financial or reputational loss) if this vulnerability is exploited, taking
      into account the severity and context.
```

Рисунок 3 – Запит для вразливості javascript_express_hardcoded_secret

Було детально розглянуто результати моделей по першій вразливості – javascript_express_hardcoded_secret. CWE-798: “Use of Hard-coded Credentials” означає, що облікові дані, наприклад паролі, секретні ключі, ключі API або інші облікові дані зберігаються безпосередньо у вихідному коді програми. Це робить систему дуже вразливою, оскільки будь-хто, хто має доступ до коду (розробники та потенційні зловмисники), може легко знайти та використати ці секрети.

GPT-4o: модель впоралась добре. Її відповідь здатна допомогти у аналізі вразливості для фахового розробника. Точність пояснень – хороша, дає розуміння проблеми, її причини та наслідки. Корисність виправлень – середня, запропоновані виправлення допоможуть в усуненні вразливості, однак самі виправлення – поверхневі та недостатньо детальні. Оцінка бізнес-впливу – релевантна та дає розуміння, які можуть бути наслідки експлуатації вразливості.

GPT-4.5: модель впоралась відмінно. Її відповідь також цілком здатна допомогти у аналізі вразливості для фахового розробника. Точність пояснень – хороша, розробник розумітиме причини виникнення та наслідки . Корисність виправлень – дуже висока, запропоновані виправлення допоможуть в усуненні вразливості, модель також додала додаткову обробку помилок у разі відсутності секретних ключів у змінних середовища. Оцінка бізнес-впливу – повністю релевантна та дає розуміння, які можуть бути наслідки експлуатації вразливості.

GPT-o3-mini-high: модель впоралась добре. Її відповідь також цілком здатна допомогти у аналізі вразливості для фахового розробника. Точність пояснень – задовільна, розробник поверхнево розумітиме проблеми, пов’язані з вразливістю. Корисність виправлень – дуже висока, запропоновані виправлення допоможуть в усуненні вразливості, модель також додала додаткову обробку помилок у разі відсутності секретних ключів у змінних середовища. Оцінка бізнес-впливу – повністю релевантна та дає розуміння, які можуть бути наслідки експлуатації вразливості.

Gemini 2.5 Pro: модель впоралась винятково, її результат – найкращий у порівнянні з іншими моделями. Її відповідь здатна повністю допомогти у аналізі вразливості для фахового розробника. Точність пояснень – відмінна, розробник матиме детальне але водночас просте пояснення, повне розуміння причин виникнення та наслідків експлуатації вразливості. Корисність виправлень – дуже висока, запропоновані виправлення допоможуть в усуненні вразливості, модель також додала додаткову обробку помилок у разі відсутності секретних ключів у змінних середовища. Оцінка бізнес-впливу – повністю релевантна та дає розуміння, які можуть бути наслідки експлуатації вразливості.

Claude 3.7 Sonnet: модель впоралась добре. Її відповідь також цілком здатна допомогти у аналізі вразливості для фахового розробника. Точність пояснень – хороша, розробник розумітиме причини виникнення та наслідки. Корисність виправлень – дуже висока, запропоновані виправлення допоможуть в усуненні вразливості, модель також додала додаткову обробку помилок у разі відсутності секретних ключів у змінних середовища. Оцінка бізнес-впливу – достатньо релевантна та дає розуміння, які можуть бути наслідки експлуатації вразливості.

Перейдемо до **другої вразливості — javascript_express_external_file_upload**. Аналогічно було сформульовано запит та проаналізовано результати п’яти моделей.

```
Analyze the SAST output.
Input:
1. SAST Rule: javascript_express_external_file_upload
2. CWE: 73
3. Severity: high
4. File: juice-shop/routes/quarantineServer.ts
5. Line number: 14
6. Line: res.sendFile(path.resolve('ftp/quarantine/', file))
7. Code Snippet: if (!file.includes('/')) {
      res.sendFile(path.resolve('ftp/quarantine/', file))
    } else {
      res.status(403)
      next(new Error('File names cannot contain forward slashes!'))
    }
Tasks:
1. Explain in simple terms what CWE [Insert CWE ID] means.
2. Code Analysis:
   a. Estimate the probability of a False Positive. What do you need
      to check in the code or logic of the application to confirm or deny this?
   b. Explain why this particular code snippet is a problem in this context.
   c. Provide a corrected code snippet for this particular location.
3. Business Impact: Estimate the potential business impact (e.g., data breach,
      financial or reputational loss) if this vulnerability is exploited, taking
      into account the severity and context.
```

Рисунок 4 – Запит для вразливості javascript_express_external_file_upload

CWE-73: “External Control of File Name or Path” означає, що вихідний код містить небезпечні логічні помилки, які дозволяють досягати файлів за вказанням шляху без його перевірки, завдяки чому зловмисник може вийти за межі призначеної для нього директорії та отримати доступ до інших файлів або каталогів на сервері, до яких він не повинен мати доступу.

GPT-4o: модель впоралась відмінно. Її відповідь здатна повністю допомогти у аналізі вразливості для фахового розробника. Точність пояснень – відмінна та дає повне розуміння проблеми, її причини та наслідки. Корисність виправлень – також відмінна, запропоновані виправлення допоможуть в усуненні вразливості. Оцінка бізнес-впливу – релевантна та дає розуміння, які можуть бути наслідки експлуатації вразливості.

GPT-4.5: модель впоралась задовільно. Її відповідь здатна допомогти у аналізі вразливості для фахового розробника. Точність пояснень – хороша, розробник розумітиме причини виникнення та наслідки. Корисність виправлень – висока, запропоновані виправлення допоможуть в усуненні вразливості. Оцінка бізнес-впливу – релевантна та дає розуміння, які можуть бути наслідки експлуатації вразливості.

GPT-o3-mini-high: модель впоралась відмінно. Її відповідь також цілком здатна допомогти у аналізі вразливості для фахового розробника. Точність пояснень – відмінна та дає повне розуміння проблеми, її причини та наслідки. Корисність виправлень – висока, запропоновані виправлення допоможуть в усуненні вразливості. Оцінка бізнес-впливу – повністю релевантна та дає розуміння, які можуть бути наслідки експлуатації вразливості.

Gemini 2.5 Pro: модель впоралась винятково, для цієї вразливості її результат – теж найкращий у порівнянні з іншими моделями. Її відповідь здатна повністю допомогти у аналізі вразливості для фахового розробника. Точність пояснень – відмінна, розробник матиме детальне але водночас просте пояснення, повне розуміння причин виникнення та наслідків експлуатації вразливості. Корисність виправлень – дуже висока, запропоновані виправлення допоможуть в усуненні вразливості, модель дуже детально написала код який запобігає вразливості. Оцінка бізнес-впливу – повністю релевантна та дає розуміння, які можуть бути наслідки експлуатації вразливості.

Claude 3.7 Sonnet: модель впоралась задовільно. Її відповідь може допомогти у аналізі вразливості для фахового розробника. Точність пояснень – задовільна, розробник розумітиме причини виникнення та наслідки, але пояснення короткі та поверхневі. Корисність виправлень – висока, запропоновані виправлення допоможуть в усуненні вразливості. Оцінка бізнес-впливу – достатньо релевантна та дає розуміння, які можуть бути наслідки експлуатації вразливості.

Перейдемо до **третьої вразливості — javascript_express_open_redirect**. Як і в попередніх випадках, було сформульовано відповідний запит та проаналізовано результати п’яти мовних моделей.

```
Analyze the SAST output.
Input:
1. SAST Rule: javascript_express_open_redirect
2. CWE: 601
3. Severity: medium
4. File: juice-shop/routes/redirect.ts
5. Line number: 19
6. Line: res.redirect(toUrl)
7. Code Snippet: if (security.isRedirectAllowed(toUrl)) {
      challengeUtils.solveIf(challenges.redirectCryptoCurrencyChallenge, () => {
        return toUrl === 'https://explorer.dash.org/address/Xr556RzuwX6hg5EGpkybbv5RanJoZN17kW'
        || toUrl === 'https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm'
        || toUrl === 'https://etherscan.io/address/0x0f933ab9fcaaa782d0279c300d73750e1311eae6' })
      challengeUtils.solveIf(challenges.redirectChallenge,
        () => { return isUnintendedRedirect(toUrl) })
      res.redirect(toUrl)
    } else {
      res.status(406)
      next(new Error('Unrecognized target URL for redirect: ' + toUrl))
    }

Tasks:
1. Explain in simple terms what CWE [Insert CWE ID] means.
2. Code Analysis:
   a. Estimate the probability of a False Positive. What do you need
      to check in the code or logic of the application to confirm or deny this?
   b. Explain why this particular code snippet is a problem in this context.
   c. Provide a corrected code snippet for this particular location.
3. Business Impact: Estimate the potential business impact (e.g., data breach,
      financial or reputational loss) if this vulnerability is exploited, taking
      into account the severity and context.
```

Рисунок 5 – Запит для вразливості javascript_express_open_redirect

CWE-601: “URL Redirection to Untrusted Site ('Open Redirect')” означає, що вразливість виникає коли веб-додаток перенаправляє користувача на іншу URL-адресу, яка вказана у вхідному параметрі запиту, але не перевіряє належним чином, чи є ця цільова URL-адреса безпечною та довіреною. Зловмисник може створити посилання, яке виглядає так, ніби веде на легітимний сайт, але насправді містить параметр, що перенаправляє користувача на фішинговий або небезпечний сайт. Користувач, довіряючи початковому посиланню, може перейти за ним і стати жертвою атаки.

GPT-4o: модель впоралась добре. Її відповідь здатна допомогти у аналізі вразливості для фахового розробника. Точність пояснень – відмінна, лаконічно пояснює проблему, її причини та можливі наслідки. Корисність виправлень – задовільна, запропоновані виправлення – поверхневі та недостатньо детальні, вони повноцінно не усувають проблему. Оцінка бізнес-впливу – релевантна та дає розуміння, які можуть бути наслідки експлуатації вразливості.

GPT-4.5: модель впоралась задовільно. Її відповідь загалом допоможе з усуненням уразливості, але не розкриває причини і наслідки проблеми. Точність пояснень – задовільна, фокусується лише на одній загрозі, пов’язаній з уразливістю. Корисність виправлень – хороша, виправлення містить додаткову обробку помилок. Оцінка бізнес-впливу – неточна, упущено декілька критичних ризиків.

GPT-o3-mini-high: модель впоралась добре. Її відповідь дозволить розробнику зрозуміти суть уразливості й усунути її. Точність пояснень – середня, надає розуміння уразливості та способи визначення хибнопозитивності спрацювання, але на відміну від інших

моделей, сам цього не оцінює. Корисність виправлень – хороша, виправлений код також містить додаткову обробку помилок. Оцінка бізнес-впливу – цілком релевантна, надає повне розуміння дає розуміння, які можуть бути наслідки експлуатації вразливості.

Gemini 2.5 Pro: модель впоралась винятково, для цієї вразливості її результат – теж найкращий у порівнянні з іншими моделями. Її відповідь здатна повністю допомогти у аналізі вразливості для фахового розробника. Точність пояснень – відмінна, розробник матиме детальне але водночас просте пояснення, повне розуміння причин виникнення та наслідків експлуатації вразливості. Корисність виправлень – дуже висока, запропоновані виправлення допоможуть в усуненні вразливості, модель дуже детально написала код який запобігає вразливості. Оцінка бізнес-впливу – повністю релевантна та дає розуміння, які можуть бути наслідки експлуатації вразливості.

Claude 3.7 Sonnet: модель впоралась задовільно. Її відповідь може допомогти у аналізі вразливості для фахового розробника. Точність пояснень – задовільна, розробник розумітиме причини виникнення та наслідки, але пояснення короткі та поверхневі. Корисність виправлень – висока, запропоновані виправлення допоможуть в усуненні вразливості. Оцінка бізнес-впливу – достатньо релевантна та дає розуміння, які можуть бути наслідки експлуатації вразливості.

Після аналізу усіх результатів роботи генеративних моделей ШІ, було проведено оцінювання згідно з чотирма критеріями – точність пояснень, корисність виправлень, узгодженість відповідей і релевантність оцінки бізнес-впливу за п’ятибальною шкалою, та винесено у окрему таблицю (табл. 1). Варто відзначити, що всі протестовані моделі продемонстрували високий рівень узгодженості відповідей, чітко дотримуючись заданої структури запиту. Найкращі результати за більшістю критеріїв продемонструвала Gemini 2.5 Pro, що отримала найвищий загальний бал. Інші моделі також показали конкурентоспроможні результати, проте мали певні недоліки, зокрема в точності пояснень або оцінці бізнес-впливу.

Таблиця 1 – Результати оцінювання роботи генеративних моделей ШІ за критеріями

	Критерії	GPT-4o	GPT-4.5	GPT-o3-mini-high	Gemini 2.5 Pro	Claude 3.7
Вразливість 1 (CWE-798)	точність пояснень	4	4	3	5	4
	корисність виправлень	3	5	5	5	5
	узгодженість відповідей	5	5	5	5	5
	релевантність оцінки бізнес-впливу	4	5	5	5	4
Вразливість 2 (CWE-73)	точність пояснень	5	4	5	5	3
	корисність виправлень	5	4	4	5	4
	узгодженість відповідей	5	5	5	5	5

	Критерії	GPT-4o	GPT-4.5	GPT-o3-mini-high	Gemini 2.5 Pro	Claude 3.7
	релевантність оцінки бізнес-впливу	4	4	5	5	4
Вразливість 3 (CWE-601)	точність пояснень	5	4	4	5	3
	корисність виправлень	3	4	4	5	4
	узгодженість відповідей	5	5	5	5	5
	релевантність оцінки бізнес-впливу	4	2	5	5	4
Фінальний бал:		**52**	**51**	**55**	**60**	**50**

Висновки

У результаті проведеного дослідження було проаналізовано вплив генеративного штучного інтелекту на аналіз результатів роботи SAST інструмента Bearer CLI. З метою порівняльної оцінки можливостей різних мовних моделей у контексті досліджуваної проблематики було розглянуто GPT-4o, GPT-4.5, GPT-o3-mini-high, Gemini 2.5 Pro та Claude 3.7.

Порівняльний аналіз показав, що найкращий результат щодо точності, зрозумілості та повноти пояснень було досягнуто за використання моделі Gemini 2.5 Pro, яка забезпечила найкращі пояснення з якісними рекомендаціями щодо виправлення вразливостей. Якісні результати показала також модель GPT-o3-mini-high. Дві попередньо названі моделі показують тенденцію, що моделі міркування демонструють найбільш точні та якісні результати. Решта моделей також показали хороший результат, який покращує розуміння результатів статичного аналізу людьми, непов'язаними з кібербезпекою.

Вище описані результати свідчать про потенціал використання генеративного ШІ для аналізу результатів SAST, що актуально для людей, які не мають достатньо глибоких знань у галузі кібербезпеки. Також дослідження підтвердило доцільність застосування генеративних моделей для надання зрозумілих рекомендацій з виправлення вразливостей.

Запропоновані рекомендації для покращення ефективності використання генеративного ШІ включають: випробування більш спеціалізованих моделей або адаптація вже доступних під конкретні вимоги інструментів статичного сканування, що може включати розробку автоматизованих агентів ШІ для зручності використання. Хорошим рішенням буде інтеграція генеративних моделей у процеси CI/CD для автоматизованого формування пояснень в реальному часі.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. OpenText. What is SAST? [Електронний ресурс]. Available from: https://www.opentext.com/what-is/sast. Accessed: April 1, 2025.
2. Ahmad, B., Tan, B., Karri, R., & Pearce, H. (2023). FLAG: Finding line anomalies (in code) with generative AI. arXiv. https://doi.org/10.48550/arXiv.2306.12643
3. Bearer. Bearer CLI documentation [Електронний ресурс]. Available from: https://docs.bearer.com. Accessed: April 1, 2025.
4. Markson, Reed & Samson, Mike & Owen, Antony. (2023). Automated Code Review: Leveraging Generative AI for Vulnerability Detection in Software Development. ResearchGate. https://www.researchgate.net/publication/390108092_Automated_Code_Review_Leveraging_Generative_AI_for_Vulnerability_Detection_in_Software_Development
5. Check Point. What is Static Application Security Testing (SAST)? [Електронний ресурс]. Available from: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-static-application-security-testing-sast. Accessed: April 1, 2025.
6. Sharma, R. An Analysis of Generative AI Capabilities in Security Testing. Evaluating Static Code Analysis Performance. Digitala Vetenskapliga Arkivet. https://www.diva-portal.org/smash/get/diva2:1941555/FULLTEXT01.pdf
7. Amazon Web Services. What is a large language model? [Електронний ресурс]. Available from: https://aws.amazon.com/what-is/large-language-model. Accessed: April 1, 2025.
8. DataCamp. How transformers work [Електронний ресурс]. Available from: https://www.datacamp.com/tutorial/how-transformers-work. Accessed: April 1, 2025.
9. Yuanjiang Cao, Quan Z. Sheng, Julian McAuley & Lina Yao. (2021). Reinforcement Learning for Generative AI: A Survey. Journal Of Latex Class Files, 14(8). https://doi.org/10.48550/arXiv.2308.14328
10. OpenAI. Guides: Reasoning [Електронний ресурс]. Available from: https://platform.openai.com/docs/guides/reasoning?api-mode=responses. Accessed: April 1, 2025.
11. Ding, A. et al., "Generative AI for Software Security Analysis: Fundamentals, Applications, and Challenges" in IEEE Software, vol. 41, no. 06, pp. 46-54, Nov.-Dec. 2024 .https://doi.ieeecomputersociety.org/10.1109/MS.2024.3416036
12. Hicken, A. (2023, 12 травня). False Positives in Static Code Analysis. Parasoft. https://www.parasoft.com/blog/false-positives-in-static-code-analysis/
13. Fan, Gang, Xie, Xiaoheng, Zheng, Xunjin, Liang, Yinan, and Di, Peng. (2023). Static Code Analysis in the AI Era: An In-depth Exploration of the Concept, Function, and Potential of Intelligent Code Analysis Agents. arXiv. https://doi.org/10.48550/arXiv.2310.08837

References

1. OpenText. What is SAST? [Електронний ресурс]. Available from: https://www.opentext.com/what-is/sast. Accessed: April 1, 2025.
2. Ahmad, B., Tan, B., Karri, R., & Pearce, H. (2023). FLAG: Finding line anomalies (in code) with generative AI. arXiv. https://doi.org/10.48550/arXiv.2306.12643
3. Bearer. Bearer CLI documentation [Електронний ресурс]. Available from: https://docs.bearer.com. Accessed: April 1, 2025.
4. Markson, Reed & Samson, Mike & Owen, Antony. (2023). Automated Code Review: Leveraging Generative AI for Vulnerability Detection in Software Development. ResearchGate. https://www.researchgate.net/publication/390108092_Automated_Code_Review_Leveraging_Generative_AI_for_Vulnerability_Detection_in_Software_Development

5. Check Point. What is Static Application Security Testing (SAST)? [Електронний ресурс]. Available from: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-static-application-security-testing-sast. Accessed: April 1, 2025.
6. Sharma, R. An Analysis of Generative AI Capabilities in Security Testing. Evaluating Static Code Analysis Performance. Digitala Vetenskapliga Arkivet. https://www.diva-portal.org/smash/get/diva2:1941555/FULLTEXT01.pdf
7. Amazon Web Services. What is a large language model? [Електронний ресурс]. Available from: https://aws.amazon.com/what-is/large-language-model. Accessed: April 1, 2025.
8. DataCamp. How transformers work [Електронний ресурс]. Available from: https://www.datacamp.com/tutorial/how-transformers-work. Accessed: April 1, 2025.
9. Yuanjiang Cao, Quan Z. Sheng, Julian McAuley & Lina Yao. (2021). Reinforcement Learning for Generative AI: A Survey. Journal Of Latex Class Files, 14(8). https://doi.org/10.48550/arXiv.2308.14328
10. OpenAI. Guides: Reasoning [Електронний ресурс]. Available from: https://platform.openai.com/docs/guides/reasoning?api-mode=responses. Accessed: April 1, 2025.
11. Ding, A. et al., "Generative AI for Software Security Analysis: Fundamentals, Applications, and Challenges" in IEEE Software, vol. 41, no. 06, pp. 46-54, Nov.-Dec. 2024 .https://doi.ieeecomputersociety.org/10.1109/MS.2024.3416036
12. Hicken, A. (2023, 12 травня). False Positives in Static Code Analysis. Parasoft. https://www.parasoft.com/blog/false-positives-in-static-code-analysis/
13. Fan, Gang, Xie, Xiaoheng, Zheng, Xunjin, Liang, Yinan, and Di, Peng. (2023). Static Code Analysis in the AI Era: An In-depth Exploration of the Concept, Function, and Potential of Intelligent Code Analysis Agents. arXiv. https://doi.org/10.48550/arXiv.2310.08837

Кластеризація та класифікація об’єктів групових цілей противника на основі нейронних мереж

Clustering and Classification of Enemy Group Targets Based on Neural Networks

Юрій Гусак [A]
д. військ. н., професор, професор кафедри інформаційно-аналітичних технологій, e-mail: y_husak1512@gmail.com, ORCID: 0000-0002-3423-2112

Ольга Василенко [B]
Corresponding author: ад’юнкт Центрального науково-дослідного інституту Збройних Сил України, e-mail: nicety@ukr.net, ORCID: 0000-0003-2633-0131

Yurii Husak [A]
Dr of Military Sciences, Professor, Professor of the Department of Information and Analytical Technologies, e-mail: y_husak1512@gmail.com, ORCID: 0000-0002-3423-2112

Olha Vasylenko [B]
Corresponding author: PhD student of Central Research Institute of the Armed Forces of Ukraine, e-mail: nicety@ukr.net, ORCID: 0000-0003-2633-0131

[A] Національний університет оборони України, м. Київ, Україна
[B] Центральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна

[A] National Defense University of Ukraine, Kyiv, Ukraine
[B] Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine

Received: April 4, 2025 | Revised: April 28, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.18

Мета роботи: розроблення нейронних мереж для кластеризації та класифікації об’єктів групових цілей противника на основі алгоритмів штучного інтелекту.

Метод дослідження: методи аналізу, індукції та дедукції; окремі положення системного підходу, методи штучного інтелекту.

Результати дослідження: розроблено та показано використання нейронних мереж кластеризації та класифікації об’єктів групових цілей противника. Нейронні мережі можуть бути використані під час пошуку та ураження роєм БпЛА нестаціонарних групових цілей противника за визначеними класифікаційними ознаками для завдавання їм максимального збитку.

Теоретична цінність дослідження: теоретична цінність дослідження полягає у використанні методів штучного інтелекту, а саме нейронних мереж для розв’язання задач кластеризації та класифікації об’єктів групових цілей противника.

Тип статті: теоретичний**,** описовий, методичний.

Purpose: The purpose of the article is to reveal the main aspects of the formation of a strategic leader and his red team in the military sphere, as well as to determine the specifics of his mission in the highest echelon of the state's military management system.

Method: the main methods of research are methods of analysis, induction and deduction; formalization and expert survey.

Findings: the main results of the article are: the results of the analysis of foreign and domestic studies devoted to the topic of leadership development in the military sphere; identification and assessment of the main factors that affect the effectiveness of the strategic military leader and his red team; identification of the main members of the strategic military leader's red team; defining the features of forming the image of a strategic military leader.

Theoretical implications: the theoretical value of the research lies in determining the main aspects of the formation of a strategic leader and his red team.

Paper type: theoretical, descriptive, methodical.

Ключові слова: кластеризація, класифікація, нейронна мережа, групова ціль, безпілотні літальні апарати, рій, згорткові нейронні мережі, російсько-українська війна.

Key words: clustering, classification, neural network, group target, unmanned aerial vehicles, swarm, convolutional neural networks, Russian-Ukrainian war.

Вступ

Досвід ведення бойових дій Збройними Силами України, особливо у 2022–2025 роках, є унікальним. Під час російсько-української війни відбуваються зміни стратегії, форм та способів застосування військ. Однією з причин цього є розвиток безпілотних систем, застосування яких стало масовим та дозволяє виконувати завдання широкого спектра.

На цей час застосування безпілотних систем є дієвим засобом ураження як у позиційній, так і в маневреній обороні. При цьому на тактичному рівні актуальними завданнями є ураження нестаціонарних групових цілей противника як на передньому краї, так і в глибині; завдавання масованих раптових ударів по об’єктах його критичної інфраструктури та важливих комунікаціях. Застосування дорогих в експлуатації та виробництві інших засобів вогневого ураження і радіоелектронного подавлення при цьому зводиться до мінімуму.

Наразі спроможності безпілотних систем збільшуються завдяки застосуванню роїв ударних БпЛА, що суттєво впливає на перебіг бойових дій [1].

Теоретичні основи дослідження

Зважаючи на перспективність технологій штучного інтелекту [1–4], розроблення нейронних мереж для кластеризації та класифікації об’єктів групових цілей є актуальною задачею.

Зокрема, у роботі [5] використано нейронну мережу для розроблення системи, що здатна навчатися розпізнаванню типу БпЛА за результатами аналізу трафіка, який передається ним на наземну станцію керування. Автором зауважено, що здатність нейронної мережі до узагальнення, за достатнього обсягу навчальної вибірки, дозволяє НМ екстраполювати свої знання про відомі види мережевих дій на невідомі види. При цьому вирішальну роль відіграє вибір адекватної поставленим завданням архітектури НМ.

У [6, 7] розглянуто застосування різних типів нейронних мереж для розпізнавання та класифікації об’єктів.

У [8, 9] здійснено кластеризацію та класифікацію ударних БпЛА на основі нейронних мереж. Результати аналізу залежності точності кластеризації від кількості нейронів у прихованому шарі показали, що нейронна мережа кластеризації ударних безпілотних літальних апаратів NN SOM FPV UAVs має найкращу точність при 18 нейронах у прихованому шарі. Кластеризація ударних безпілотних літальних апаратів продемонструвала, що їх можна поділити на 4 кластери. При цьому за кількістю БпЛА у кожному кластері їх можна згрупувати у 3 класи. Навчання CNN FPV UAVs здійснювалось за допомогою алгоритму Левенберга – Марквардта, загальна точність нейронної мережі класифікації ударних безпілотних літальних апаратів становила 98,9%.

Загалом аналіз наукових публікацій свідчить про те, що розвиток технологій класифікації об’єктів на основі нейронних мереж має значні перспективи, особливо у контексті підвищення точності, швидкості роботи та стійкості до швидкозмінних умов.

Питанням кластеризації та класифікації об’єктів групових цілей на основі нейронних мереж приділено недостатньо уваги. Отже, особливої уваги заслуговує кластеризація і класифікація групових цілей – з одного боку, і визначених класів ударних БпЛА – з іншого боку.

Постановка проблеми

Нині застосування груп (роїв) ударних БпЛА суттєво впливає на перебіг бойових дій [1].

Можуть застосовуватися як однорідні за типами ударних БпЛА рої, так і неоднорідні. При цьому, з точки зору організації управління роєм, рої мають складатися з однотипних (або з БпЛА квадрокоптернового типу, або з БПЛА літакового типу) ударних БпЛА [1].

Однорідні рої ударних БпЛА складаються з однакових ударних БпЛА, а неоднорідні – з БпЛА різних класів.

Оскільки групова ціль майже завжди складається з неоднорідних об’єктів, то для знищення такої цілі має бути застосовано неоднорідний рій ударних БпЛА.

Для ураження неоднорідної групової цілі неоднорідним роєм ударних БпЛА з максимальною ефективністю необхідно розв’язати оптимізаційну задачу розподілу неоднорідних ударних БпЛА по об’єктах неоднорідної групової цілі.

Для розв’язання зазначеної оптимізаційної задачі необхідно, щоб система цілерозподілу БпЛА по об’єктах групової цілі здійснила класифікацію об’єктів групової цілі та призначила кожному об’єкту ударний БпЛА або декілька ударних БпЛА відповідного класу.

Для класифікації об’єктів групової цілі може бути застосовано методи та алгоритми штучного інтелекту, а саме нейронні мережі (НМ) [2, 3].

Метою статті є розроблення нейронних мереж для кластеризації та класифікації об’єктів групових цілей противника на основі алгоритмів штучного інтелекту.

Результати

У роботі [10] запропоновано використовувати таку класифікацію типів об'єктів (цілей), розташованих у наземних (надводних) і повітряних областях земного простору:

а) перший тип – точкові об'єкти (зразки наземної (надводної) техніки, люди, невеликі групи людей);

б) другий тип – лінійні об'єкти (колони техніки, автомобільні й залізничні, нафто- і газотрубопроводи, лінії електропередач);

в) третій тип – пласкі об'єкти (великі групи точкових об'єктів, агрополя, лісові масиви, населені пункти, зони повеней і землетрусів);

г) четвертий тип – просторові об'єкти (області хімічного і радіоактивного зараження повітряного басейну).

Крім того, об'єкти групової цілі може бути класифіковано за групами вогневого ураження (табл. 1).

Таблиця 1 – Групи об'єктів вогневого ураження

Номер групи вогневого ураження	Назва групи об'єктів	Об'єкти вогневого ураження
1-ша група	Засоби ВТЗ, РУК(РВК), ПУ ОТР (ТР), артилерія, РСЗВ	Взводи ПУ ТР (ОТР), артилерійські взводи (батареї), взводи (батареї) РСЗВ, мінометні роти
2-га група	Пункти управління військами і зброєю	КП (ПКП, ОКП) ПА, АК, дивізій, бригад, батальйонів, ПУВ, ЦУВ, засоби розвідки та РЕБ
3-тя група	Об'єкти авіаційного угруповання	Тактична авіація на аеродромах, армійська авіація на посадкових майданчиках
4-та група	Об'єкти ППО	Батареї (взводи) ЗРК
5-та група	Військові угруповання	Мотопіхотні, піхотні, танкові, мінометні роти, винищувальні протитанкові роти у районах зосередження, на марші, під час висування та розгортання
6-та група	Інші об'єкти	Об'єкти тилу, інфраструктури та ін.

Отже, маємо досить велику кількість різноманітних (за характером) об'єктів в оперативній побудові противника, що підкреслює необхідність зваженого підходу до раціонального розподілу ударних БпЛА по об'єктах групової цілі з урахуванням їхньої пріоритетності.

Розглянемо, як завдання кластеризації та класифікації об'єктів групової цілі може бути вирішено із застосуванням нейронних мереж.

Створення та використання нейронних мереж для класифікації об'єктів групової цілі передбачає [8] (рис. 1): 1) формування бази даних об'єктів групової цілі; 2) вибір архітектури нейронної мережі; 3) вибір алгоритму навчання нейронної мережі; 4) навчання нейронної мережі; 5) оцінювання результатів навчання нейронної мережі; 6) використання нейронної мережі класифікації об'єктів групової цілі.

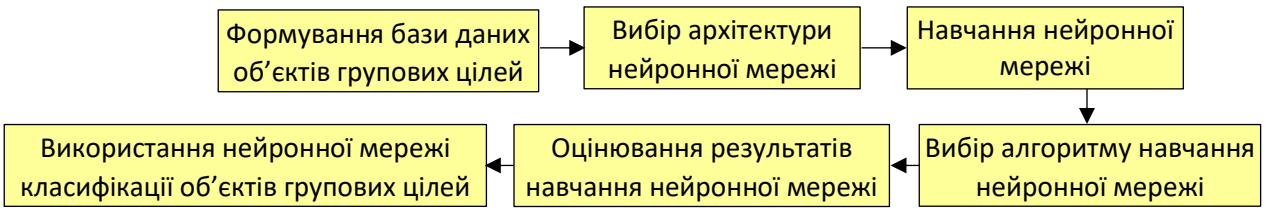


Рисунок 1 – Етапи створення та використання нейронної мережі класифікації об'єктів групових цілей

1. Формування бази даних об'єктів групової цілі. База даних об'єктів групової цілі формувалась з різних типів озброєння та військової техніки (ОВТ): танки, реактивні системи залпового вогню, артилерійські системи калібру 100-мм та більше, міномети, протитанкові ракетні комплекси, засоби протиповітряної оборони, літаки, автомобілі, протикорабельні засоби, бойові кораблі, БпЛА противника (табл. 2).

Таблиця 2 – Кількість зразків об'єктів групових цілей за типами озброєння та військової техніки

№ з/п	Типи озброєння та військової техніки	Кількість
1.	Танки	50
2.	БМП	27
3.	БТР	27
4.	ББМ	18
5.	ПУ тактичних та оперативно-тактичних ракет	5
6.	Реактивні системи залпового вогню	9
7.	Артилерійські системи калібру 100-мм та більше	22
8.	Міномети	27
9.	Протитанкові засоби (артилерія)	5
10.	Протитанкові ракетні комплекси	21
11.	Засоби протиповітряної оборони	81
12.	Літаки	73
13.	Вертольоти	20
14.	Автомобілі	20
15.	Протикорабельні засоби	5
16.	Бойові кораблі	26
17.	Безпілотні літальні апарати	17
18.	Особовий склад (група, відділення тощо)	5
	Загальна кількість зразків:	456

У табл. 2 наведено 456 зразків різних типів ОВТ, які застосовує противник у російсько-українській війні.

Об'єкти групових цілей противника, які представлено у табл. 1, може бути згруповано по класах.

2. Вибір архітектури нейронної мережі кластеризації об'єктів групової цілі. Для того, щоб здійснити розподіл об'єктів групової цілі за класами, застосуємо процедуру кластеризації. У задачі кластеризації нейронна мережа буде групувати об'єкти групової цілі по кластерах за значенням бойового потенціалу зразка ОВТ.

Для кластеризації об'єктів групової цілі за допомогою нейронної мережі необхідно створити і навчити мережу, а також оцінити її ефективність за допомогою різноманітних інструментів візуалізації (додаток Clastering у пакеті прикладних програм MATLAB).

Для кластеризації об'єктів групових цілей виберемо нейронну мережу типу SELFORGMAP (самоорганізовані карти), яка складається з шару нейронів, що може класифікувати набір даних векторів з будь-якою розмірністю на стільки класів, скільки нейронів має шар. Нейрони розташовані у двовимірній топології, що дозволяє шару формувати представлення розподілу та двовимірну апроксимацію топології набору даних. Навчання мережі проведемо за допомогою пакетного алгоритму self-organizing map (SOM).

Самоорганізовані карти навчаються кластеризувати дані на основі подібності, топології, з перевагою призначення однакової кількості екземплярів кожному класу.

3. Кластеризація об'єктів групових цілей. Для кластеризації об'єктів групових цілей сформовано матрицю із вхідними даними розміром 1x456 (табл. 2).

Експериментальним шляхом встановлено, що самоорганізована карта має складатися з 5 нейронів, а в нейронній мережі має бути один вхід та один вихід.

Архітектуру нейронної мережі кластеризації об'єктів групових цілей наведено на рис. 2.

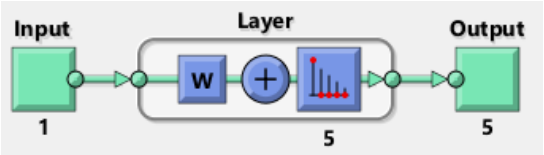


Рисунок 2 – Архітектура нейронної мережі кластеризації об'єктів групових цілей (NN SOM GTs)

NN SOM GTs підтримує топологію hextop, яка створює набір нейронів, що розташовуються у гексагональному порядку (рис. 3).

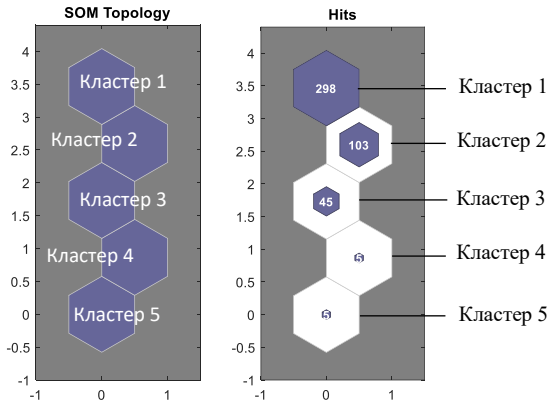


Рисунок 3 – Діаграми кластерів для об'єктів групових цілей: а) за кластерами та б) за кількістю об'єктів групових цілей

Результати аналізу даних щодо об'єктів групових цілей (табл. 1) за допомогою нейронної мережі SELFORGMAP об'єктів групових цілей (NN SOM GTs) продемонстровано на рис. 3 та рис. 4.

Отже, до кластера 1 входить 298 об'єктів групових цілей, до кластера 2 – 103, до кластера 3 – 45, до кластера 4 – 5 та до кластера 5 – 5 об'єктів.

Результати розподілу об'єктів групових цілей на кластери внесено до табл. 2.

У подальшому це дозволить використовувати створену нейронну мережу кластеризації об'єктів групової цілі (NN SOM GTs) для їхнього розподілу на класи.



Рисунок 4 – Розподіл об'єктів групових цілей по кластерах

На рис. 4 зображено розподіл об'єктів групових цілей по кластерах у вигляді зелених точок, які показують, як NN SOM GTs класифікує об'єкти групових цілей.

Отже, кластеризація об’єктів групових цілей противника дала можливість здійснити їхній поділ на класи.

Було виділено 5 класів об’єктів групових цілей противника:

до 1-го класу належать об’єкти групових цілей, які мають бойовий потенціал 0,6–2,7;

до 2-го класу – об’єкти групових цілей, що мають бойовий потенціал в інтервалі від 2,7 до 8;

до 3-го класу – об’єкти групових цілей, що мають бойовий потенціал в інтервалі від 8 до 23;

до 4-го класу – об’єкти групових цілей, які мають бойовий потенціал в інтервалі від 23 до 90;

до 5-го класу – об’єкти групових цілей, які мають бойовий потенціал понад 90.

4. Вибір архітектури нейронної мережі для класифікації об’єктів групових цілей. У пакеті прикладних програм MATLAB було розроблено нейронну мережу класифікації об’єктів групових цілей за значеннями їхніх бойових потенціалів.

Підготовка даних. Дані для задачі класифікації об’єктів групових цілей налаштовуються для нейронної мережі завдяки організації даних у дві матриці: вхідну матрицю X(p) і цільову матрицю T(y).

Для проведення дослідження було використано характеристики більш ніж 456 зразків об’єктів групових цілей противника.

Нейронна мережа для класифікації об’єктів групових цілей має два шари нейронів: прихований та вихідний (рис. 5).

Експериментально встановлено, що найкращий результат класифікації досягається, якщо кількість нейронів у прихованому шарі становить 15 нейронів.

Зв’язок між нейронами у прихованому шарі здійснюється за допомогою функції tansig, а у вихідному шарі – з використанням функції lin [9].

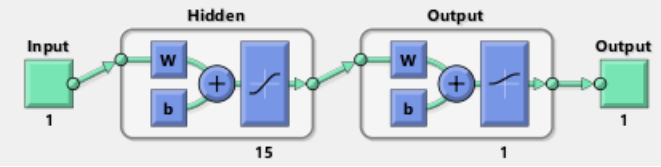


Рисунок 5 – Архітектура нейронної мережі класифікації об’єктів групових цілей (CNN GTs)

Розподілимо базу даних об’єктів групових цілей на набори для навчання, перевірки та тестування.

Навчальний набір використовується для навчання нейронної мережі. Навчання триває до того часу, поки мережа продовжує покращувати набір перевірки. Навчання нейронної мережі можна розглядати як розв’язання оптимізаційної задачі. Її метою є мінімізація функції похибок на цій вибірці шляхом вибору значень ваг W. Функцією навчання нейронної мережі класифікації об’єктів групових цілей обрано функцію trainbr.

Функція trainbr – баєсівська регуляризація зворотного поширення. Це функція навчання мережі, яка оновлює значення ваг та зміщення відповідно до оптимізації Левенберга – Марквардта, яка мінімізує комбінацію квадратичних похибок, ваг і зміщень, а потім визначає правильну комбінацію, щоб створити мережу, яка добре узагальнює. Такий процес називається баєсівською регуляризацією.

Навчання відбувається відповідно до trainbr параметрів навчання. Такими параметрами у програмному середовищі Matlab є:

net.trainParam.epochs – максимальна кількість епох для навчання (значення за замовчуванням – 1000);

net.trainParam.show – епохи між дисплеями (NaN якщо дисплеїв немає) – 25;

net.trainParam.showCommandLine – створення виведення командного рядка (значення за замовчуванням – false);

net.trainParam.showWindow – показати графічний інтерфейс навчання (значення за замовчуванням – true);

net.trainParam.mu – параметр регулювання Марквардта (значення за замовчуванням 0,005);

net.trainParam.mu_dec – коефіцієнт зменшення для mu (значення за замовчуванням – 0,1);

net.trainParam.mu_inc – коефіцієнт збільшення для mu (значення за замовчуванням – 10);

net.trainParam.mu_max – максимальне значення для mu (значення за замовчуванням – $1e^{10}$);

net.trainParam.max_fail – максимальна кількість помилок перевірки (значення за замовчуванням – 0);

net.trainParam.min_grad – мінімальний градієнт продуктивності (значення за замовчуванням – $1e^{-7}$);

net.trainParam.time – максимальний час навчання в секундах (значення за замовчуванням – inf).

Кожна вага та зміщення оновлюються відповідно до своєї функції навчання після кожної епохи (один прохід через увесь набір вхідних векторів).

Тестовий набір забезпечує абсолютно незалежне оцінювання точності класифікації нейронною мережею об’єктів групової цілі.

Отже, формуємо дані, створюємо та навчаємо нейронну мережу, а також оцінюємо її продуктивність за допомогою середньоквадратичної похибки та регресійного аналізу.

Із 456 об’єктів групових цілей здійснюється такий їхній розподіл: 319 (70%) – навчання; 69 – перевірка; 68 – тестування.

Навчання нейронної мережі здійснювалось за допомогою алгоритму Левенберга – Марквардта [5].

На рис. 6. представлено матрицю похибок під час навчання, перевірки і тестування нейронної мережі класифікації об’єктів групових цілей.

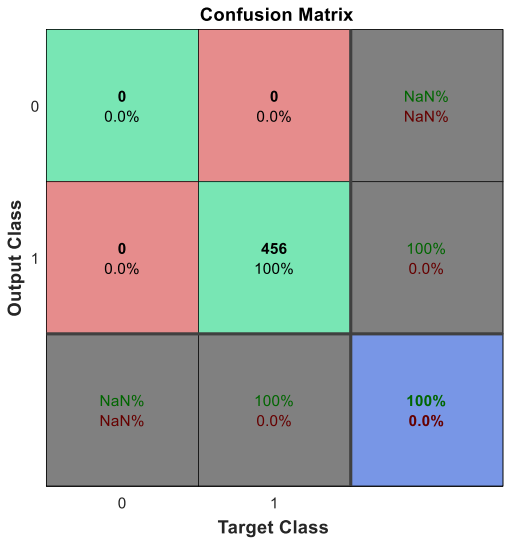


Рисунок 6 – Матриці похибок під час навчання, перевірки і тестування нейронної мережі класифікації об’єктів групових цілей

На рис. 6 видно, що нейронну мережу класифікації об’єктів групових цілей було навчено, перевірено і протестовано з точностями 100%, а загальна точність нейронної мережі класифікації об’єктів групових цілей становить 100%.

Під час розв'язання задачі оптимізації виконують обчислення перших похідних цільових і нелінійних функцій обмежень, а за допомогою функції checkGradients здійснюється перевірка запрограмованих похідних. Крім того, здійснюється перевірка, чи правильно обчислюється градієнт поблизу випадкової початкової точки [11–12].

На рис. 7 показано результати оцінювання градієнта цільової функції.

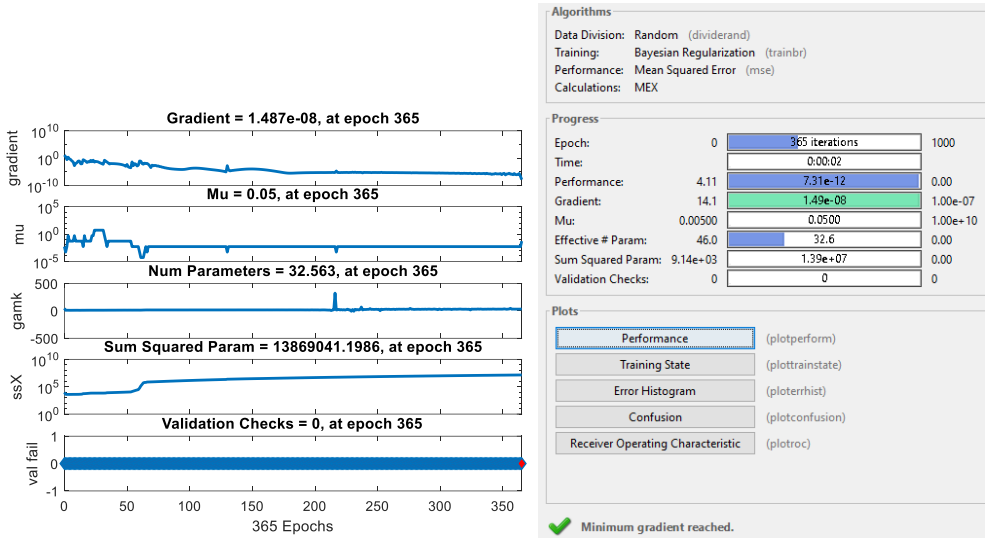


Рисунок 7 – а) Перевірка дійсності градієнтів; б) Перевірка продуктивності навчання CCN GTs

Рис. 7 показує, що найкраща продуктивність навчання CCN GTs досягається на 365-ій епосі.

На рис. 8 наведено гістограму похибок між цільовими значеннями та прогнозованими значеннями після навчання нейронної мережі класифікації об'єктів групових цілей. Гістограма показує, що CNN GTs має похибку з точністю до п'ятого знака.

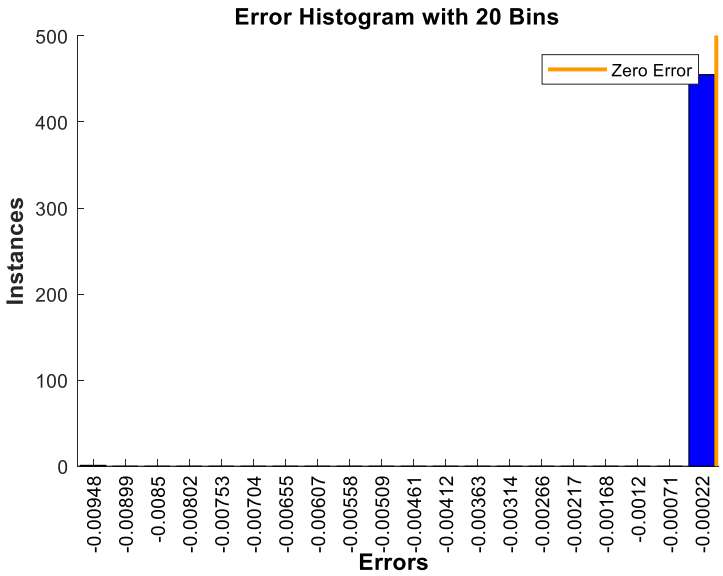


Рисунок 8 – Гістограма похибок

Значення похибки 0,00022 вказує на найкращу продуктивність мережі. Оскільки похибки близькі до нуля, то нейронна мережа класифікації об'єктів групових цілей моделює добре.

На рис. 9 зображено графік, що представляє дані навчання, перевірки та тестування нейронної мережі класифікації об’єктів групових цілей.

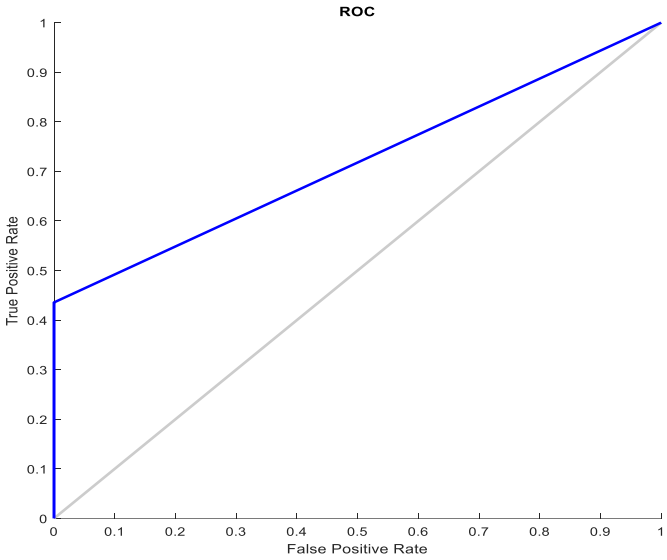


Рисунок 9 – Дані навчання, перевірки та тестування нейронної мережі класифікації об’єктів групових цілей

Пунктирна лінія на графіку представляє оптимальний результат, а суцільна лінія – лінія лінійної регресії, яка найкраще підходить між результатами та цільовими показниками.

Графік зміни значення цільової функції за епохами – циклами навчання наведено на рис. 10.

Серед параметрів навчання задано:

goal – максимально припустиме значення цільової функції;

epochs – максимально припустиму кількість циклів навчання мережі;

show – крок виведення на екран інформації про навчання мережі, задається у циклах навчання.

Графік вказує ітерацію, на якій ефективність перевірки досягла мінімуму [11–12].

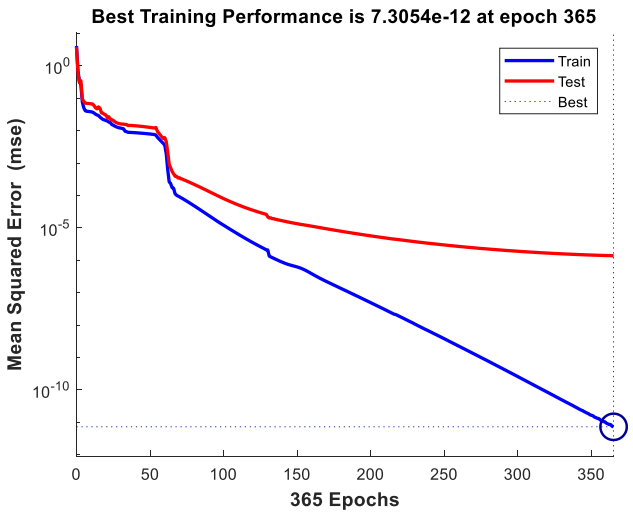


Рисунок 10 – Графік зміни значення цільової функції у процесі навчання

На рис. 10 видно, що на 365-й ітерації досягнуто локального мінімуму цільової функції.

Отже, згорткову нейронну мережу класифікації об’єктів групових цілей (CNN GTs) може бути застосовано для класифікації об’єктів групових цілей з різними значеннями бойових потенціалів.

Для перевірки роботи CNN GTs було взято довільний набір об’єктів групових цілей зі значеннями бойових потенціалів, які наведено у табл. 3.

Результати роботи CNN GTs представлено у четвертому рядку табл. 3.

Таблиця 3 – Результати роботи CNN GTs

№ з/п	Об’єкти групових цілей	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	Бойовий потенціал	91.74	50.15	35.46	27.85	25.98	23.00	20.15	18.50	17.43	17.00	16.50	16.00	16.00	14.14	14.00	2.93
2	Клас (фактичний)	5	4	4	4	4	4	3	3	3	3	3	3	3	3	3	2
3	Клас (нейронна мережа)	5	4	4	4	4	4	3	3	3	3	3	3	3	3	3	2
4	Збіг	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
№ з/п	Об’єкти групових цілей	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	Бойовий потенціал	2.90	2.89	2.88	2.86	2.86	2.74	2.73	2.70	2.58	2.57	2.47	2.46	2.45	2.37	2.30	2.30
2	Клас (фактичний)	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1
3	Клас (нейронна мережа)	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1
4	Збіг	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Результати аналізу фактичних даних та даних, які отримано з використанням CNN GTs, показують 100 % збіг класів об’єктів групових цілей.

Отже, згорткову нейронну мережу класифікації об’єктів групової цілі (CNN GTs) може бути застосовано для класифікації об’єктів групових цілей противника з різними значеннями бойового потенціалу.

Таким чином, у роботі продемонстровано, що для розв’язання задач кластеризації та класифікації об’єктів групових цілей противника може бути застосовано нейронні мережі.

Для розв’язання задачі кластеризації об’єктів групових цілей може бути обрано нейронну мережу типу SELFORGMAP (самоорганізовані карти), яка складається з шару нейронів і може класифікувати набір даних векторів з будь-якою розмірністю на стільки класів, скільки нейронів має шар.

NN SOM GTs підтримує топологію hextop, яка створює набір нейронів у вигляді гексагонального шаблону (тобто нейрони розташовуються у гексагональному порядку). При цьому в загальному випадку ми можемо застосувати різні топології для початкового розташування нейронів за допомогою функцій gridtop, hextop та randtop.

Кластеризація об’єктів групових цілей, які наведено у табл. 2, показала, що ці об’єкти за своїми бойовими потенціалами може бути поділено на 5 кластерів.

Визначення класу об’єктів групових цілей дає можливість точно визначити, яким типом ударного БпЛА та з якою масою бойової частини доцільно уражати групові цілі противника.

Навчання CNN GTs здійснювалось за допомогою алгоритму Левенберга – Марквардта на наборі даних, який наведено у табл. 1. Критерієм оптимізації є середньоквадратична

похибка моделі на навчальній вибірці. Алгоритм полягає в послідовному наближенні заданих початкових значень параметрів до шуканого локального оптимуму.

За результатами навчання нейронну мережу класифікації об'єктів групових цілей було навчено, перевірено і протестовано з точностями 100% і загальною точністю нейронної мережі класифікації об'єктів групових цілей 100%.

При цьому результати аналізу гістограми похибок між цільовими значеннями та прогнозованими значеннями після навчання нейронної мережі класифікації об'єктів групових цілей свідчать про те, що значення похибки становить 0,00022. Оскільки похибки близькі до нуля, то навчена нейронна мережа здійснює класифікацію об'єктів групових цілей добре.

Перевірка роботи CNN GTs на довільному наборі об'єктів групових цілей (табл. 3) показала 100% збіг класів фактичних об'єктів групових цілей та даних, які отримано з використанням CNN GTs.

Висновки

Для класифікації об'єктів групових цілей противника може бути обрано згорткову нейронну мережу типу CNN GTs. Навчання CNN GTs за допомогою алгоритму Левенберга – Марквардта показало гарні результати. За результатами навчання нейронну мережу класифікації об'єктів групової цілі було навчено, перевірено і протестовано з точностями 100%, а загальна точність нейронної мережі класифікації об'єктів групових цілей становила 100%. Результати аналізу гістограми похибок між цільовими значеннями та прогнозованими значеннями після навчання нейронної мережі класифікації об'єктів групових цілей свідчать про те, що значення похибки становить 0,00022. Оскільки похибки близькі до нуля, то навчена нейронна мережа здійснює класифікацію об'єктів групових цілей добре. Перевірка роботи CNN GTs на довільному наборі об'єктів групових цілей показала 100% збіг класів фактичних об'єктів групових цілей, які отримано з використанням CNN GTs.

Напрямом подальшого дослідження може бути створення нейронних мереж для розв'язання задачі розподілу неоднорідного рою ударних безпілотних літальних апаратів по об'єктах нестаціонарної неоднорідної групової цілі. Матеріали статті можуть бути корисними для наукових та науково-педагогічних працівників у галузі математичного моделювання складних систем воєнного призначення, а також для здобувачів вищої освіти (курсантів, студентів, слухачів та ад'юнктів), які вивчають зазначені питання.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Шовкошитний І.І., Василенко О.А. Розроблення логіко-часової моделі ройового застосування ударних безпілотних літальних апаратів з урахуванням типових способів їх групового застосування в сучасних умовах // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України. 2024. № 3 (83). С. 108–116.
2. Нікітіна Л. О., Нікітін С. О. Моделі та методи штучного інтелекту у комп'ютерних іграх. Харків: «Друкарня Мадрид», 2018. 102 с.
3. Методи та системи штучного інтелекту: навч. пос. / Укл. Д. В. Лубко, С. В. Шаров. Мелітополь: ФОП Однорог Т. В., 2019. 264 с.
4. Штучний інтелект і нейромережі. 12 книжок в одній, що допоможуть Вам втілити інновації в життя. Харків: ТОВ «Моноліт Бізз», 2024. 216 с.

5. Іващенко А. Інформаційне та програмне забезпечення системи ідентифікації безпілотних літальних апаратів. Кваліф. робота бакалавра. Суми: Сумський держ. ун-т, 2022. URL : https://essuir.sumdu.edu.ua/bitstream-download/123456789/88897/1/Ivashchenko_bac_rob.pdf
6. Оганезов А. Л. Применение нейронных сетей в задачах распознавания образов. Автореф. дисс. … канд. физ.-мат. наук: 05.13.11. Тбилиси. 2006. 20 с.
7. Перепеліцин С. О. Система захисту від загроз удару БпЛА із використанням блоків нейромережевого аналізу. Наукоємні технології. 2020. № 1 (45). https://doi.org/10.18372/2310-5461.45.14579.
8. Гусак Ю. А., Василенко О. А. Кластеризація та класифікація ударних безпілотних літальних апаратів на основі нейронних мереж. Повітряна міць України. 2024. № 1 (6). С. 141–152. https://doi.org/10.33099/2786-7714-2024-1-6-141-152.
9. Гусак Ю. А., Василенко О. А. Алгоритм створення нейронної мережі класифікації ударних безпілотних літальних апаратів. Сучасні інформаційні технології у сфері безпеки та оборони. 2024. № 2 (50). С. 54–68. https://doi.org/10.33099/2311-7249/2024-50-2-54-68.
10. Бережний А. О. Методи та інформаційна технологія автоматизованого планування маршрутів польотів безпілотних літальних апаратів для підвищення ефективності пошуку об’єктів. Дис. … канд. техн. наук. 05.13.06. Харків: ХНУПС, 2020.
11. Довідник з MATLAB: електронний навч. пос. з курсового і дипломного проектування. Київ: НТУУ «КПІ», 2013. 132 с.
12. Терейковський І. А., Бушуєв Д. А., Терейковська Л. О. Штучні нейронні мережі: базові положення. Київ: НТУУ «КПІ», 2022. 123 с.

References

1. Shovkoshytnyi I.I., Vasylenko O.A. Rozroblennia lohiko-chasovoi modeli roiovoho zastosuvannia udarnykh bezpilotnykh litalnykh aparativ z urakhuvanniam typovykh sposobiv yikh hrupovoho zastosuvannia v suchasnykh umovakh. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy*. 2024. № 3 (83). S. 108–116.
2. Nikitina L. O., Nikitin S. O. Modeli ta metody shtuchnoho intelektu u kompiuternykh ihrakh. Xarkiv: «Drukarnia Madryd», 2018. 102 s.
3. Metody ta systemy shtuchnoho intelektu: navch. pos. / Ukl. D. V. Lubko, S. V. Sharov. Melitopol: FOP Odnoroh T. V., 2019. 264 s.
4. Shtuchnyi intelekt i neiromerezhi. 12 knyzhok v odnii, shcho dopomozhut Vam vtilyty innovatsii v zhyttia. Kharkiv: TOV «Monolit Bizz», 2024. 216 s.
5. Ivashchenko A. Informatsiine ta prohramne zabezpechennia systemy identyfikatsii bezpilotnykh litalnykh aparativ. Kvalif. robota bakalavra. Sumy: Sumskyi derzh. un-t, 2022. Available from : https://essuir.sumdu.edu.ua/bitstream-download/123456789/88897/1/Ivashchenko_bac_rob.pdf
6. Ohanezov A. L. Prymenenye neironnыkh setei v zadachakh raspoznavanyia obrazov. Avtoref. dyss. … kand. fyz.-mat. nauk: 05.13.11. Tbylysy. 2006. 20 s.
7. Perepelitsyn S. O. Systema zakhystu vid zahroz udaru BpLA iz vykorystanniam blokiv neiromerezhevoho analizu. *Naukoiemni tekhnolohii*. 2020. № 1 (45). https://doi.org/10.18372/2310-5461.45.14579.
8. Husak Yu. A., Vasylenko O. A. Klasteryzatsiia ta klasyfikatsiia udarnykh bezpilotnykh litalnykh aparativ na osnovi neironnykh merezh // Povitriana mits Ukrainy. 2024. № 1 (6). S. 141–152. https://doi.org/10.33099/2786-7714-2024-1-6-141-152.
9. Husak Yu. A., Vasylenko O. A. Alhorytm stvorennia neironnoi merezhi klasyfikatsii udarnykh bezpilotnykh litalnykh aparativ. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony. 2024. № 2 (50). S. 54–68. https://doi.org/10.33099/2311-7249/2024-50-2-54-68.

10. Berezhnyi A. O. Metody ta informatsiina tekhnolohiia avtomatyzovanoho planuvannia marshrutiv polotiv bezpilotnykh litalnykh aparativ dlia pidvyshchennia efektyvnosti poshuku obiektiv. Dys. … kand. tekhn. nauk. 05.13.06. Kharkiv: KhNUPS, 2020.
11. Dovidnyk z MATLAB: elektronnyi navch. pos. z kursovoho i dyplomnoho proektuvannia. Kyiv: NTUU «KPI», 2013. 132 c.
12. Tereikovskyi I. A., Bushuiev D. A., Tereikovska L. O. Shtuchni neironni merezhi: bazovi polozhennia. Kyiv: NTUU «KPI», 2022. 123 s.

Аналіз методів проведення аудиту безпеки хмарного середовища відповідно до міжнародних стандартів

Analysis of Methods for Conducting Cloud Security Audits According to International Standards

Владислав Франкевич [A]
студент кафедри Захист інформації, e-mail: vladyslav.frankevych.kb.2021@lpnu.ua, ORCID0009-0006-7888-3861

Соломія Долішня [A]
студент кафедри Захист інформації, e-mail: solomiia.dolishnia.kb.2021@lpnu.ua, ORCID: 0009-0002-2038-4374

Вікторія Савчук [A]
студент кафедри Захист інформації, e-mail: viktoriia.savchuk.kb.2021@lpnu.ua, ORCID: 0009-0003-3904-7391

Євгеній Курій [A]
асистент кафедри Захист інформації, e-mail: yevhenii.o.kurii@lpnu.ua, ORCID: 0000-0002-3423-5655

Віталій Сусукайло [A]
Corresponding author: доктор філософії, асистент кафедри Захисту інформації, e-mail: vitalii.a.susukailo@lpnu.ua, ORCID: 0000-0003-4431-9964

Vladyslav Frankevych [A]
Student of the Department Information Protection, e-mail: vladyslav.frankevych.kb.2021@lpnu.ua, ORCID0009-0006-7888-3861

Solomiia Dolishnia [A]
Student of the Department Information Protection, e-mail: solomiia.dolishnia.kb.2021@lpnu.ua, ORCID: 0009-0002-2038-4374

Viktoriia Savchuk [A]
Student of the Department Information Protection, e-mail: viktoriia.savchuk.kb.2021@lpnu.ua, ORCID: 0009-0003-3904-7391

Yevhenii Kurii [A]
Assistant of the Department, e-mail: yevhenii.o.kurii@lpnu.ua, ORCID: 0000-0002-3423-5655

Vitalii Susukailo [A]
Corresponding author: Doctor of Philosophy, Assistant of the Department, e-mail: vitalii.a.susukailo@lpnu.ua, ORCID: 0000-0003-4431-9964

[A] Національний університет "Львівська політехніка", Львів, Україна
[A] Lviv Polytechnic National University, Lviv, Ukraine

Received: April 8, 2025 | Revised: April 28, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.19

Мета роботи: Порівняння методів аудиту безпеки хмарних середовищ (ручний, автоматизований, вбудований) для визначення їх ефективності у відповідності міжнародним стандартам, зокрема, з урахуванням специфіки хмарних платформ та мінімізацією ризиків.

Метод дослідження: Емпіричне дослідження.

Результати дослідження: Автоматизовані інструменти забезпечують швидкість та економічність, однак ручний аудит, попри свою трудомісткість, забезпечує глибину аналізу нестандартних конфігурацій. Вбудовані засоби надають миттєвий огляд безпеки, але мають обмежену гнучкість, тоді як інтеграція стандартів, хоча й підвищує загальний рівень захищеності, виявляє прогалини в адаптації вимог до специфічних потреб організацій.

Теоретична цінність дослідження: Дослідження підтверджує актуальність існуючих теоретичних рамок, а саме міжнародних стандартів для оцінки безпеки, але вказує на необхідність їх адаптації до динамічних хмарних середовищ. Результати підкреслюють роль адаптивних моделей для покращення відповідності стандартам.

Практична цінність дослідження: Системні адміністратори та інженери з безпеки можуть комбінувати автоматизовані інструменти, ручний аудит та вбудовані засоби для оптимізації витрат і підвищення точності оцінки безпеки. Інтеграція машинного навчання для прогнозування ризиків і адаптації стандартів дозволить розробляти проактивні стратегії захисту хмарних середовищ, зокрема для фільтрації хибнопозитивних результатів та пріоритизації вразливостей.

Цінність дослідження: Порівняльний аналіз трьох методів з урахуванням їх взаємодії, вартості та відповідності стандартам. Надано практичні критерії для вибору стратегій безпеки за обмежених ресурсів.

Тип статті: Емпіричне дослідження з елементами теоретичного аналізу.

Purpose: Comparison of cloud security audit methods (manual, automated, embedded) to determine their effectiveness in accordance with international standards, in particular, taking into account the specifics of cloud platforms and risk minimization.

Method: The empirical study.

Findings: Automated tools provide speed and cost-effectiveness, but manual auditing, while laborious, reveals the depth of analysis of non-standard configurations. Built-in tools provide an instant security overview but have limited flexibility, while standards integration, while increasing the overall level of security, reveals gaps in adapting requirements to the specific needs of organizations.

Theoretical implications: The study confirms the relevance of existing theoretical frameworks, namely international standards for security assessment, but points to the need to adapt them to dynamic cloud environments. The results highlight the role of adaptive models in improving compliance with standards.

Practical implications: System administrators and security engineers can combine automated tools, manual auditing, and built-in tools to optimize costs and improve the accuracy of security assessments. Integrating machine learning for risk prediction and standards adaptation will allow for proactive cloud security strategies, including filtering false positives and prioritizing vulnerabilities.

Value: A comparative analysis of three methods, taking into account their interaction, cost, and compliance with standards. Practical criteria for choosing security strategies under limited resources are provided.

Paper type: Empirical research with elements of theoretical analysis.

Ключові слова: інформаційна безпека; хмарна безпека; аудит безпеки; міжнародні стандарти безпеки; автоматизований аудит.

Key words: information security; cloud security; security audit; international security standards; automated audit.

Вступ

Сучасні хмарні середовища, такі як Microsoft 365, Amazon Web Services та Google Workspace, стали основою цифрової інфраструктури для більшості організацій, що працюють у різноманітних галузях. Проте зростаючі кіберзагрози, складність конфігурацій цих платформ та вимоги до відповідності міжнародним стандартам безпеки, таким як ISO 27001, SOC 2, NIST CSF, створюють серйозні виклики для забезпечення належного рівня захищеності. У цих умовах питання безпеки стає критично важливим, адже навіть найменші вразливості можуть призвести до значних фінансових та репутаційних втрат для організацій.

Для оцінки рівня безпеки хмарних середовищ використовуються різні підходи, зокрема автоматизовані та вбудовані інструменти, які мають на меті забезпечити швидкість і ефективність аудиту. Проте такі інструменти часто стикаються з обмеженнями щодо підтримки специфічних фреймворків і вимог. Ручні методи аудиту, хоча і дають змогу здійснити глибокий аналіз нестандартних налаштувань, є трудомісткими і не завжди відповідають сучасним вимогам ефективності.

Метою даної роботи є вивчення та порівняння різних підходів до аудиту безпеки хмарних середовищ, визначення їхніх переваг і недоліків, а також оцінка їх ефективності в контексті міжнародних стандартів безпеки.

Теоретичні основи дослідження

Хмарні середовища забезпечують доступ до обчислювальних ресурсів через інтернет, що надає організаціям гнучкість, масштабованість та економічну ефективність. Вони характеризуються можливістю швидко змінювати обсяги ресурсів (масштабування вгору або вниз), автоматично адаптуватися до навантаження та надавати доступ до даних у будь-який час і з будь-якого місця. Модель оплати “pay-as-you-go” дозволяє знижувати витрати на підтримку інфраструктури, а централізоване управління спрощує контроль над ресурсами. Реплікація даних та інтеграція з різними платформами забезпечують високу доступність та адаптивність. Однак ці переваги створюють виклики для безпеки, особливо через конфігураційні помилки та несанкціонований доступ.

Хмарні сервіси класифікуються за рівнем наданих ресурсів: IaaS, PaaS та SaaS. IaaS надає базову інфраструктуру (наприклад, AWS EC2, Azure VMs), що дозволяє користувачам контролювати ресурси, але потребує технічної експертизи та відповідальності за безпеку. PaaS (Google App Engine, Heroku) спрощує розробку додатків, однак зменшує контроль над інфраструктурою. SaaS (Microsoft 365, Salesforce) надає готові програмні рішення, які не потребують установки, але обмежують можливості кастомізації.

Критичні ресурси включають дані (персональні, фінансові, конфіденційні), обчислювальні ресурси (сервери, бази даних), мережеву інфраструктуру (брандмауери, VPN) та інструменти управління (системи аутентифікації, API). Наприклад, в AWS важливими є IAM, S3-бакети та KMS, у Microsoft Azure — AAD, Blob Storage та Security Center. Компрометація цих ресурсів може призвести до фінансових збитків, порушення безперервності бізнесу або втрати довіри клієнтів.

Основні вектори атак у хмарних середовищах включають неправильну конфігурацію, таку як відкриті S3-бакети та некоректні політики доступу, а також вразливості програмного забезпечення, як-от непатчені програми чи контейнери. До того ж, фішинг та компрометація облікових записів, зокрема через брутфорс-атаки або викрадені токени, є поширеними методами доступу до систем. Атаки типу DoS/DDoS можуть призвести до недоступності сервісів, що серйозно порушує роботу організацій. Інсайдерські загрози також становлять небезпеку, коли співробітники здійснюють зловмисні дії. Серед найбільших загроз у хмарних середовищах можна виділити втрату даних, компрометацію конфіденційності, фінансові

збитки через несанкціоноване використання ресурсів та репутаційні втрати через витоки інформації.

Основні загрози в хмарних середовищах створюють серйозні виклики для організацій, які використовують такі сервіси. Неправильна конфігурація, вразливості програмного забезпечення, компрометація облікових записів, DoS/DDoS-атаки та інсайдерські загрози можуть спричинити фінансові збитки, порушення безперервності бізнесу та втрату довіри клієнтів. Успішна експлуатація цих загроз може призвести до витоку даних, несанкціонованого використання ресурсів та порушення роботи критичних сервісів. Для зменшення цих ризиків необхідно застосовувати ефективні заходи безпеки та методи управління ризиками.

Ефективність управління ризиками в хмарних середовищах безпосередньо залежить від належної реалізації контролів безпеки, зокрема рекомендацій CIS Benchmarks. Для оцінки ризиків використовується модель, яка враховує ймовірність виникнення інциденту (P) та його потенційні втрати (L). Ризик (R) визначається за формулою $R = P \cdot L$, де P — ймовірність виникнення події. L — потенційні втрати, що виникають внаслідок інциденту.

Аналіз ризикових сценаріїв допомагає виявити найбільш ймовірні загрози для безпеки в хмарі. Один із таких сценаріїв — відкритий S3 Bucket з конфіденційною інформацією. Якщо не налаштувати політику "Block public access" для S3-бакетів, це створює ризик несанкціонованого доступу до даних. За оцінками, до 30% хмарних середовищ можуть містити такі помилки, що дає ймовірність виникнення інциденту на рівні 30%. У разі компрометації може відбутися витік персональних даних клієнтів. Якщо припустити, що в системі знаходиться 10000 записів, а середня вартість одного запису згідно з даними IBM на 2023 рік складає 165 доларів (6876 грн) [1], то загальна сума потенційних втрат становитиме 68760000 грн. Враховуючи ймовірність виникнення інциденту на рівні 30%, ризик для організації буде становити 20628000 грн.

Захист інформації та забезпечення безпеки хмарних середовищ є критично важливим аспектом сучасної кібербезпеки. Міжнародні стандарти безпеки встановлюють загальні вимоги та кращі практики для захисту даних, інфраструктури та забезпечення належної безпеки хмарних сервісів.

ISO/IEC 27001 є міжнародним стандартом для систем управління інформаційною безпекою (ISMS), який визначає вимоги щодо створення, реалізації, підтримки та вдосконалення системи управління інформаційною безпекою на підприємстві. Згідно з цим стандартом, організації повинні проводити оцінку ризиків для своїх інформаційних активів і вживати відповідні заходи для їх мінімізації, а також налаштовувати системи та процеси для обмеження доступу до конфіденційної інформації [2]. Також важливим є регулярний моніторинг діяльності та проведення аудитів, щоб виявити потенційні вразливості в інформаційних системах. Стандарт передбачає наявність процедур для оперативного реагування на інциденти безпеки та встановлює вимоги до оцінки та контролю безпеки постачальників і партнерів, що мають доступ до інформаційних систем.

SOC 2 (System and Organization Controls 2) — це набір стандартів, що визначають вимоги до систем обробки даних та встановлюють критерії для перевірки безпеки, доступності, конфіденційності, цілісності обробки та конфіденційності даних. Цей стандарт є важливим для компаній, які працюють з персональними даними, особливо для хмарних провайдерів. SOC 2 оцінює, чи захищена система від несанкціонованого доступу, чи здатна вона бути доступною і готовою до використання, чи забезпечується точність та якість обробки даних, а також чи надається належний захист конфіденційної інформації, що обробляється або зберігається в системах. Крім того, особливу увагу приділяється контролю доступу до персональних і корпоративних даних, що є важливою частиною забезпечення їх безпеки та конфіденційності.

GDPR (General Data Protection Regulation) є законодавчим актом Європейського Союзу, який регулює обробку персональних даних і є обов’язковим для організацій, що обробляють

дані громадян ЄС, незалежно від їхнього місцезнаходження [3]. Однією з основних вимог для хмарних середовищ є забезпечення прозорості та контролю, що означає право користувачів знати, які дані збираються та як вони обробляються. Крім того, організації повинні отримати явну згоду користувачів перед обробкою їх персональних даних, надавши їм право на доступ до своїх даних та можливість вимагати їх виправлення. Окрім цього, хмарні сервіси зобов'язані забезпечити належний рівень безпеки обробки персональних даних, а також негайно, протягом 72 годин, повідомляти про будь-які порушення безпеки даних.

NIST CSF (Cybersecurity Framework) — це набір керівних принципів, розроблений Національним інститутом стандартів і технологій США для покращення кібербезпеки в організаціях. Він визначає вимоги, що забезпечують захист хмарних середовищ через три основні функції: ідентифікацію ризиків, захист систем та даних, а також виявлення потенційних загроз. Це включає в себе оцінку ризиків, встановлення засобів для захисту інфраструктури та постійний моніторинг на наявність загроз. Крім того, NIST CSF передбачає розробку планів реагування на інциденти безпеки та відновлення систем після можливих кіберінцидентів.

CIS Controls v8 — це набір з 18 контролів, що визначають найкращі практики для забезпечення кібербезпеки організацій [4]. Вони спрямовані на правильний захист хмарних середовищ, включаючи ідентифікацію та управління активами, що включає визначення всіх пристроїв, програм і даних, що зберігаються в хмарі, управління вразливостями через регулярне сканування та патчинг, а також захист даних за допомогою шифрування на етапах зберігання і передачі. Окрім того, важливим є управління доступом із застосуванням принципу найменших привілеїв і багатоетапної автентифікації для контролю доступу, а також моніторинг та реагування на інциденти, що включає виявлення аномалій і негайну реакцію на інциденти безпеки.

Використання бенчмарків та фреймворків для підвищення безпеки хмарних середовищ є важливим кроком для забезпечення конфіденційності, цілісності та доступності даних. Ці стандарти надають рекомендації з налаштувань конфігурацій, які допомагають захистити хмарні інфраструктури від різноманітних кіберзагроз. Вони включають практичні керівництва, які розроблені з урахуванням найкращих практик в індустрії, та допомагають організаціям забезпечити належний рівень безпеки для своїх хмарних середовищ.

CIS Benchmarks (Center for Internet Security Benchmarks) — це набір рекомендованих конфігурацій для більш ніж 25 продуктів різних постачальників [5]. Вони розроблені експертами з кібербезпеки по всьому світу з метою забезпечення кращого захисту від загроз та вразливостей для інформаційних систем. CIS Benchmarks складаються з конкретних рекомендацій щодо налаштування безпеки, які можуть бути застосовані для широкого спектра хмарних платформ та інших технологій.

До хмарних постачальників, для яких існують CIS Benchmarks, належать Alibaba Cloud, Amazon Web Services (AWS), Google Cloud Computing Platform (GCP), Google Workspace, IBM Cloud Foundations, Microsoft 365, Microsoft Azure, Microsoft Dynamics 365 Power Platform, Oracle Cloud Infrastructure.

CIS Benchmarks забезпечують організації конкретними кроками для посилення безпеки їхніх хмарних середовищ, включаючи налаштування доступу, шифрування даних, моніторинг безпеки та методи реагування на інциденти. Використання CIS Benchmarks дозволяє мінімізувати ризики внаслідок людських помилок або невідповідності стандартам безпеки.

CISA — це агентство Міністерства внутрішньої безпеки США, яке відповідає за забезпечення кібербезпеки та захист критичної інфраструктури [6]. CISA керує національними програмами з кібербезпеки та надає ресурси для організацій, що працюють із критично важливою інформацією, зокрема в хмарних середовищах [7]. Одним із важливих проектів агентства є Secure Cloud Business Applications (SCuBA).

Проект SCuBA надає рекомендації та інструменти для захисту хмарних бізнес-додатків і забезпечує захист федеральних даних, що зберігаються в хмарі [8]. SCuBA фокусується на забезпеченні безпеки для інформаційних активів у хмарних середовищах через стандартизовані, сучасні та керовані конфігурації безпеки. Це дозволяє ефективно налаштовувати безпеку хмарних додатків і забезпечити конфіденційність даних.

SCuBA включає важливі фреймворки для забезпечення безпеки в хмарних середовищах, такі як Microsoft 365 (M365) і Google Workspace (GWS). Для обох платформ існують спеціалізовані Secure Configuration Baselines, що надають прості та зрозумілі рекомендації для налаштування безпеки. Ці базові конфігурації сприяють підвищенню безпеки хмарних сервісів, узгоджуючи налаштування з унікальними вимогами і рівнями ризику кожної організації.

Бенчмарки та фреймворки, такі як CIS Benchmarks та CISA спеціалізовані базові конфігурації безпеки, є важливими інструментами для підвищення безпеки хмарних середовищ. Вони надають чіткі, погоджені рекомендації для налаштування хмарних систем і допомагають організаціям захистити свої дані від потенційних загроз. Інтеграція цих стандартів у практики забезпечення безпеки допомагає підвищити рівень захисту та зменшити ймовірність виникнення інцидентів безпеки.

Ручне проведення аудиту безпеки хмарного середовища полягає в аудиті конфігураційних налаштувань сервісів, що працюють у хмарі, з метою перевірки їх відповідності стандартам безпеки, таким як CIS Benchmarks, CISA Baselines чи іншим рекомендаціям щодо підвищення безпеки. На початковому етапі необхідно визначити хмарне середовище та відповідні сервіси, які підлягають перевірці, а також встановити стандарти для перевірки, які будуть використовуватись для оцінки безпеки.

Далі аудитор безпосередньо входить у консоль керування хмарним середовищем і перевіряє налаштування різних сервісів. Він аналізує налаштування доступу, конфігурації безпеки, параметри логів та моніторингу, налаштування резервного копіювання і відновлення даних, а також політики безпеки для інтегрованих програм і сервісів. Після цього результати перевірки порівнюються з вимогами стандартів, що дозволяє оцінити відповідність налаштувань хмарних сервісів встановленим критеріям безпеки і виявити потенційні вразливості.

Проведення аудиту супроводжується складанням детального звіту, в якому фіксуються всі виявлені невідповідності стандартам безпеки. У звіті надається перелік знайдених проблем, оцінка ризиків для організації та рекомендації щодо виправлення недоліків, при цьому зазначаються конкретні вимоги фреймворків або бенчмарків, які не виконуються.

Ручне проведення аудиту має значні переваги, серед яких можливість глибокого аналізу конкретних аспектів налаштувань, що можуть бути пропущені автоматизованими інструментами. Аудитор може перевірити нестандартні конфігурації, детально проаналізувати кожне налаштування та виявити навіть найменші порушення, що дозволяє забезпечити більш високу точність перевірки. Також ручне проведення аудиту дозволяє охопити більший обсяг аспектів безпеки, ніж це може зробити автоматизована перевірка, оскільки аудитор має змогу врахувати додаткові моменти, які не входять до базових вимог стандартних фреймворків.

Однак цей метод має і недоліки. Проведення аудиту вручну потребує значно більше часу порівняно з автоматизованими рішеннями, особливо в умовах великих або складних хмарних інфраструктур. Також існує ризик помилок через людський фактор, коли аудитор може пропустити важливі налаштування або неправильно їх інтерпретувати. Цей підхід не завжди ефективний для масштабних проектів, оскільки перевірка великої кількості ресурсів може призвести до значного ускладнення процесу і збільшення вартості робіт. Крім того, складання звіту вручну є трудомістким етапом, що підвищує ризик помилок та пропусків.

Ручне проведення аудиту залежить від досвіду аудитора, тому відсутність кваліфікованих спеціалістів може знизити якість перевірки і уповільнити весь процес.

Автоматизовані засоби проведення аудиту безпеки хмарних середовищ, зокрема скрипти та інструменти, як-от Prowler, дозволяють значно підвищити ефективність процесу. Вони охоплюють різноманітні стандарти, фреймворки та бенчмарки, що зменшує час проведення аудиту та забезпечує більш об'єктивну оцінку стану безпеки. Prowler є потужним відкритим інструментом для оцінки безпеки, який підтримує хмарні платформи, такі як AWS, Azure, GCP та Kubernetes, і дозволяє здійснювати безперервний моніторинг, оцінки безпеки, аудити, відповіді на інциденти, забезпечення відповідності стандартам, зміцнення захисту та готовність до проведення судово-розслідувальних заходів [9].

Інструмент охоплює понад 500 перевірок для різних хмарних платформ, включаючи стандарти CIS, NIST 800, FedRAMP, PCI-DSS, GDPR, SOC2 та інші. Завдяки автоматизації процесу, Prowler дозволяє значно зменшити час, необхідний для оцінки конфігурацій, а також знижує ризики, пов'язані з людським фактором. Детальні звіти, що генеруються інструментом, дозволяють оперативно оцінити відповідність хмарного середовища вимогам безпеки, а також отримувати історичні дані для аналізу тенденцій у безпеці (рис. 1).

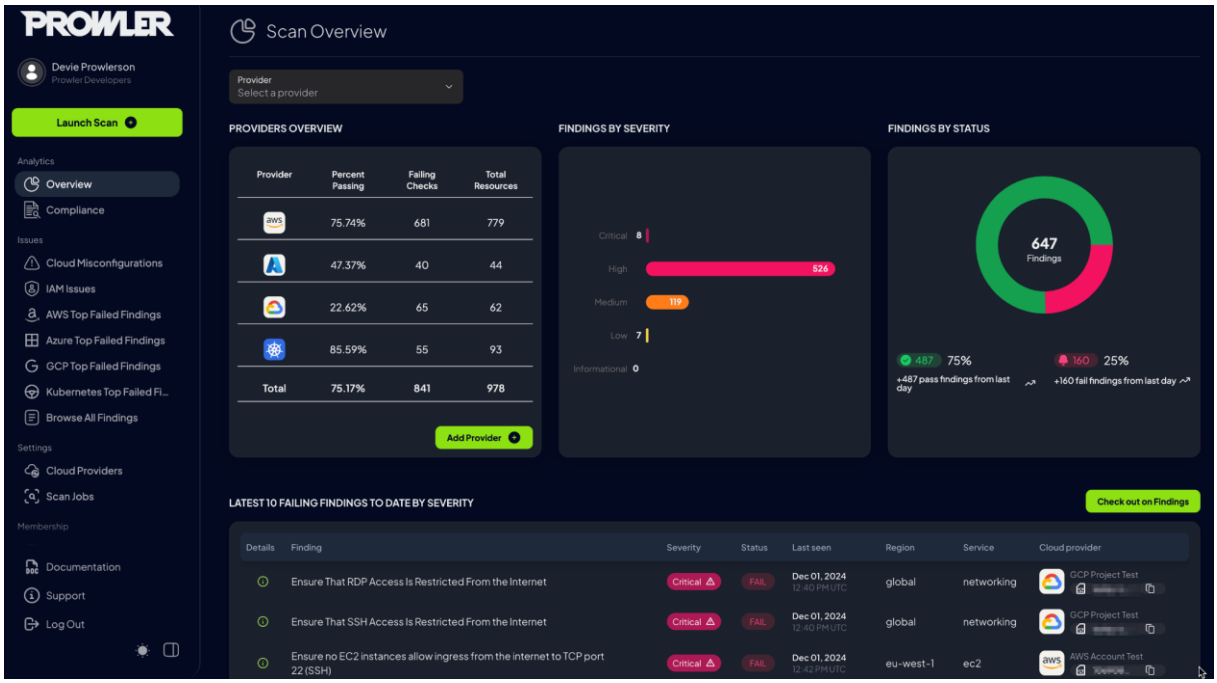


Рисунок 1 – Інтерфейс веб-додатку Prowler
Джерело: https://docs.prowler.com/projects/prowler-open-source/en/latest/

Автоматизація проведення аудиту значно скорочує час перевірки безпеки, оскільки інструмент здатний здійснювати перевірки в кілька разів швидше за ручний метод, що дозволяє оперативно виявляти вразливості та недоліки. Генеровані звіти, які базуються на заданих стандартах та фреймворках, дають змогу отримати чітку та зрозумілу оцінку стану безпеки, а також порівнювати результати з попередніми перевірками для відслідковування змін. Підтримка численних фреймворків та стандартів дозволяє проводити оцінку відповідності хмарних середовищ міжнародним вимогам, а інтеграція з різноманітними системами аналітики забезпечує глибокий аналіз стану безпеки, надаючи детальну інформацію про потенційні загрози, тренди та патерни.

Незважаючи на переваги, Prowler має свої обмеження. Не всі хмарні провайдери можуть бути повністю охоплені необхідними перевірками, що стає проблемою для менш

популярних платформ або специфічних стандартів [10]. Налаштування інструменту на власній інфраструктурі може бути трудомістким процесом для користувачів без відповідного досвіду, а також оцінка конфігурацій без врахування специфіки конкретних даних чи критичності ресурсів може призводити до недооцінки деяких проблем. Крім того, можливості кастомізації звітів зазвичай обмежені у порівнянні з ручними звітами, які дозволяють створити більш індивідуалізовану інформацію з урахуванням конкретних вимог організації.

ScubaGear є інструментом для оцінки безпеки, частиною проекту SCuBA, розробленого Агентством з кібербезпеки та інфраструктурної безпеки США (CISA). Він призначений для перевірки конфігурацій Microsoft 365 на відповідність політикам безпеки, описаним у документах Microsoft 365 Secure Configuration Baselines, що дозволяє адміністраторам перевіряти свої середовища для забезпечення захисту інформації, що створюється, зберігається та передається через хмарні бізнес-застосунки. ScubaGear працює за трьома етапами (рис. 2): спочатку здійснюється запит через PowerShell до API Microsoft 365 для отримання налаштувань, потім ці налаштування порівнюються з політиками безпеки за допомогою Open Policy Agent, а в кінцевому результаті формується звіт про результати порівняння, який може бути наданий у форматах HTML, JSON або CSV.

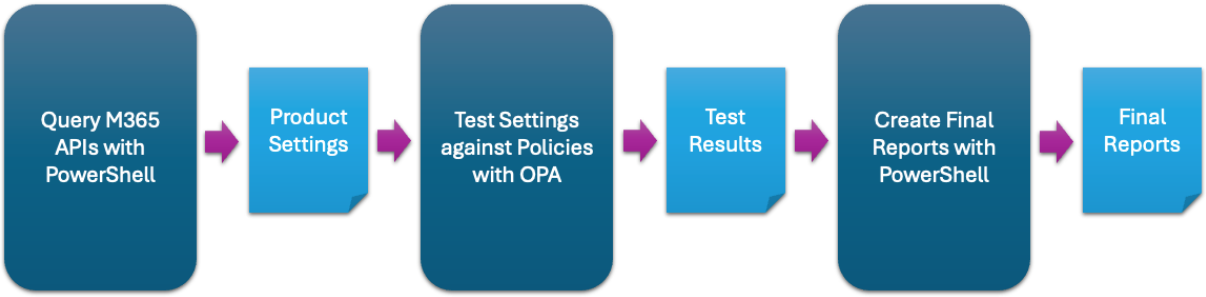


Рисунок 2 – Етапи роботи ScubaGear
Джерело: https://github.com/cisagov/ScubaGear

Інструмент може працювати як в інтерактивному режимі, коли через термінал відкривається веб-вікно для надання доступу до акаунту Microsoft, так і в безінтерактивному режимі, коли налаштовується службовий принципал з відповідними дозволами. Налаштування для безінтерактивного запуску включає створення службового принципала, формування сертифіката та його зв'язування з принципалом. Використання ScubaGear дозволяє автоматизувати перевірки конфігурацій Microsoft 365, що знижує навантаження на адміністраторів і прискорює процес перевірки, хоча налаштування службового принципала може бути складним для пересічного користувача. Інструмент орієнтований виключно на Microsoft 365, що обмежує його застосування в інших хмарних середовищах, а можливості кастомізації перевірок і звітів залишаються обмеженими, особливо при тестуванні нестандартних налаштувань або застосуванні специфічних внутрішніх політик безпеки.

ScubaGoggles є інструментом для оцінки безпеки, розробленим у рамках проекту SCuBA агентством CISA, і призначеним для перевірки конфігурацій Google Workspace на відповідність політикам безпеки, описаним у документах SCuBA Secure Configuration Baseline. Як аналог для Google Workspace, цей інструмент допомагає адміністраторам перевірити налаштування своїх середовищ для забезпечення захисту інформації, яка створюється, зберігається та передається через хмарні бізнес-застосунки Google. ScubaGoggles використовує трьохетапний процес: спочатку здійснюється експорт налаштувань за допомогою Google Admin SDK API, дані серіалізуються у формат JSON і доповнюються метаданими організації, після чого отримані налаштування порівнюються з вимогами, прописаними в SCuBA Secure Configuration Baseline за допомогою OPA Rego, і нарешті формується звіт у форматах HTML та JSON [11]. Основна

частина перевірок залежить від журналів адміністратора Google Workspace, тому при відсутності певного журналу інструмент повідомляє про необхідність вручну перевірити відповідну конфігурацію.

Для роботи ScubaGoggles необхідно завантажити інструмент та встановити залежності, включаючи Python та OPA Executable, а також налаштувати методи аутентифікації, такі як OAuth або службовий обліковий запис для автоматизованих процесів, і використати конфігураційний файл для визначення параметрів аудиту. Використання цього інструменту дозволяє автоматизувати перевірку конфігурацій Google Workspace відповідно до актуальних стандартів, що значно прискорює процес порівняння і забезпечує консистентність перевірок, а зручна генерація звітів у форматах HTML та JSON дозволяє легко інтегрувати результати в існуючі процеси безпеки компанії. Проте ScubaGoggles перебуває на стадії альфа-версії, тому існує ризик виникнення помилок або некоректних результатів перевірок, а також можливе обмеження перевірки деяких політик через відсутність відповідних журналів у Google Workspace. Обмежена можливість кастомізації перевірок та необхідність налаштування сертифікатів і прав доступу до акаунтів може ускладнити використання інструменту для адміністраторів без належного досвіду.

Amazon Web Services (AWS) пропонує потужні вбудовані інструменти для забезпечення безпеки в хмарному середовищі, серед яких IAM Trusted Advisor, IAM Access Analyzer та AWS Security Hub. Ці засоби автоматизують процеси проведення аудиту та моніторингу безпеки, дозволяючи організаціям швидко виявляти вразливості та відповідати на них [12]. AWS Security Hub виступає як центр управління безпекою, що дозволяє автоматизувати перевірку безпеки, отримувати попередження про потенційні загрози та порушення, а також отримувати огляд загального стану безпеки для всіх акаунтів AWS. Він централізує перевірки та попередження безпеки від різних сервісів AWS і підтримуваних сторонніх продуктів, що спрощує процес моніторингу та реагування. Крім того, завдяки інтеграції з іншими сервісами, такими як EventBridge та AWS Config, Security Hub може автоматично оновлювати статуси виявлених проблем, дозволяючи організаціям ефективно керувати ризиками. Водночас, використання цього інструменту пов’язане з певними витратами, оскільки оплата визначається за кількістю перевірок, подій та автоматизованих правил, а для ефективної роботи потрібно забезпечити належну інтеграцію з іншими сервісами AWS [13].

AWS Trusted Advisor допомагає оптимізувати інфраструктуру, знижувати витрати та покращувати безпеку шляхом надання рекомендацій щодо покращення конфігурацій ресурсів. Він виявляє потенційні вразливості, зокрема неправильні налаштування доступу або надмірно широкі дозволи, а також пропонує рекомендації щодо оптимізації витрат за рахунок видалення неактивних ресурсів. Проте повний доступ до всіх його функцій можливий лише з підпискою на Business або Enterprise Support, що може стати додатковим фінансовим навантаженням.

AWS IAM Access Analyzer спрямований на моніторинг та аналіз доступу до ресурсів AWS, допомагаючи визначити, хто має доступ до критичних даних і чи не надано надмірних дозволів зовнішнім користувачам. Цей інструмент аналізує політики доступу і забезпечує автоматичне сповіщення про будь-які зміни, що є важливим для оперативного реагування на потенційні загрози. Однак для отримання повної інформації про доступ може знадобитися додаткове налаштування або інтеграція з іншими сервісами, такими як AWS CloudTrail, що може ускладнити процес.

Microsoft 365 також пропонує потужні інструменти для аудиту безпеки, серед яких Microsoft Secure Score та Microsoft Purview Compliance Manager. Microsoft Secure Score дозволяє організаціям оцінити рівень їхньої безпеки шляхом вимірювання виконання рекомендованих заходів, що відображається у вигляді числового показника, який порівнюється із середніми значеннями для подібних організацій. Цей інструмент дає

можливість аналізувати поточний стан безпеки, відстежувати виконання ключових показників ефективності та визначати напрямки для покращення [14]. Microsoft Purview Compliance Manager, у свою чергу, допомагає організаціям автоматично оцінювати відповідність вимогам стандартів та регламентів, пропонуючи детальні кроки для покращення відповідності та зниження ризиків, пов'язаних із захистом даних. Разом ці інструменти створюють комплексну систему для управління безпекою та відповідністю у середовищі Microsoft 365 [15].

Google Workspace надає адміністраторам можливість моніторити та налаштовувати параметри захисту через спеціально розроблений розділ Security Health, доступний в консолі адміністратора. Цей інструмент забезпечує зручний огляд налаштувань безпеки організації, дозволяючи відстежувати стан двофакторної аутентифікації, управління доступом до Google Drive, безпечну обробку електронної пошти та керування мобільними пристроями. Сторінка безпеки дає змогу визначати конфігурації, які можуть становити ризик, і отримувати рекомендації для їх усунення, враховуючи як потреби безпеки, так і специфіку роботи організації. Адміністратори можуть моніторити налаштування в розрізі організаційних підрозділів, змінювати параметри для дочірніх одиниць та враховувати особливості тарифних планів, що впливають на функціонал інструмента. Цей підхід дозволяє забезпечити безперебійну та безпечну роботу організації в умовах постійно змінюваних викликів у кіберпросторі.

Постановка проблеми

Основною проблемою, розглянутою в цій статті, є відсутність універсальних методів аудиту, які поєднують швидкість, глибину аналізу та постійний моніторинг, відповідаючи вимогам міжнародних стандартів. Автоматизовані інструменти здатні швидко виявляти вразливості, але не здатні адаптуватися до нестандартних налаштувань систем. З іншого боку, ручний аудит є надзвичайно трудомістким і дорогим.

У таких умовах виникає необхідність у розробці системного підходу, який враховує ці обмеження і дозволяє забезпечити ефективний аудит. Ігнорування цієї проблеми може призвести до значних труднощів у підтримці безпеки та стабільності інформаційних систем, особливо в умовах постійного зростання кіберзагроз і складності технологічних середовищ.

Попри важливість цієї теми, в науковій літературі спостерігається недостатня увага до створення інтегрованих методів аудиту, які можуть задовольнити сучасні вимоги до швидкості, точності та адаптивності. Рішення цієї проблеми потребує комплексного підходу, що дозволить забезпечити ефективний моніторинг та виявлення вразливостей в умовах постійно змінюваних технологічних умов.

Методологія дослідження

У цьому дослідженні було обрано хмарне середовище Microsoft 365 як об'єкт аудиту безпеки через його популярність, широке використання в корпоративних середовищах і наявність базових інструментів управління безпекою, що дозволяють аналізувати й оцінювати рівень захисту даних. Дослідження проводилось на тестовому обліковому записі з безкоштовним пробним періодом, при якому створено мінімалістичне середовище, що імітує роботу невеликої організації, з мінімально необхідними ресурсами. У цьому середовищі реалізовано два типи користувачів: адміністратор із повним доступом для управління ресурсами та звичайний користувач із обмеженим доступом до корпоративних даних у OneDrive і поштових скриньках Exchange Online. Усі файли в OneDrive за замовчуванням є приватними, а для адміністратора ввімкнено багатофакторну автентифікацію (MFA). Така конфігурація дозволяє знизити складність дослідження, зберігаючи можливість детального аналізу налаштувань безпеки.

Критеріями оцінки безпеки було встановлено виявлення вразливостей у конфігурації хмарного середовища, оцінка ефективності наявних заходів безпеки та перевірка відповідності налаштувань загальноприйнятим рекомендаціям, таким як CIS Benchmarks. До основних показників належить аналіз налаштувань доступу до сховищ OneDrive та сайтів SharePoint, перевірка правильного розмежування прав доступу до публічних і приватних ресурсів, оцінка впровадження багатофакторної автентифікації, аналіз політик щодо паролів, моніторинг журналювання змін конфігурацій і доступу до об'єктів, порівняння конфігурації середовища з рекомендованими стандартами та виявлення слабких місць, що дозволяє оцінити потенційні ризики.

Ручне проведення аудиту налаштувань безпеки Microsoft 365 виконувалось за методикою, що базується на CIS Microsoft 365 Foundations Benchmark v3.1.0. Для автоматизованої оцінки стану безпеки та відповідності середовища Microsoft 365 було використано вбудоване рішення Compliance Manager з платформи Microsoft Purview. Для автоматизованого проведення аудиту також було використано сторонній сервіс ScubaGear, доступний з офіційного репозиторію GitHub [16]. Цей інструмент, що є частиною проекту SCuBA, розробленого Агентством з кібербезпеки та інфраструктурної безпеки США (CISA), перевіряє конфігурації Microsoft 365 на відповідність політикам безпеки, визначеним у Microsoft 365 Secure Configuration Baselines.

Результати

Дослідження показало, що безпека хмарних середовищ може перевірятися трьома підходами: ручним, автоматизованим та за допомогою вбудованих засобів. Для ручного проведення аудиту, що базується на стандартах CIS Benchmarks і CISA Baselines, середній час однієї перевірки складає 5 хвилин, що призводить до значних витрат часу при збільшенні кількості контролів. Автоматизовані засоби, такі як Prowler, ScubaGear та ScubaGoggles, дозволяють виконувати одну перевірку за 3 секунди, що суттєво скорочує загальний час аудиту навіть при великій кількості перевірок. Вбудовані засоби, як AWS Trusted Advisor, Security Hub, IAM Access Analyzer або Purview Manager, забезпечують збір даних у режимі реального часу, що дозволяє отримувати результати практично миттєво. Це порівняння підсумовано в табл. 1.

Таблиця 1 – Порівняння підходів проведення аудиту безпеки хмарних середовищ

Метод проведення аудиту	Засоби	Швидкість перевірки	Ресурси, необхідні для виконання	Ефективність у масштабах великої системи
Ручний	Немає	5 хвилин для кожної перевірки	Висока залежність від кваліфікації та досвіду аналітика	Низька, оскільки потребує набагато більше ресурсів
Автоматизований	Prowler, ScubaGear, ScubaGoggles	3 секунди на одну перевірку	Необхідне налаштування інструментів, регулярне оновлення	Висока, оскільки може обробляти сотні перевірок за лічені хвилини
Вбудований	AWS Trusted Advisor, Security Hub, IAM Access Analyzer, Purview Manager	0 секунд, оскільки дані завжди доступні, збираються в реальному часі	Мінімальні: інтегровано в хмарне середовище; доступ через консоль або API	Максимальна, оскільки повністю інтегроване рішення

Розглянемо середню кількість перевірок для організації, що складається з 100 контролів, і порівняємо ефективність їх виконання (рис. 3). Ручний метод займає найбільше часу, досягаючи 500 хвилин, що значно перевищує час, витрачений на автоматизовані та

вбудовані рішення, особливо при збільшенні кількості перевірок. Автоматизований підхід дозволяє значно скоротити час виконання до 5 хвилин, що робить його швидким навіть для великої кількості перевірок, хоча вимагає певної підготовки. Вбудоване рішення є найефективнішим, оскільки надає дані миттєво без додаткового часу на виконання та працює в режимі реального часу, не потребуючи ручного запуску.

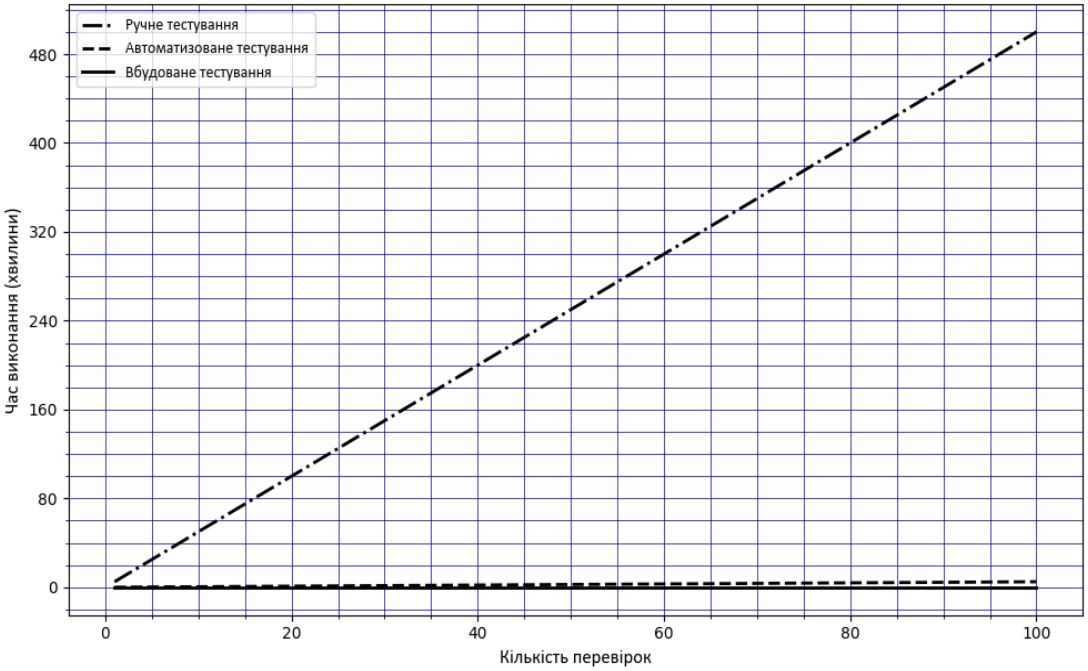


Рисунок 3 – Графік залежності часу від кількості перевірок

Ручний підхід забезпечує найвищий рівень деталізації завдяки можливості фахівця адаптувати перевірки, змінювати критичність контролів та враховувати специфіку організації, що дозволяє виявити навіть найменші невідповідності. Проте цей метод є трудомістким і залежить від кваліфікації спеціаліста. Автоматизовані засоби забезпечують стандартизовані звіти, які є корисними для загальної оцінки безпеки, але мають обмежені можливості для кастомізації, що може знижувати релевантність результатів для унікальних сценаріїв. Вбудовані засоби, такі як дашборди Microsoft Secure Score або AWS Security Hub, надають візуальне представлення стану безпеки в режимі реального часу, проте деталізація їхніх звітів є нижчою, що обмежує можливості для глибокого аналізу.

Вартість реалізації проведення аудиту безпеки в хмарних середовищах залежить від обраного методу: ручного, автоматизованого або вбудованого. Кожен підхід має свої особливості, які впливають на витрати, як прямі (витрати на інструменти та ресурси), так і непрямі (витрати на час співробітників, використання інфраструктури тощо). Ручне проведення аудиту є безкоштовним з точки зору використання інструментів, але має значні непрямі витрати, пов’язані з оплатою праці спеціалістів. Для розрахунку непрямих витрат враховується середня заробітна плата спеціаліста з інформаційної безпеки в Україні на березень 2025 року, яка становить 40000 грн на місяць при 8-годинному робочому дні та 20 робочих днях [17]. Це дає погодинну ставку 250 грн.

Для виконання 100 перевірок безпеки вручну потрібно витратити 5 хвилин на кожну перевірку та 3 години на створення звіту. Таким чином, витрати на виконання перевірок становлять 2083,33 грн, а створення звіту коштує 750 грн. Загальні витрати складають 2833,33 грн. Ручне проведення аудиту підходить для невеликих середовищ або ситуацій, коли потрібно провести глибокий аналіз складних аспектів безпеки, але цей метод є трудомістким і вимагає високої кваліфікації персоналу, що збільшує час і витрати в міру зростання масштабу перевірок.

Автоматизовані засоби проведення аудиту дозволяють запускати скрипти для перевірки конфігурацій безпеки на локальних чи хмарних ресурсах. Цей підхід зазвичай є безкоштовним, якщо використовуються власні ресурси, однак має непрямі витрати при використанні хмарних обчислювальних потужностей. Наприклад, для запуску перевірок на Amazon EC2 вартість базового екземпляру t2.medium становить 0,0464 USD/година. Нехай вартість реалізації, а саме налаштування ресурсу, конфігурація та встановлення, займе 2 години при песимістичному підході. В такому разі витрати на проведення аудиту в хмарі складуть ≈ 3,88 грн (за курсом на березень 2025 року 1 USD ≈ 41,79 гривні).

Вбудовані інструменти, такі як AWS Security Hub, автоматизують більшість перевірок і інтегруються безпосередньо з хмарною платформою. Прямі витрати включають оплату за кількість перевірок, обробку подій та використання додаткових функцій. Варто зазначити, що Security Hub перевіряє кожен контроль для кожного ресурсу в кожному регіоні. Для розрахунку вартості можна взяти середньостатистичний AWS-акаунт, який розгорнутий у двох регіонах і включає 20 S3 бакетів, 10 EC2 інстансів, 5 IAM ролей, 3 VPC, кожна з яких має 2 Security Groups із 10 правилами в кожній, 2 Network ACLs із 20 правилами в кожній, 3 RDS бази даних, кожна з яких має 2 підключення, та 2 KMS ключі. Загальна кількість перевірок для акаунту з такою інфраструктурою складає ≈ 2480 перевірок. Вартість перевірок розраховується на основі ставки 0.001 USD за кожну перевірку для перших 100,000 перевірок. Таким чином, для 2480 перевірок загальна вартість складе 2480 · 0,001 USD, що приблизно дорівнює 103.64 грн.

Ручне проведення аудиту є найбільш витратним через значні непрямі витрати на оплату праці спеціалістів. Вбудовані інструменти, як AWS Security Hub, мають незначні прямі витрати і не вимагають непрямих витрат. Автоматизоване проведення аудиту має незначні непрямі витрати, якщо використовуються хмарні обчислення, але його вартість значно нижча, ніж у випадку ручного аудиту, що робить цей метод найбільш економним. Це порівняння підсумовано в табл. 2.

Таблиця 2 – Порівняння витрат для різних методів проведення аудиту безпеки хмарних середовищ

Метод проведення аудиту	Прямі витрати, грн	Непрямі витрати, грн
Ручний	0	2833,33
Автоматизований	0	3,88
Вбудований	103,64	0

Висновки

У результаті дослідження було проведено аналіз різних методів проведення аудиту безпеки хмарних середовищ, включаючи ручне, автоматизоване та вбудовані засоби перевірки. Визначено ключові переваги та недоліки кожного з підходів, а також їхню ефективність у різних сценаріях використання. Автоматизовані методи виявилися найбільш ефективними з точки зору швидкості та економічної доцільності, тоді як ручне проведення аудиту забезпечує вищу гнучкість та деталізованість аналізу. Вбудовані засоби моніторингу, які пропонують хмарні провайдери, виявилися корисними для постійного моніторингу змін у конфігураціях, але мають певні обмеження щодо гнучкості та підтримки нестандартних перевірок.

Дослідження показало, що використання автоматизованих інструментів дозволяє значно скоротити час проведення аудиту, знизити витрати та мінімізувати ризики людського фактора. Витрати на автоматизоване проведення аудиту становлять менш ніж 1% від вартості ручного підходу, що робить його значно більш економічно ефективним. Завдяки використанню автоматизованих рішень можна досягти значної економії ресурсів, підвищити точність оцінки безпеки та зменшити ймовірність пропуску критичних вразливостей. При цьому ручне проведення аудиту залишається актуальним у випадках, коли необхідний

індивідуальний підхід до аналізу складних конфігурацій та нестандартних налаштувань безпеки.

Результати дослідження також вказують на необхідність удосконалення підходів до аудиту безпеки шляхом інтеграції методів машинного навчання та штучного інтелекту. Використання алгоритмів аналізу даних дозволить підвищити ефективність автоматизованого аудиту, зокрема через можливість визначення критичності знайдених вразливостей та фільтрації неактуальних перевірок для конкретної організації. Застосування машинного навчання допоможе створити систему адаптивного аудиту, яка зможе ідентифікувати найбільш важливі контролі безпеки, усувати нерелевантні перевірки та знижувати кількість хибнопозитивних результатів. Це дозволить оптимізувати процес аудиту, зменшуючи навантаження на ресурси та підвищуючи його ефективність.

Подальші дослідження можуть бути зосереджені на розробці інтелектуальних систем аналізу ризиків, що здатні самостійно визначати пріоритетність виявлених загроз та рекомендувати заходи з їх усунення. Використання технологій глибокого навчання дозволить створити моделі прогнозування потенційних атак та вразливостей, що забезпечить проактивний підхід до забезпечення безпеки хмарних середовищ. Такі підходи сприятимуть підвищенню рівня захисту даних та критичних ресурсів у хмарній інфраструктурі, забезпечуючи їх відповідність сучасним стандартам безпеки.

Таким чином, результати проведеного дослідження підтверджують необхідність подальшого розвитку автоматизованих та інтелектуальних систем аудиту безпеки хмарних середовищ. Це дозволить не лише підвищити ефективність процесу оцінювання ризиків, а й зробити хмарні сервіси більш безпечними та адаптованими до сучасних викликів кібербезпеки.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. HIPA Journal. IBM: Average Cost of a Healthcare Data Breach Increases to Almost $11 Million. Retrieved from : https://www.hipaajournal.com/2023-cost-healthcare-data-breach/
2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Retrieved from : https://www.iso.org/standard/27001
3. GDPR (General Data Protection Regulation). General Data Protection Regulation. Retrieved from :https://gdpr-info.eu/
4. CIS Security. Center for Internet Security. Retrieved from : https://www.cisecurity.org/controls/v8
5. CIS Microsoft 365 Foundations Benchmark v3.1.0. Center for Internet Security, Benchmarks. Retrieved from :https://www.cisecurity.org/cis-benchmarks
6. Cybersecurity and Infrastructure Security Agency (CISA). Cybersecurity and Infrastructure Security Agency. Retrieved from : https://en.wikipedia.org/wiki/Cybersecurity_and_Infrastructure_Security_Agency
7. CISA – Official Website. Cybersecurity and Infrastructure Security Agency: Official Site. Retrieved from : https://www.cisa.gov/about

8. CISA Secure Cloud Business Applications. SCuBA project by CISA. Retrieved from : https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project
9. Prowler. AWS Security Tool. Retrieved from : https://prowler.com/
10. GitHub: Prowler. Prowler repository on GitHub. Retrieved from : https://github.com/prowler-cloud/prowler
11. GitHub: ScubaGoggles. ScubaGoggles repository. Retrieved from : https://github.com/cisagov/ScubaGoggles
12. AWS Security Hub User Guide. AWS Security Hub: User Guide. Retrieved from : https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html
13. AWS Security Hub. AWS Security Hub. Retrieved from : https://aws.amazon.com/ru/security-hub/
14. Microsoft Secure Score. Microsoft Secure Score. Retrieved from : https://learn.microsoft.com/en-us/defender-xdr/microsoft-secure-score
15. Microsoft Compliance Manager. Microsoft Compliance Manager. Retrieved from : https://learn.microsoft.com/en-us/purview/compliance-manager
16. GitHub: ScubaGear. ScubaGear repository. Retrieved from : https://github.com/cisagov/ScubaGear
17. Work.ua. Information security specialist: average salary in Ukraine. Retrieved from : https://www.work.ua/en/salary-information+security+specialist/

References

1. HIPA Journal. IBM: Average Cost of a Healthcare Data Breach Increases to Almost $11 Million. Retrieved from : https://www.hipaajournal.com/2023-cost-healthcare-data-breach/
2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Retrieved from : https://www.iso.org/standard/27001
3. GDPR (General Data Protection Regulation). General Data Protection Regulation. Retrieved from :https://gdpr-info.eu/
4. CIS Security. Center for Internet Security. Retrieved from : https://www.cisecurity.org/controls/v8
5. CIS Microsoft 365 Foundations Benchmark v3.1.0. Center for Internet Security, Benchmarks. Retrieved from :https://www.cisecurity.org/cis-benchmarks
6. Cybersecurity and Infrastructure Security Agency (CISA). Cybersecurity and Infrastructure Security Agency. Retrieved from : https://en.wikipedia.org/wiki/Cybersecurity_and_Infrastructure_Security_Agency
7. CISA – Official Website. Cybersecurity and Infrastructure Security Agency: Official Site. Retrieved from : https://www.cisa.gov/about
8. CISA Secure Cloud Business Applications. SCuBA project by CISA. Retrieved from : https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project
9. Prowler. AWS Security Tool. Retrieved from : https://prowler.com/
10. GitHub: Prowler. Prowler repository on GitHub. Retrieved from : https://github.com/prowler-cloud/prowler
11. GitHub: ScubaGoggles. ScubaGoggles repository. Retrieved from : https://github.com/cisagov/ScubaGoggles
12. AWS Security Hub User Guide. AWS Security Hub: User Guide. Retrieved from : https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html

13. AWS Security Hub. AWS Security Hub. Retrieved from : https://aws.amazon.com/ru/security-hub/
14. Microsoft Secure Score. Microsoft Secure Score. Retrieved from : https://learn.microsoft.com/en-us/defender-xdr/microsoft-secure-score
15. Microsoft Compliance Manager. Microsoft Compliance Manager. Retrieved from : https://learn.microsoft.com/en-us/purview/compliance-manager
16. GitHub: ScubaGear. ScubaGear repository. Retrieved from : https://github.com/cisagov/ScubaGear
17. Work.ua. Information security specialist: average salary in Ukraine. Retrieved from : https://www.work.ua/en/salary-information+security+specialist/

The Probability of the Military Potential Increase: Financial and Economic Factors

Ймовірність підвищення рейтингу військового потенціалу: фінансові та економічні фактори

Oleksandr Ostapenko [A]

Corresponding author: PhD in Economics, Head of the Department of Financial Support of Troops, e-mail: ap080011@knu.ua, ORCID: 0000-0003-3194-0372

Oles Koval [A]

PhD in Finance, Associate Professor of the Department of Financial Support of Troops, e-mail: oles.koval@knu.ua, ORCID: 0000-0003-2696-7204

Олександр Остапенко [A]

Corresponding author: к. tкономн. наук, начальник кафедри фінансового забезпечення військ, e-mail: ap080011@knu.ua, ORCID: 0000-0003-3194-0372

Олесь Коваль [A]

доктор філософії з фінансів, банківської справи та страхування, доцент кафедри фінансового забезпечення військ, e-mail: oles.koval@knu.ua, ORCID: 0000-0003-2696-7204

[A] Military Institute of Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

[A] Військовий інститут Київського національного університету імені Тараса Шевченка, Київ, Україна

Received: March 12, 2025 | Revised: Aprile 20, 2025 | Accepted: Aprile 30, 2025

JEL Classification: C51, E12, E13.

DOI: 10.33445/sds.2025.15.2.20

Purpose: To model financial and economic indicators and determine their real impact on Ukraine's military power (military potential).

Method: Non-linear modelling.

Findings: The results of the preliminary exploratory data analysis indicate that it is advisable to use the following variables for modelling: business environment and credit. Thus, an increase in the business environment indicator (improvement in the following parameters: stability of economic policy for doing business; economic policy and entrepreneurship culture) adds 3.64% to the probability of improving the military potential rating; an increase in the credit indicator (financing start-ups and scaling up; domestic loans to the private sector, as a percentage of GDP; loans to microfinance institutions, as a percentage of GDP) adds 2.04% to the probability of improving the military potential rating.

Theoretical implications: The understanding of Ukraine's economic capabilities has been expanded to include the following factors: investment; credit; business environment; general infrastructure; intangible assets; trade, diversification and market scale. Ukraine's military potential has good chances for growth if defence production, i.e. military entrepreneurship, is properly supported, which in turn requires improvement of business tools and the business climate. Meanwhile, business activities related to the production of weapons and military equipment require proper crediting—financial support from the state and local budgets.

Value: Classical and neoclassical theories have become a sufficient basis for an empirical study, which indicates that, given the positive dynamics of the financial and economic sector of Ukraine, the process of military building takes place in the plane of a favourable business climate and lending to entrepreneurial activities, in particular, the production of weapons and military equipment.

Future research: The prospect of further research is to expand the range of time series, countries, and methods of nonlinear modelling.

Майбутні дослідження: Перспектива подальших досліджень полягає в розширені діапазону часових рядів, країн та методів нелінійного моделювання.

Paper type: емпірична.

Мета: здійснити моделювання фінансових та економічних індикаторів для з'ясування їхнього реального впливу на військову могутність (військовий потенціал) України.

Метод дослідження: нелінійне моделювання

Результати дослідження: Результати аналізу даних свідчать про те, що для моделювання доцільно використати наступні змінні: бізнес середовище та кредитування. Так, зростання індикатора бізнес середовища (покращення показників: стабільності економічної політики для ведення бізнесу; економічної політики та культури підприємництва) додає ймовірності покращення рейтингу військового потенціалу на 3,64 %; зростання індикатора кредитування (фінансування стартапів та масштабування; внутрішні кредити приватному сектору, у % від ВВП; кредити мікрофінансових організацій, у % від ВВП) додає ймовірності покращення рейтингу військового потенціалу на 2,04 %.

Теоретична цінність дослідження: Розширено розуміння економічних спроможностей України за рахунок таких факторів: інвестування; кредитування; бізнес середовище; загальна інфраструктура; нематеріальні активи; торгівля, диверсифікація та розміри ринку. Військовий потенціал України має хороші шанси для розвитку, якщо належним чином буде забезпечено оборонно-промислове виробництво, тобто військову підприємницьку діяльність, яка свою чергою потребує вдосконалення інструментів ведення бізнесу та безпосередньо покращення бізнес клімату. Водночас підприємницька діяльність з виробництва озброєння та військової техніки потребує належного кредитування, зокрема, фінансової підтримки з державного та місцевого бюджетів.

Цінність дослідження: Класичні та неокласичні теорії стали достатнім підґрунтям для проведення емпіричного дослідження, яке вказує на те, що за умови позитивної динаміки фінансово-економічного сектору України, процес військового будівництва відбувається у площині сприятливого бізнесового клімату й кредитування підприємницької діяльності, зокрема, з виробництва озброєння та військової техніки.

Майбутні дослідження: Перспектива подальших досліджень полягає в розширені діапазону часових рядів, країн та методів нелінійного моделювання.

Тип статті: empirical.

Key words: probit regression, military potential, finance, economics.

Ключові слова: пробіт регресія, військовий потенціал, фінанси, економіка.

Introduction

It is obvious that the economy of a country always faces an extraordinary challenge: the approval and implementation of an effective strategy for positive economic growth in the long term, which, accordingly, is supported by appropriate government decisions. Thus, it is reasonable to consider the economy as the main engine of the country, which in turn needs to be maintained and secured, and thus protected from external influences. Building up and maintaining a high level of defense sector capabilities is closely linked to the smooth functioning of the economic system at the macro, micro, and mezzo levels. And vice versa: the higher the level of security and military potential, the more guarantees there are for the economic engine. Thus, it is reasonable to talk about such concepts as "economic security", "defense potential" and "strategy of development and interaction".

Table 1 — Components of Economic Capabilities: Financial and Economic Factors of Influence on Military Potential

MILITARY POTENTIAL ⇕ two-way causation					
Capabilities of the state's economy					
Investment	**Credit**	**Business environment**	**General infrastructure**	**Intangible assets**	**Trade, diversification and market scale**

Source*:* created by the authors.

It is natural for state leaders and military commanders to strive for a degree of cooperation in which the adjustment of the state's socio-economic development leads to improved norms and standards of living, i.e. social welfare, and, in general, well-being. This raises the question of the necessary amount of resources that could satisfy an uncompromisingly favourable investment environment, which is also a significant contribution to the development of the state. The formula is simple: more accumulated resources are a key driver in ensuring economic security, defense capabilities, and the development strategy in general. At the same time, resources need to be efficiently allocated and redistributed, considering the state's long-term priorities.

Theoretical Foundations of Research

Whatever the priorities, the mechanisms of filling the state budget remain an important characteristic of the effective functioning of the economy, among which the key role should be given to exports of goods and attraction of foreign investment in production, as opposed to excessive imports, despite the implementation of protectionist policies and loan repayment. Hence, it is advisable to identify the first important economic factor that could affect the defense sector: investment.

The second and no less important factor is lending. It is worth noting that any system is relatively stable if it has sufficient reserves. Potential problems with foreign currency outflows, in particular because of a negative trade balance, worsen stability. It is fair to say that such problems are already real for Ukraine, at least given the phenomenal volumes of imported weapons and other goods and services, the production of which has significantly decreased in Ukraine since the beginning of the full-scale war. In turn, the weaker ability to meet the needs of the domestic market increases the need for imports, through the instruments of internal and external obligations. Obviously, in such a scenario, an additional burden for the state's economy would be the

introduction of effective credit mechanisms that would provide financing for startups and forward-looking enterprises by providing domestic loans to the private sector (at the expense of state funding) and obtaining loans by enterprises from microfinance organizations.

Table 2 — Market development: investment indicator and relevant indicators in Ukraine for 2024

Market sophistication *(25,7)*			
Investment *(2,6)*			
Market capitalization, % GDP *(4,3)*	Venture capital (VC) investors, deals/bn PPP$ GDP *(0,1)*	VC recipients, deals/bn PPP$ GDP *(0,0)*	VC received, value, % GDP *(0,0)*

** score/value is indicated in brackets*

Created by the authors based on **source**: *Global Innovation Index…, 2024*.

At the same time, the effect of such decisions would be of strategic importance for the development of Ukraine's economic and defense sectors, and the corresponding "dividends" would serve to promote sustainable development and strengthen defense capabilities. Neoclassical economists argue that the private sector is more dynamic than the public sector and thus can serve as a more efficient allocation of defense spending. The Ministry of Defense can ensure the development and modernization of weapons by conducting defense procurement from the private sector, which in turn receives grants from the state budget. At the same time, the consumption of defense products on the domestic market is strategically important for the development of the state, as it simultaneously satisfies several needs: the availability of a defense order and the increase of state reserves.

Table 3 — Market development: lending indicator and relevant indicators in Ukraine for 2024

Market sophistication *(25,7)*		
Credit *(13,8)*		
Finance for startups and scaleups *(34,8)*	Domestic credit to private sector, % GDP *(23,5)*	Loans from microfinance institutions, % GDP (0,1)

Created by the authors based on **source**: *Global Innovation Index…, 2024*.

Besides credit, an important role in strengthening economic capacity belongs to the creation and maintenance of a proper business climate, which results in the production of goods and services. Thus, the third factor influencing defense capability is the business environment. Neglecting this role, along with the outflow of foreign investment and insufficient credit, can lead to inevitable stagnation of the national economy. Instead, creating a favorable investment climate, credit, and a business environment in general can stimulate the economy, by meeting consumer needs. Thus, the implementation of Keynesian theory could have quite positive consequences for economic growth and, consequently, for the development of the defense sector. Neoclassical scholars Gupta and others argue that the multiplier effect occurs during the period of increased military expenditures and production stimulation (Gupta S., et. al., 2004). It is worth noting that the multiplier effect would work in the context of the development of the business environment, including the introduction of an effective economic policy to stabilize business development,

business policy and culture, which would have a positive impact on the development of the defense sector. This also makes sense for the development of defense production, which is a strategically important task for Ukraine.

Table 4 — Market development: business environment indicator and relevant indicators in Ukraine for 2024

Institutions *(30,8)*	
Business environment *(38,2)*	
Policy stability for doing business *(46,0)*	Entrepreneurship policies and culture (30,3)

Created by the authors based on **source**: *Global Innovation Index…, 2024*.

From both a theoretical and practical point of view, it may be inappropriate to explain economic growth because of increased expenditures of the Ministry of Defense under the budget program for the purchase and modernization of weapons and military equipment. Increased public spending should be accompanied by improvements in institutional development, human capital, market sophistication, creativity, and infrastructure. Earlier it was mentioned that the national economy has better chances of growth through the production of goods for export. However, such production cannot be effective without the development of the overall infrastructure through such tools as electricity generation, logistics, and gross capital formation (as a percentage of GDP). That is why the fourth important factor is the development of *general infrastructure*.

Table 5 — Market development: general infrastructure indicator and relevant indicators in Ukraine for 2024

Infrastructure *(35,5)*		
General infrastructure *(13,8)*		
Electricity output, GWh/mn pop. *(3605,8)*	Logistics performance (27,3)	Gross capital formation, % GDP (14,1)

Created by the authors based on **source**: *Global Innovation Index…, 2024*.

Finally, the private sector, based on democratic principles, functions using innovation, which is also the engine of economic progress. The authoritative opinions of prominent figures of the productive capacity school, Adam Smith and David Ricardo, as well as the neoclassical theories of Paul Krugman, suggest that market efficiency is achieved through the exploitation of natural and human resources. However, Joseph Schumpeter aptly noted that the basis of any production is the involvement of innovation. In general, market efficiency is based on the following postulate: the productive capacity of various economic activities provides a so-called “window of opportunity” for achieving a high level of social welfare. At the same time, policymakers tend to forget that technology is the “invisible hand” of production progress.

In turn, technology is not born by itself. Of course, there can be a positive relationship between technology development and the four factors listed above: investment, credit, general infrastructure, and the business environment. Technology, which is so important for building military capabilities, is a derivative of intangible assets. That is why we tend to assume that intangible assets are the fifth factor influencing military potential. At the same time, the intangible assets indicator is expressed in the following indicators: intensity of intangible assets use; trademarks by origin; global value of brands; industrial designs by origin.

The problem of the printing press (an invention that was negatively perceived in some Eastern cultures) can explain the existence of barriers to development, the most obvious of which is the government's refusal to abandon archaism and allow innovation to influence state-building processes, including economic growth and military potential through improved weapons and military equipment production technologies. However, even when allowing innovation in the economic and security sector, governments can exercise undemocratic control over the use of modern technologies, thus demonstrating the absolutism and extractivity of a rentier economy that functions mainly on revenues from the extraction and sale of natural resources and monopolies among elites close to a strong authoritarian leader. According to Solow, products generate products, so innovations generate innovations.

Table 6 — Market development: creative development indicator and relevant indicators in Ukraine for 2024

Creative outputs *(23,7)*			
Intangible assets *(25,8)*			
Intangible asset intensity, top 15, % (n/a)	Trademarks by origin/bn PPP$ GDP (52,3)	Global brand value, top 5,000, % GDP (0,4)	Industrial designs by origin/bn PPP$ GDP(4,0)

Created by the authors based on **source**: *Global Innovation Index…, 2024*.

Obviously, the production of goods by the Ukrainian defence industry has a high chance of positively affecting Ukraine's economic growth, at least due to the democratic policy of using war-born innovations. According to Abramovitz, the expansion of innovation capabilities, compared to capital accumulation, is a better explanation of economic growth (Abramovitz, 1986). Meeting the demand of the Ministry of Defence of Ukraine 'here and now' is exactly the progressive niche that the Government has been meeting since 2021 mainly through imports. Economically developed countries of the world 'earn' from the war by lifting restrictions on the export of military and dual-use goods to recipient countries. Meeting the supply and demand for military goods and services under martial law through domestic production to guarantee sovereignty, territorial integrity and inviolability requires new ideas.

First, it is worth noting that the neoclassical theory of economic capability development cannot be applied to the economic growth of developing countries. Richard Nelson, who studied the issues related to the constant inflow of innovations in various spheres of economic activity, believed the use of modern technologies in production gives rise to the possibility of 'doing things in a new way' (Malerba, 2011). If we link this idea to the property of self-reproduction in the context of the Solow model, according to which part of the manufactured products is returned to the production system, we can achieve significant results in the development of defence capability in the context of defence production. Ensuring such a production philosophy requires a symbiosis with the main determinant of avoiding monopoly—market competition. In the presence of competition, each producer resorts to innovations in the production process to differentiate goods and services.

In response to a rather controversial question, it is essential to note that the benefits of innovation in industrial production are more economically favourable to inclusive public or private institutions, and this strategy implies a steady and uncompromising development of trade, diversification and market size. When it comes to the development of market relations, it is assumed that such an institution is formed mainly through inclusive state institutional support. In this context, inclusiveness should be understood as the quintessence of the rights and freedoms of entrepreneurs, free interaction between stakeholders in the relevant production, and democratic

principles of regulatory and controlling state functions. In general, entrepreneurs tend to choose the perspective of capital accumulation. That is why the development of the state's economic capacity through international trade in goods and services, including military and dual-use goods, primarily involves the introduction and use of effective mechanisms of competitiveness in the domestic market—through government encouragement of the development of private defence enterprises that are able to structure the production of goods in accordance with the principles of adaptability, flexibility and openness.

Table 7 — Market sophistication: an indicator of trade, diversification, market size and relevant indicators in Ukraine for 2024

Market sophistication *(25,7)*		
Trade, diversification and market scale *(60,7)*		
Applied tariff rate, weighted avg., % *(1,6)*	Domestic industry diversification (85,6)	Domestic market scale, bn PPP$ (474,8)

Created by the authors based on **source**: *Global Innovation Index…, 2024*.

Before competing in the global market, which in turn will create a favourable interest of potential importers, it is necessary to take care of the ability to freely move and sell goods in the national economy. The form of sale of military and dual-use goods, which form the basis of military potential—*the military power of the state*—in a democratic manner is generated by the demand for such goods from the guarantors of defence capability, which has become especially relevant for Ukraine. In this way, supply and value added will guarantee national and economic security and maintain a high level of defence capability.

Porter identifies four steps to sustainable economic growth based on industrial production, which implies market competitiveness and is focused on investment, innovation and social welfare (Porter, 1990). Public and private companies that have access to leading technologies—*for example, in the fields of artificial intelligence and aerospace construction*—gain a significant advantage over other economies that grow mainly through low-cost textile production or the assembly of electronic components. In this way, the advanced technological potential of economically developed countries will serve as a kind of boost to the rapid introduction of innovations when creating a new product, even if this product is not related to the scope of available innovations. In this way, the production of military and dual-use goods will be competitive and guarantee a high level of defence capability.

Problem Statement

Despite the advantages of protectionist policies, there are still open issues related to the direct maintenance of a high level of functioning of national production capacities. The main difficulty may lie in insufficient investment, financial support, poorly developed business environment, etc. Thus, there is every reason to believe that there may be a threat to national producers of armaments and military equipment and thus risks to the development and maintenance of the appropriate level of Ukraine's military potential.

The development of Ukraine's military potential through the introduction of effective mechanisms and the use of efficient financial and economic instruments requires, first, an analysis of the prevailing circumstances and modelling the impact of economic and financial factors on Ukraine's military power. The main challenges include the relevance of classical and neoclassical economic doctrines to the selection of indicators required for modelling. In addition, some of the indicators used in the modelling may not follow normal or lognormal distributions, which in turn creates risks for the least biased interpretation of the results.

Research Methodology

The use of probit and logit models is a common method for calculating the probability of a certain event occurring. For example, Ismawati Isti Yuli and Faturohma Taufik used logistic regression for a credit scoring model to determine the probability of default in a financial institution (Ismawati, I. Y., & Faturohma, T, 2023). The study identified nine variables that were used as predictors of default probability, namely: job type, work experience, net financial value, term, car brand, asset price, down payment percentage, interest, and income. All nine variables meet the goodness of fit criteria, which consist of WOE, IV, and p-value.

Durango-Gutiérrez, María Patricia and Lara-Rubio, Juan and Navarro-Galera, Andrés applied logistic regression to analyse the risk of default in financial organisations (micro level) (Durango-Gutiérrez et al, 2023). The results obtained were clear and convincing both for the use of logistic and probit models in statistical analysis and calculation of the probability of an event that is somehow related to the financial and economic sector of activity.

Despite the widespread use of the probit model, most applied researchers misinterpret the interaction term in nonlinear models. Ai, C. R. and Norton, E. C. conducted a review of economic journals to determine whether researchers use interaction terms in nonlinear models (Ai, C. R., & Norton, E. C., 2003). The authors pointed out that none of the studies interpreted the coefficient on the interaction terms correctly. Thus, it is important to focus on the correct interpretation of the modelling results, considering the recommendations of the researchers.

Thus, we can see that logistic and probit regression are widely used in studies related to calculating the probability of a certain event. It is also noticeable that the authors of these studies use different software—R, Python, Excel, Stata. The STATISTICA software product is somewhat less commonly used.

Meanwhile, the main condition for using probit models is that they follow a standard normal or lognormal distribution. The probit model can also be applied not only to continuous variables that follow a normal distribution, but also to categorical values that have a binomial distribution and can be approximated to a standard normal distribution, which is why the capabilities of probit models are much wider than those of logit models.

Before moving on to the model, it is necessary to explain the choice of nonlinear modelling, namely the probit model. It is well known that in applied research, scientists often estimate interaction coefficients to draw conclusions about the impact of one independent variable on other dependent variables and the impact of time series (indicators). For example, whether the level of investment in the domestic defence industry affects the overall level of development of production capabilities. To find out, it is advisable to use linear regression in terms of its two functions, namely:

observing the linear relationship of past periods. If the coefficient is statistically significant, there is a difference between state-owned and private enterprises in terms of sources of funding;

make forecasts. The disadvantage of forecasting is that the input parameters can take on values ranging from the minimum and maximum values of past observations, which, in turn, makes it impossible to study any other cases and deviations in the forecasted future.

Interaction terms are also very often used in nonlinear models, such as logit and probit models. Unfortunately, the logic of linear regression models does not apply to nonlinear models. In addition, the sign may be different for different observations. Statistical significance cannot be determined based on the z-statistic reported in the regression results. The odds ratio interpretation for logit coefficients cannot be used for interaction terms. However, unlike linear regression, nonlinear probabilistic regression allows the results to be interpreted in terms of the probability of a particular event occurring, which can be either true or false (1 or 0).

In general, the range of possible values can be from 0 to 1. Meanwhile, the results allow us to calculate the chances of a specific event characterised by a dichotomous variable. Since the

scientific interest is in fulfilling the goal of increasing military potential, it is also expedient to determine the chances of increasing the military potential rating based on the observations of indicators characterised by explanatory variables.

Results and Discussion

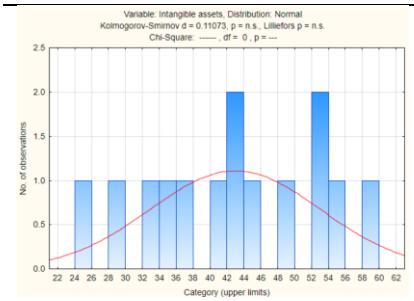
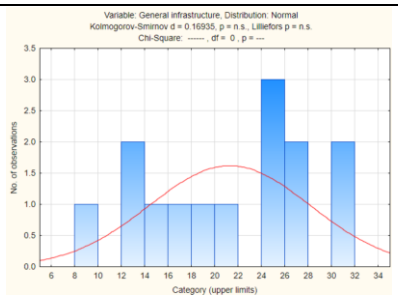
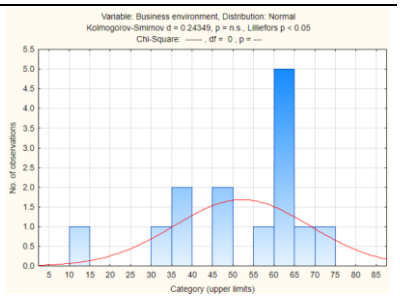
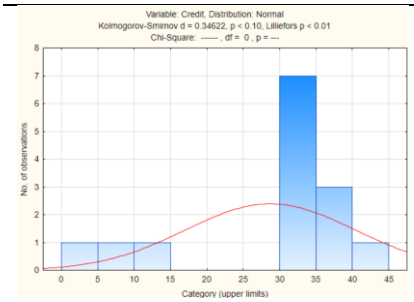
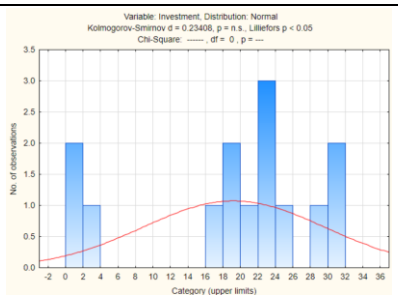
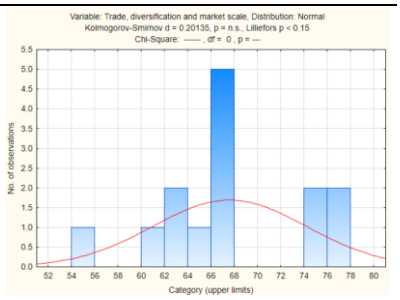
Given the relevance of conducting an empirical study to calculate the probability of increasing the rating of Ukraine's military potential, it is necessary to use explanatory variables and a dichotomous (dependent) variable. The explanatory variables were defined earlier, namely: *intangible assets* (1), *general infrastructure* (2), *business environment* (3), *credit* (4), *investment* (5), *trade, diversification, market scale* (6). A dichotomous variable is the fact that Ukraine is included in the ranking of the top 25 countries in terms of military power development—Global Firepower Index (Global Firepower, 2025). This will make it possible to determine the level of interrelationships between the explanatory variables, as well as to directly calculate the probability of increasing the rating of Ukraine's military potential through economic capabilities—the explanatory variables.

First, it is necessary to conduct an exploratory analysis of the data: a test for normal distribution is performed. The Kolmogorov-Smirnov method is preliminarily applied. Although the interpretation of the results of this method can be ambiguous, the results are clearly structured and understandable.

The normal distribution allows only numerical values, i.e. all explanatory variables can be used, except for the military power variable (which is categorical and thus dichotomous). It is important to note that an additional test for lognormality is performed, since the dependent variable contains categorical data, namely, whether a country is in the top 25 countries in terms of military power or not. As noted earlier, the advantage of probit models is the ability to analyse and model non-numerical, i.e. categorical, variables.

Tables 8 and 9 show the results of the normal distribution of the data. Based on the results of the analysis, decisions are made regarding further modelling.

Table 8 — Results of the normal distribution of data

Intangible assets	*General infrastructure*	*Business environment*
		
Credit	*Investment*	*Trade, diversification, market scale*
		

Source*:* created by the authors

Table 9 — Results of the normal distribution of data

Variable	Observed mean	Observed variance	Kolmogorov-Smirnov test	Lilliefors p	p-value	Most expected value	Percent Expected
Business environment	52,21	275,25	0,24	<0,05	n.s.	65	35,71
General infrastructure	21,28	47,56	0,17	n.s.	n.s.	26	21,43
Credit	28,72	136,46	0,35	<0,01	<0,1	35	50
Investment	19,25	108,20	0,23	<0,05	n.s.	24	21,43
Trade, diversification, and market scale	67,59	43,63	0,20	<0,15	n.s.	68	35,71
Intangible assets	42,99	101,30	0,11	n.s.	n.s.	54	14,29

Source: created by the authors

According to the results, it is noticeable that for all variables the p-value is unsatisfactory or at least unknown, except for the variable credit, which has a p-value <0.1, i.e. the distribution does not follow a normal distribution. Investigate the p-value for those variables for which it was unavailable or unsatisfactory—perhaps by testing for a lognormal distribution and changing the test parameters.

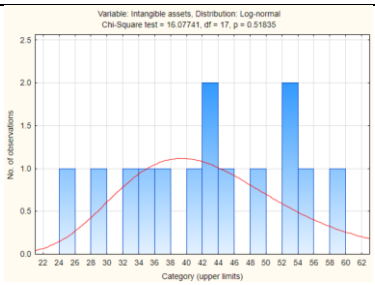
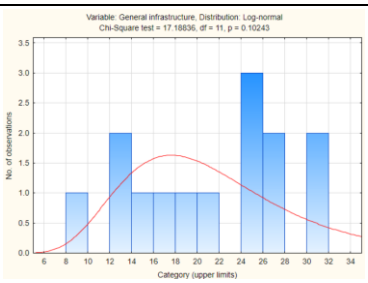
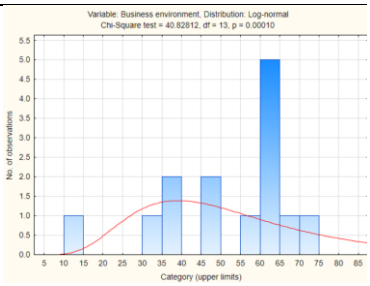
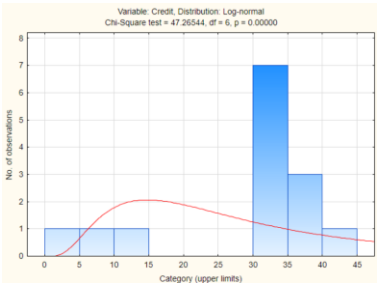
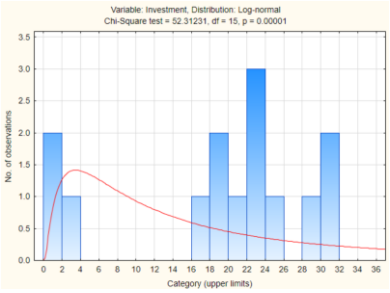
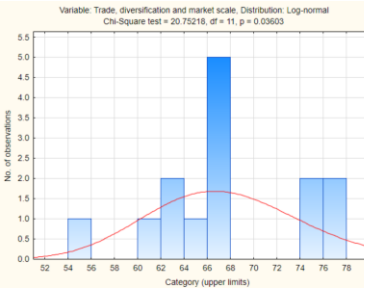
That is why the next step is to test for a lognormal distribution and to include an additional Chi-square test (*without combining the categories*, since there is no reason to expect the binary frequency to be less than or equal to 5). It is assumed that with such parameters, the test can demonstrate clearer results than the previous one.

Table 10 — Results of the lognormal distribution of data

Variable	Chi-square	df	p-value
Business environment	40,83	13	0,00010
General infrastructure	17,18	11	0,10243
Credit	47,27	6	0,00000
Investment	52,31	15	0,00001
Trade, diversification, and market scale	20,75	11	0,03603
Intangible assets	16,08	17	0,51835

Source: created by the authors

Table 11 — Results of lognormal distribution of data in graphical representation

Intangible assets	*General infrastructure*	*Business environment*
		
Credit	*Investment*	*Trade, diversification, market scale*
		

Source: created by the authors

According to the results of the lognormal distribution, it is noticeable that:

1. Variables that follow the lognormal distribution:
- general infrastructure (hereinafter—GI);
- intangible assets (hereinafter—IA);
2. Variables that do not follow a lognormal distribution:
- business environment (hereinafter—BE);
- credit (hereinafter—CR);
- investment (hereinafter—IN);
- trade, diversification, and market scale (hereinafter—TDMS).

Based on the results of the lognormal distribution, it is reasonable to assume that variables that do not follow the distribution are more unstable and sensitive to any endogenous and exogenous factors of influence. At the same time, these variables can still be included in further modelling.

In turn, this may indicate the need for further identification of the factors of influence, as well as the fact that the listed variables and their unstable state may be a signal for taking measures to further stabilise them, given the state of uncertainty.

The next stage of the analysis involves finding out the correlation between the variables, i.e. how closely they are related. Since all the variables are numerical and do not contain ranks, it is not advisable to use Spearman's correlation, but rather to use contingency tables and present the results in the form of a matrix.

It should be noted that the values obtained should be compared with a p-value < 0.05. Moreover, there is a scale of correlation on which the obtained values are compared:

- $0 < r < 0.3$—weak;
- $0.3 < r < 0.5$—moderate;
- $0.5 < r < 0.7$—noticeable;
- $0.7 < r < 0.9$—high;
- $r > 0.9$—very high (variables are highly correlated—there is a functional relationship).

Also, do not confuse p-values with r^2-value (the degree of correlation). These indicators are complementary, but not interchangeable.

For example, if the obtained correlation value is 0.5 and the p-value is < 0.05, this indicates that the obtained correlation value is not significant and, therefore, can be disregarded for modelling.

Table 12 shows the correlation indices for the identified variables.

Table 12 — Correlation matrix (correlation level)

	BE	GI	CR	IN	TDMS	IA
BE		0,28	0,52	0,60	0,09	0,56
GI	0,28		0,21	0,47	0,28	0,27
CR	0,52	0,21		0,84	0,31	0,21
IN	0,60	0,47	0,84		0,26	0,58
TDMS	0,09	0,28	0,31	0,26		0,07
IA	0,56	0,27	0,21	0,58	0,07	

Source: created by the authors

Based on the results obtained, the *r*^2-values of the relationship between the variables become noticeable. For a more meaningful assessment of the results, the p-values are presented in Table 13.

Table 13 — Correlation matrix (p-values)

	BE	GI	CR	IN	TDMS	IA
BE		0,33	0,06	0,02	0,76	0,04
GI	0,33		0,48	0,09	0,34	0,35
CR	0,06	0,48		0,00	0,28	0,47
IN	0,02	0,09	0,00		0,37	0,03
TDMS	0,76	0,34	0,28	0,37		0,80
IA	0,04	0,35	0,47	0,03	0,80	

Source: created by the authors

It is also advisable to provide additional descriptive statistics, such as the paired N, T-statistics, and slopes and intercepts of the regression equations for each correlation variable. It is advisable to perform additional checks after the selection of variables.

Before interpreting the data, it is necessary to use the Maximax or Optimism Criterion for more objective decision-making. This criterion determines which of the variables has the highest aggregate value of the relationship with the others. Next, all p-values are summed up in terms of one variable. The results are shown in Table 14.

$$max_{\theta_j} U(a_j; \theta_j) \quad (1)$$

When considering the results, it is worth highlighting the variables that have the highest cumulative correlation among all variables:

- business environment;
- credit;
- investment.

Table 14 — Summing p-values

BE	GI	CR	IN	TDMS	IA
3,05	2,51	3,09	3,76	2,01	2,69

Source: created by the authors

These variables were selected because the aggregate utility of each is greater than 3.0. Table 15 presents additional descriptive statistics from the exploratory data analysis.

Table 15 — Additional statistical analysis

	Mean	Std. Dv	r(X,Y)	r^2	t	df	p	N	Const. dep: Y	Slope dep: Y	Const. dep: X	Slope dep: X
BE	52,21	16,59										
BE	52,21	16,59	1,00	1,00		9,00		14,00	0,00	1,00	0,00	1,00
BR	52,21	16,59										
CR	28,72	11,68	0,52	0,27	2,10		0,06	14,00	9,68	0,36	31,07	0,74
BE	52,21	16,59										
IN	19,25	10,40	0,60	0,36	2,60		0,02	14,00	-0,39	0,38	33,79	0,96
CR	28,72	11,68										
BE	52,21	16,59	0,52	0,27	2,10		0,06	14,00	31,07	0,74	9,68	0,36
CR	28,72	11,68										
CR	28,72	11,68	1,00	1,00		9,00		14,00	0,00	1,00	0,00	1,00
CR	28,72	11,68										
IN	19,25	10,40	0,84	0,71	5,38		0,00	14,00	-2,26	0,75	10,54	0,94
IN	19,25	10,40										
BE	52,21	16,59	0,60	0,36	2,60		0,02	14,00	33,79	0,96	-0,39	0,38
IN	19,25	10,40										
CR	28,72	11,68	0,84	0,71	5,38		0,00	14,00	10,54	0,94	-2,26	0,75
IN	19,25	10,40										
IN	19,25	10,40	1,00	1,00		9,00		14,00	0,00	1,00	0,00	1,00

Source: created by the authors

The results show that the investment variable has a moderate level of correlation with the business environment and a high level of correlation with lending. At the same time, these

relationships cannot be significant, as the p-value is below 0.05. Therefore, we accept the correlation between the business environment and lending, which, although moderate, is significant (p-value>0.05).

This completes the exploratory analysis of the data for the presence of a relationship between the variables. Now it is advisable to build a probit model of the probability of increasing the level of military potential due to financial and economic capability. In this case, the binary values are the data of the GFI Top 25 variable (whether Ukraine is among the top 25 most powerful countries in the world), i.e. Yes/No. According to the intelligence analysis, it is proposed to include the following independent variables in the module: business environment; credit; investment.

It should be noted that the nonlinear estimations module always estimates the parameters by maximum likelihood for probit models. Conventional least-squares estimation assumes of constant error variance (or residual variance) for different values of the independent variables. In this case (the binary dependent variable GFI Top 25), this assumption is clearly violated, so it is advisable to use the maximum likelihood criterion to estimate the parameters of the probit regression model.

To evaluate the results, it is enough to build a model using the simplex method. Additionally, the error coverage of the asymptotes is selected. The results of the preliminary descriptive statistics are presented in Table 16.

Table 16 — Results of descriptive statistics

	Mean	Std. Dev.	Min	Max
BE	52,21	16,59	12,20	74,60
CR	28,72	11,68	4,90	41,20
IN	19,25	10,40	1,20	31,60

Source: created by the authors

The test results show the mean values of the variables, as well as the standard deviations known and used in the previous calculations. Parameter estimates for probit regression are concerned with predicting the z values of a normal distribution. If the normal integral of the z values is taken, values can be obtained that will never fall outside the range of 0-1.

The predicted values can be viewed as probabilities. The probit model is built with each variable separately, i.e., it checks how each individual indicator affects the country's ability to be among the top 25 countries in terms of military potential. Thus, when building the probit model, the values shown in Table 17 are obtained:

Table 17 — Probability modelling results

	Const.B0	BE	Const.B0	CR	Const.B0*	IN*
Estimate	**-4,43**	**0,07**	**-1,78**	**0,05**	**-19,52**	**0,82**
Std. Err.	2,57	0,04	1,45	0,04		
t(12)	-1,72	1,70	-1,23	1,05		
-95%CL	-10,03	-0,02	-4,93	-0,05		
+95%CL	1,17	0,16	1,37	0,14		
p-value	*0,11*	*0,12*	*0,24*	*0,31*		

** the matrix is poorly conditioned; standard errors cannot be calculated*

Source: created by the authors

For the investment variable, the matrix is ill-conditioned, and thus standard errors cannot be calculated (since the maximum number of specified iterations was exceeded during the modelling). This is probably due to a lack of information for the model. It is possible that the model is simply identified (it has 0 df), or the model may be empirically unidentified (Bollen, K. A, 1989). In this case, the result of the likelihood calculation may not be adequate. Another reason is likely to be the requirement for a minimum number of observations to build both logit and probit models.

Given the above calculations, it is advisable to model the probability of increasing the military potential rating using business environment and credit indicators. The data obtained can be used to calculate the value of z, the function of z, and the marginal effect. The results are presented in Table 19.

$$f(Z) = \left(1/\sqrt{2\pi}\right) * e^{\frac{1}{2}*z^2} \quad (2)$$

Table 18 — Standard calculations

Index	Value
$\sqrt{2\pi}$	2.51
π	3.14
e	2.72
$1/\sqrt{2\pi}$	0.39

Source: created by the authors

Table 19 — Results of calculations of Z, f(Z) and β

	Z	$f(Z)$	β
BE	-0,699081	0,509	0,036409849
CR	-0,445515	0,441	0,020436968

Source: created by the authors

The results of the calculations indicate that:

an increase in the business environment indicator (improvement of the following indicators: stability of economic policy for doing business; economic policy and entrepreneurship culture) adds to the probability of improving the military potential rating by 3.64%;

an increase in the credit score (financing of start-ups and scaling up; domestic loans to the private sector, as a percentage of GDP; loans to microfinance institutions, as a percentage of GDP) increases the likelihood of improving the rating of military potential by 2.04%.

The results can be interpreted as follows: financial and economic factors imply a well-developed system of economic policy and financial institutions, which in turn have a positive impact on improving the rating of Ukraine's military potential.

Conclusion

Thus, an exploratory analysis of the data was carried out and the probability of improving Ukraine's military potential rating was calculated when economic capabilities are the factors (explanatory variables). Six factors of Ukraine's economic capability were identified, which, according to classical and neoclassical economic doctrines, can best influence both economic growth and the improvement of Ukraine's military potential rating.

The explanatory variables were selected based on the annual Global Innovation Index report, which contains the necessary statistical data for the calculations. This report contains many indicators that can be used in the most concise and understandable way to model the improvement

of Ukraine's military potential rating, considering financial and economic factors of influence, namely *intangible assets* (1), *general infrastructure* (2), *business environment* (3), *credit* (4), *investment* (5), *trade, diversification, market scale* (6).

It is worth noting that the probit model was used for modelling from among the nonlinear modelling methods, as the scientific interest was in calculating the probability, which, in turn, is assumed to be nonlinear. The study of the trends of the last decade has confirmed the rationality and significance of research based on logistic and probit regression using differentiated software. Thus, the software STASISTICA 10.0 with the built-in module Advanced Models/Nonlinear Estimations was used. It is worth noting that the modelling results fully satisfy the objectives, and therefore the aim of the study has been achieved.

The classical and neoclassical doctrines, which were referred to in the text of the article, proved to be useful, as the modelling results confirmed the positive impact of some financial and economic factors on the fundamental factor of state-building: military potential. Thus, improving the business environment and credit increases the probability of improving Ukraine's military potential rating by 3.64% and 2.04%, respectively. In turn, this indicates that Ukraine's military potential has good chances for development if defence production, i.e. military entrepreneurship, is properly supported, which in turn requires improving business tools and directly improving the business climate. At the same time, business activities in the production of weapons and military equipment require proper lending, i.e. financial support from the state and local budgets.

This suggests that over the period under study (the statistical data used for modelling was collected from 2011 to 2024), the improvement of the business environment, in particular, business lending, improved Ukraine's military potential. Thus, this indicates a positive trend that the Government of Ukraine should continue to pursue, particularly given the current geopolitical and economic challenges facing the country (the context of the Russian-Ukrainian war, Ukraine's Euro-Atlantic integration, and further development prospects). At the same time, the question of calculating the probability of raising the military potential rating for the European Union and key geopolitical players who are somehow related to the situation in modern Ukraine remains open. It is also interesting to conduct the study over a longer period.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

Abramovitz, M. (1986). Catching Up, Forging Ahead, and Falling Behind. *The Journal of Economic History*, *46*(2), 385–406. https://doi.org/10.1017/S0022050700046209

Ai, C. R., & Norton, E. C. (2003). Interaction terms in logit and probit models. *ECONOMICS LETTERS*, *80*(1), 123–129.https://doi.org/10.1016/S0165–1765(03)00032–6

Bollen, K. A. (1989). *Structural Equations with Latent Variables*. John Wiley & Sons

Durango-Gutiérrez, M. P., Lara-Rubio, J., & Navarro-Galera, A. (2023). Analysis of default risk in microfinance institutions under the Basel III framework. *International Journal of Finance and Economics*, *28*(2), 1261–1278. Scopus. https://doi.org/10.1002/ijfe.2475

Global Firepower—2025 World Military Strength Rankings. (n.d.). Retrieved 7 February 2025, from https://www.globalfirepower.com/

Global Innovation Index 2024. (n.d.). Retrieved 6 February 2025, from https://www.wipo.int/web-publications/global-innovation-index-2024/index.html

Gupta S., et. al. (2004). Fiscal consequences of armed conflict and terrorism in low and middle income countries. *European journal of political economy*. 2 (20), 403–421. https://doi.org/10.5089/9781451856262.001

Ismawati, I. Y., & Faturohma, T. (2023). CREDIT RISK SCORING MODEL FOR CONSUMER FINANCING: LOGISTIC REGRESSION METHOD. *International Symposia in Economic Theory and Econometrics*, *31*, 167–189. Scopus. https://doi.org/10.1108/S1571-038620230000031023

Malerba, F., & Nelson, R. (2011). Learning and catching up in different sectoral systems: Evidence from six industries. *Industrial and Corporate Change*, *20*(6), 1645–1675. https://doi.org/10.1093/icc/dtr062

Porter, M. E. (1990, March 1). The Competitive Advantage of Nations. *Harvard Business Review*. https://hbr.org/1990/03/the-competitive-advantage-of-nations

Список використаних джерел

Abramovitz, M. (1986). Catching Up, Forging Ahead, and Falling Behind. *The Journal of Economic History*, *46*(2), 385–406. https://doi.org/10.1017/S0022050700046209

Ai, C. R., & Norton, E. C. (2003). Interaction terms in logit and probit models. *ECONOMICS LETTERS*, *80*(1), 123–129.https://doi.org/10.1016/S0165–1765(03)00032–6

Bollen, K. A. (1989). *Structural Equations with Latent Variables*. John Wiley & Sons

Durango-Gutiérrez, M. P., Lara-Rubio, J., & Navarro-Galera, A. (2023). Analysis of default risk in microfinance institutions under the Basel III framework. *International Journal of Finance and Economics*, *28*(2), 1261–1278. Scopus. https://doi.org/10.1002/ijfe.2475

Global Firepower—2025 World Military Strength Rankings. (n.d.). Retrieved 7 February 2025, from https://www.globalfirepower.com/

Global Innovation Index 2024. (n.d.). Retrieved 6 February 2025, from https://www.wipo.int/web-publications/global-innovation-index-2024/index.html

Gupta S., et. al. (2004). Fiscal consequences of armed conflict and terrorism in low and middle income countries. *European journal of political economy*. 2 (20), 403–421. https://doi.org/10.5089/9781451856262.001

Ismawati, I. Y., & Faturohma, T. (2023). CREDIT RISK SCORING MODEL FOR CONSUMER FINANCING: LOGISTIC REGRESSION METHOD. *International Symposia in Economic Theory and Econometrics*, *31*, 167–189. Scopus. https://doi.org/10.1108/S1571-038620230000031023

Malerba, F., & Nelson, R. (2011). Learning and catching up in different sectoral systems: Evidence from six industries. *Industrial and Corporate Change*, *20*(6), 1645–1675. https://doi.org/10.1093/icc/dtr062

Porter, M. E. (1990, March 1). The Competitive Advantage of Nations. *Harvard Business Review*. https://hbr.org/1990/03/the-competitive-advantage-of-nations

Human Security at the Helm of the Socio-Economic Development

Безпека людини як визначальний чинник соціально-економічного розвитку

Primrose Thandekile Sabela [A]
e-mail: ramphabanaL@ukzn.ac.za
Mfundo Mandla Masuku [B]
e-mail: ramphabanaL@ukzn.ac.za
Mbongeni Shadrack [C]
e-mail: ramphabanaL@ukzn.ac.za
Livhuwani Bethuel Ramphabana [B]
Corresponding author: e-mail: ramphabanaL@ukzn.ac.za

Примула Тандекіле Сабела [A]
e-mail: ramphabanaL@ukzn.ac.za
Мфундо Мандла Масуку [B]
e-mail: ramphabanaL@ukzn.ac.za
Мбонгені Шедрак [C]
e-mail: ramphabanaL@ukzn.ac.za
Лівхувані Бетуель Рамфабана [B]
Corresponding author: e-mail: ramphabanaL@ukzn.ac.za

[A] University of Mpumalanga, South Africa
[B] University of KwaZulu-Natal, South Africa
[C] University of the Western Cape, South Africa

[A] Університет Мпумаланги, Південна Африка
[B] Університет Квазулу-Натал, Південна Африка
[C] Університет Західної Капської провінції, Південна Африка

Received: March 25, 2025 | Revised: Aprile 28, 2025 | Accepted: Aprile 30, 2025

DOI: 10.33445/sds.2025.15.2.21

Purpose: The article aims to critically analyze the complex interrelationship between security and socio-economic development. It explores the concept of human security as a driver of peace, security, and sustainable socio-economic development.

Method: The study uses a qualitative approach. It uses an analysis of existing literature to shed light on human security as an approach to safety and the improvement of human life. The study analyzes secondary data with a special emphasis on the contributions of other scholars.

Findings: The article highlights the importance of human security in socio-economic development. It argues that human security should be viewed as a comprehensive and multifaceted approach that takes into account different aspects of human well-being. It also emphasizes the need for clear guidelines and indicators for measuring and achieving human security.

Theoretical implications: The article contributes to the existing literature on human security by providing a critical analysis of the concept and its relationship to socio-economic development. It offers a theoretical framework for understanding the complex dynamics between security and development.

Practical implications: The article offers insights for policymakers, researchers, and practitioners working in the fields of development and security. It highlights the importance of integrating human security into development programs and promoting peace, stability, and social justice.

Paper type: analytical.

Мета: здійснити критичний аналіз складного взаємозв'язку між безпекою та соціально-економічним розвитком. Вона досліджує концепцію людської безпеки як рушія миру, безпеки та сталого соціально-економічного розвитку.

Метод дослідження: У дослідженні використовується якісний підхід. Він використовує аналіз наявної літератури, щоб пролити світло на людську безпеку як підхід до безпеки та покращення людського життя. Дослідження аналізує вторинні дані з особливим акцентом на внеску інших науковців.

Результати дослідження: У статті підкреслюється важливість людської безпеки у соціально-економічному розвитку. Вона стверджує, що людську безпеку слід розглядати як комплексний та багатогранний підхід, що враховує різні аспекти людського добробуту. Вона також підкреслює необхідність чітких керівних принципів та показників для вимірювання людської безпеки та досягнення її.

Теоретична цінність дослідження: Стаття сприяє існуючій літературі з людської безпеки, надаючи критичний аналіз концепції та її взаємозв'язку з соціально-економічним розвитком. Вона пропонує теоретичну основу для розуміння складної динаміки між безпекою та розвитком.

Практична цінність дослідження: Стаття пропонує розуміння для політиків, дослідників та практиків, які працюють у галузі розвитку та безпеки. Вона підкреслює важливість врахування людської безпеки в програмах розвитку та сприяння миру, стабільності та соціальної справедливості.

Тип статті: аналітична.

Key words: human security, human rights, peace, socio-economic development.

Ключові слова: безпека людини, права людини, мир, соціально-економічний розвиток.

Introduction

Development does not stand a chance without security or in the presence of violent conflicts. In the context of sustainable development, various human threats — namely political, economic, social, and ecological — persist and intersect (Bhandari, 2024; Jacobs, 2016).

This paper seeks to provide a critical analysis of the complex relationship between security and socio-economic development. It employs the human security approach and the capability approach as analytical lenses and frameworks for advancing inclusive and sustainable socio-economic development. Human security emerges as a lever for transformative programs aimed at creating an environment conducive to development agendas within developing countries.

In its narrow sense, aligned with the focus of this paper, human security is described "as the security of the human species, or as the security of human individuals" (Gasper, 2010:25). One of the motives guiding this paper, and the approach undertaken herein, is what Krause and Jütersonke (2005) assert: the realization that security and development concerns have seldom been linked.

The security and development nexus relates to a virtuous circle of increasing human well-being and fulfilment. Andersen-Rodgers and Crawford (2018) maintain that peace, security, and development are closely connected and must be viewed as key to effective strategies for addressing the root causes of social unrest and violence. Furthermore, Mastrojeni (2017) identifies a number of persistent and growing threats to peace, security, and development, such as rising financial instability, unemployment, economic inequality, social tension, cultural conflict, competition for scarce resources, ecological destruction, political instability, and other challenges.

Habiyaremye et al. (2022) argue that the process of social organization is key to socio-economic development. Conflict, violence, and the absence of peace tend to undermine a country's security and development.

The 2030 Agenda for Sustainable Development states that sustainable development cannot be realised without peace and security, and that both are at risk without sustainable development (United Nations, 2015). The agenda recognizes the need to live in a world free of disruptive conflict, poverty, disease, and unemployment and proposes environments characterized by equitable and universal access to quality education, health care, social protection from violence and repression, and access to reliable and sustainable energy. Furthermore, the Agenda resolves to build peaceful, just, and inclusive societies.

Jacobs (2016) and Smith (2024) suggest that disruptive conflict, social unrest, instability, and other challenges are not attributes of a well-functioning society or healthy social organisations. Despite peace and security being fundamental for development, Jacobs (2016) maintains that violence and insecurity persist in developing countries, claiming that the ideal of peace and human security for the majority remains elusive, distant, and utopian. Jacobs (2016:50) states that "the social compact for peace, freedom and prosperity for all enthusiastically embraced in the early 1990s has been replaced by a growing sense of uncertainty and insecurity regarding the future of the human community."

This study followed a qualitative approach, with specific interest in critically analysing human security as a driver for peace, security, and socio-economic development. It draws on a range of studies to shed light on the question of human security as an approach to security and the betterment of human lives. Secondary data was analysed, with a special focus on the contributions of other scholars.

In the first part, the paper explains what constitutes human security in relation to human rights. It then establishes the relationship between human security and socio-economic development, including a critical reflection on the peace, security, and development nexus. The final part concludes by focusing on how human security can serve as a lever for transformative development programmes.

Theoretical background

The discussion on human security as a driver for socio-economic development is anchored in the human security approach and the capability approach. These two approaches play a complementary role as lenses for explaining human security.

On the one hand, the human security approach challenges the state-centric view of security in favour of a people-centred perspective. As Hama (2017:2) asserts, the human security approach regards "individuals as the referent objects of security, with states being viewed as the means to serve such ends." This approach is defined by Dinshak and Danfulani (2018) as a hybrid of critical security theory and the concept of human security. The adopted theory rejects security models that emphasize military primacy, due to their undue focus on threats and the use of force, which are no longer functional given today's realities. Dinshak and Danfulani (2018) argue that the concept of security has broadened and deepened to include individual security, while embracing the importance of analysing inequalities between the rich and the poor, poverty, and other threats to socio-economic development. The broad and multidimensional focus of security recognises freedom, peace, safety, participation in governance, and access to resources and basic necessities for a dignified life and a safe environment.

On the other hand, the capability approach is found relevant in studies related to human development. In this regard, human beings are regarded as playing a critical role in development. The pioneer of the capability approach, Amartya Sen, identified two key concepts — functionings and capabilities — as essential for explaining this approach (Alkire, 2005; Robeyns, 2017). A truly developed society is thus described as one that enables individuals to achieve a sense of being and the ability to live and act in certain valuable ways. Robeyns (2017:45) further identifies conversion factors as those that acknowledge individuals' different abilities to "convert resources into functionings." The capability approach shifts the focus from material indicators to the actual opportunities available to individuals that allow them to live fulfilling and dignified lives.

Results and Discussion

Conceptual Understanding of Security

Security is a contested and ambiguous concept requiring a unique interpretation, particularly when the concept is directly linked to peace and socio-economic development. When narrowly defined, security is conceived as relating to national security, which guarantees protection from external threats. The traditional view of security presents a feeling of being safe from harm or danger and is restricted to military defence, protection and preservation of core values, and the absence of threats to acquired values (Ahsan, 2016).

In addition, Newman (2021) attributes the conception of security to a state-centric and military vision characterised by a failure to recognize the freedoms that human beings are entitled to — that is, freedom from want, freedom from fear, and recognition of human dignity. Security within realist theories emphasises national security, particularly the preservation of the state's territorial integrity and the safety of its inhabitants. The focus is on threats to the nation, which trivialises individual security and ignores the coeval nature of state and individual security.

Recognition of both state and individual security requires a unique interpretation: that state security exists for the sake of individual security. This acknowledges the relationship between state and individual security. While one acknowledges the importance of national security, individual security is equally important, as neglecting it has the potential to pose threats to national security.

Critical human security theory draws attention to the seriousness of threats — whether global, regional, national, or internal — arguing that traditional security claims are often used to justify exclusions and discrimination. Jamshidi (2022) maintains that the way states use security claims often relates to the justification of invasions of other nations, while communities use security claims to protect and defend their human rights. Jamshidi (2022) argues that the security agenda should foster political and socio-economic benefits and opportunities for marginalized and excluded groups. This relates to creating an environment that embraces social justice and prioritizes inclusion, justice, and equality.

Human Security as Complementary to Human Rights

Security within the human context and human-based rights is recognised as providing a platform to relate security to human beings and their rights. Therefore, a multidimensional and broadened view of security includes a reflective synopsis encompassing a human rights and sustainable development explanation of issues such as environmental decline, migration, poverty, natural disasters, deadly diseases, scarcity, and inadequate access to productive resources and services. Ahsan (2016) further maintains that a key element in defining security and transforming how the concept is viewed is the consideration of ownership of key economic resources and economic capability. Literature claims that threats cannot be tackled purely by military means, and cautions that the most important questions to answer when examining security include understanding (Robinson, 2006; Ahsan, 2016; O'Brien and Williams, 2016). These questions arise: Whose security is considered? Security by whom? What security? Robinson (2006) further views development and human rights as end goals, emphasising that the focus must be on the quality and richness of human lives.

Additionally, the concept of security within the human context and human-based rights provides a platform for relating security to human beings and their rights as promulgated in the United Nations Universal Declaration of Human Rights of 1948, which encapsulates human rights, including political and civil rights, as well as social, cultural, and economic rights (Butcher and Hallward, 2017). The Declaration was created on the belief that the violation of human rights threatens the very core of peace and development. Articles 55 and 56 of the United Nations Charter urge states to promote universal respect for human rights, obligating them to ensure that human security is prioritised.

Other instruments and legislative frameworks, such as the International Covenant on Civil and Political Rights (ICCPR), which entered into force in 1976, and the International Covenant on Economic, Social and Cultural Rights (ICESCR) of 1976, promote human rights and prohibit all forms of discrimination, whether political, property-based, racial, gender-based, class-based, national, religious, or social in origin. The founding values of the South African Constitution of 1996 also include human dignity, equality, and freedom. Similarly, Chapter 2 of the Bill of Rights encapsulates socio-economic rights that relate to issues such as education, healthcare, food, housing, water, and social security, while also emphasising humanity, human dignity, and human rights.

According to Taylor (2002) and Fuo and Du Plessis (2014), the issue of core obligations of states with regard to socio-economic rights requires critical engagement with certain fundamental human needs considered non-negotiable.

Sustainable Development Goal 16 promotes peace, justice, and the development of strong institutions, maintaining that all countries must strive towards realising the goal of peaceful, just, and inclusive societies (United Nations, 2022). A country cannot develop, and people cannot achieve food security, access better education, secure employment, or raise families in disruptive conditions without peace. Furthermore, the 2030 Agenda for Sustainable Development recognises the need to build peaceful, just, and inclusive societies that provide equal access to justice based on respect for human rights, including the right to development (United Nations, 2015). The agenda highlights factors giving rise to violence, insecurity, and injustice — including inequality, corruption, poor governance, and illicit financial and arms flows — as threats to the advancement of development.

Butcher and Hallward (2017) argue that there is no shortcut to peace and development without considering the rights and well-being of people. Likewise, Ngira (2018) and Pavleski (2023) view human rights as fundamental attributes, entitlements, or necessities that human beings are inherently entitled to, and whose violation demands intervention. These rights, including dignity, life, freedom, and equality, are inherent and must be fulfilled by the state; they stem from being human and cannot be taken away. However, Butcher and Hallward (2017) and Jacobs (2016) claim

that many signatories to peace and human rights treaties, declarations, and covenants — particularly in developing countries — continue to violate the political and civil rights of their citizens. The authors assert that threats to peace, security, and development persist and continue to grow unabated.

The United Nations Report (United Nations, 2019) on progress towards achieving the Sustainable Development Goals worldwide indicates significant but slow and uneven progress in establishing legal and institutional frameworks for the defence of human rights. The Report notes that in 2018, only 39 percent of all countries were found to have successfully achieved compliance, meaning that 50 percent of all countries are projected to have compliant National Human Rights Institutions (NHRIs) by 2030 (UN Report, 2019). Furthermore, the Report states that realising the goal of peaceful, just, and inclusive societies remains elusive, as millions of people continue to be deprived of security, rights, and opportunities, which in turn holds back development.

Conflicts and various forms of violence pose significant challenges to sustainable development; the Report also notes an increase in the number of people fleeing war, persecution, and conflict, with the global number exceeding 70 million (UN Report, 2019).

Linking human rights to security and development is the concept of human security, defined by the UN Commission on Human Security (2003) as the protection of the vital core of all human lives with the aim of enhancing human freedom and human fulfilment. Appiah (2018) describes human security as encompassing not only the narrow traditional conceptualisation of security but also a broader, human-oriented conceptualisation. O'Brien and Williams (2016) argue that human security as an approach seeks to shift the focus from the state-centric traditional approach to a people-centred one, expanding the security agenda to include the perspectives of individuals and communities.

Brownlee and Cruft (2024) and Robinson (2006) view human rights as ethical claims on behalf of all human beings and human security as an important class of human rights, as it demands both ethical force and political recognition. The idea of human security can be traced back to dissatisfaction with the notions of security and development in the 1960s–1980s (Acharya, Singhdeo, and Rajaretnam, 2011).

Through the **Human Development Report** (1994), the United Nations recognised the need to broaden the traditional notion of security, which focused on state security and military defence, to include other dimensions such as environmental, food, health, and personal security, and other challenges affecting individuals daily.

Human security places greater emphasis on human well-being, while acknowledging the interconnected nature of the peace-security-development nexus. It entails several dimensions, including food security, personal security, community security, environmental security, economic security, and health security.

However, Homolar (2015) highlights the need for a clear set of guidelines specifying what these dimensions of human security encompass, as well as indicators to map the major signposts of insecurity within each dimension.

Ngira (2018) points out that the security of the individual is multifaceted, incorporating physical, psychological, social, and economic dimensions. Therefore, human security offers a more comprehensive and multidimensional approach that better serves the survival and conditions of human existence. The concept is grounded in morality or humanity, the promotion of rights (legal), and considerations of self-interest (Kaldor and Salmon, 2006).

However, Jacobs (2016) and Asaka (2018) argue that human security is often treated as a complementary "add-on" to security policies, rather than being considered an integral part of state security. Jacobs (2016) contends that this conception reflects a negative and narrow focus, failing to address the basic human needs of people, which, in turn, sparks social unrest and violence.

The author's claims resonate with the assumption that peace refers merely to the absence

of violence and that health refers simply to the absence of disease. Within a multidimensional lens, human security requires a much broader description, encompassing both physical and material security, including protection of individuals from political and economic threats.

Conceptualising Human Security within the Socio-Economic Development Context

Scholarly literature has demonstrated varied arguments about the link between security, conflict, and socio-economic development. Among such scholars are Stewart (2004), Jooma (2005), and Boshkoska (2017), who argue that poverty, characterised by inadequate or lacking income, education, food, shelter, and health, constitutes an assault on human dignity.

Ngira (2018) and Newman (2021) reason that underdevelopment could be caused by instability (both political and financial), poverty, unemployment, inequality, and other socio-economic factors. Jooma (2005) and Alence and Pitcher (2019) support the idea of the interconnectedness of poverty, underdevelopment, and civil strife, arguing that conflict and civil war often reflect not merely a development problem, but rather the failure of development itself.

Economic stagnation and high levels of poverty serve as preconditions for conflicts, violent protests, and physical insecurity. Development promotes lasting peace, whereas a lack of development leads to various forms of frustration, discontent, and violence.

Esterhuyse (2016), however, seems to be an opponent of human security and a proponent of the traditional approach to security, arguing that military power remains an essential element of security. The suitability and appropriateness of human security as an organising framework for the armed forces is viewed as problematic. With reference to South Africa, Esterhuyse (2016) argues that human security has become a sanctuary for avoiding tough questions and decisions about defence. The defence sector and its leadership appear to be unclear about how a military should be organised, trained, and equipped for human security operations.

Conversely, Article 1 of the International Covenant on Economic, Social and Cultural Rights proclaims the freedom of individuals to pursue economic, social, and cultural development, while Article 3 obliges State Parties to take reasonable and appropriate measures to ensure the realisation of economic, social, and cultural development, recognising the equal rights of men and women to enjoy all economic, social, and cultural rights.

The Convention, in accordance with the Universal Declaration of Human Rights, recognises the ideal of freedom from fear and want, which can only be achieved when everyone enjoys economic, social, and cultural rights. Article 55 of the United Nations Charter stipulates that the UN shall promote higher standards of living, full employment, and conditions of economic and social progress and development.

The Charter acknowledges that peace and global security cannot be achieved without focusing on individual well-being and emphasises promoting various forms of security, including economic, social, political, environmental, and developmental security (Scanlon and Murithi, 2006; Vietti and Scribner, 2013).

Langenhove (2004) alludes to the notion of the “securitisation of development”, arguing that human security is becoming increasingly linked to sustainable development. The question raised by this assertion concerns the interpretation and operationalisation of development as a security issue.

Evidently, insecurities and underdevelopment contribute to instability, armed conflicts, and wars, particularly in developing countries. Langenhove (2004) describes the human security approach as ideal for creating an environment conducive to freedom from want and fear, where protection against poverty, hunger, inequality, and other related social ills exists.

Human security enhances access, protection, and empowerment of individuals regarding both the material and non-material dimensions of human existence, namely food, clothing, shelter, education, health, freedom, liberty, and participation in decision-making processes.

The security of the individual is the primary focus of human security, with significant

implications for democratic participation and empowerment (Ahsan, 2016). Furthermore, the broader understanding of human security relates to the notion of freedom from want and fear, amounting to sustainable security, and offers much to the field of sustainable development with its three major pillars: economic, social, and environmental sustainability (ibid.).

Broadly, human security addresses the challenges individuals experience daily, including unemployment, job security, educational opportunities, access to health and other services, and cultural freedoms.

The question raised concerns the extent to which human security is viewed as a framework for analysing the protection of all human lives in ways that advance human freedoms and fulfilment, as well as the conceptualisation and operationalisation of the different dimensions of human security.

Economic Security Dimension

Ongoing literature embraces the multidimensional conceptualisation of human security and its holistic approach in identifying the greatest areas of individual vulnerability and insecurity (Langenhove, 2004; Homolar, 2015; Boshkoska, 2017).

Zondi (2017) also maintains that a comprehensive approach to peace and security must take into consideration social and economic opportunities, as well as political rights. The author argues that there can be no effective and lasting solution to promoting peace and human security if opportunities for gainful employment or alternative means of social welfare are not considered.

Jacobs (2016) maintains that access to employment is the principal means through which individuals acquire the purchasing power to meet basic human needs and fulfil their rising aspirations. Without adequate access to facilities, employment, and freedom, conflict and violence erupt, making development unattainable.

However, Homolar (2015) reflects on critical concerns relating to the concept, pointing to the elusive explanations and lack of specificity regarding what exactly constitutes the interlinked components of human security, how to establish indicators for measuring success and failure, and the implicit standards involved.

Leaning and Arie (2000) also noted a tendency to theorise about the nature of human security without attempting to recognise or identify the situations that support or undermine it. Homolar (2015) further argues that each component of the human security framework suffers from vagueness regarding conceptualisation and operationalisation. Furthermore, it is claimed that the selected indicators are based on unexplained, value-laden assumptions about factors contributing to individual security across different dimensions of human security.

For example, human security focuses on the creation of opportunities for the eradication of income poverty (material dimension) and human poverty (promotion of human dignity). Economic security, for instance, highlights important markers such as insecure working conditions, underemployment, a decrease in the value of nominal wages, and lack of or inadequate social security.

Homolar (ibid.) states that the main challenge could be linked to data limitations regarding the conversion of various constituent elements of income insecurity into a set of applicable measurable economic security indicators.

Linked to economic security is the health security dimension, measured as the ability of individuals, communities, and societies to avoid premature deaths. Key sources include common infectious and parasitic diseases, lifestyle diseases, and diseases caused by environmental degradation.

O'Brien and Williams (2016) allude to the link between health and security, stating that health is a critical component of well-being, and that poor health has implications for the quality of life an individual may attain. The authors maintain that a country could be directly or indirectly affected by the prevalence and spread of communicable diseases, as these may undermine state capacity and foster economic and political discord.

The impact of poor health threatens the stability and prosperity of a country and can become

both a political and economic threat.

Within the South African context, the government has proposed mechanisms to ensure equal access to the healthcare system. This is demonstrated through the National Health Insurance (NHI) Bill, which provides South Africans, particularly poor and vulnerable groups (children, women, and the elderly), with an opportunity to address the disequilibrium in access to healthcare services that exists within the health sector.

In principle, the bill should be welfare-enhancing, as it is aimed at providing access to quality healthcare for all citizens, regardless of their income level or status.

Harris et al. (2011) maintain that the present system fails to promote equal access to health services, as only 16 percent of the population have health insurance and medical aid, enabling them to access quality services in the private sector. Meanwhile, the majority of the population are relegated to the inefficient public healthcare system, which skews healthcare supply in favour of individuals with higher incomes.

As elucidated in the NHI Bill and other studies (Harris et al., 2011; Mayosi and Benatar, 2014), there is a need for a comprehensive public health framework capable of delivering equitable universal healthcare. However, the dilemma again relates to the lack of clarity on the unit of analysis, which tends to be defined at the national level, thereby overshadowing individual well-being when the focus remains on aggregate national outcomes such as mortality and fertility rates.

Security and Development Nexus in the African Context

Johansson (2015) argues that a link exists between security and development and that the concepts are connected in a mutually reinforcing relationship. If the link is weakened, the mutuality is destroyed, meaning that development cannot be attained without peace and security. However, it is sometimes difficult to establish the existence of this link because of the broadness of the concepts. This has implications for the understanding and interpretation of the concepts and for determining or setting guidelines to measure the achievement of freedom.

Scanlon and Murithi (2006) suggest that the United Nations' Seminal Report of 2006 reveals that conflicts and inter-state tensions have plagued the African continent, creating ongoing security challenges. The Report further highlights a series of humanitarian crises and wars in Africa, noting an increase in the number of refugees — approximately 6 million refugees outside the continent and more than 12.7 million internally displaced persons across 20 countries. The Report also notes the growing disparities between rich and poor inhabitants, health insecurity, and wars, all of which dramatically impact children's health and education.

Esterhuyse (2016) and Cohen (2019) argue that underlying assumptions and speculations about the role and utility of the military influenced the broadening of the security agenda. For some, it meant the end of war; for others, it signified the loss of military relevance.

The relationship between security and development within the African context was captured in the seminal 1991 Kampala Document, which argued that insecurity and instability were major impediments to economic integration and socio-economic transformation in Africa. Areas identified as requiring attention included security, stability, development, and cooperation.

Africa (2015) notes that the concept of security went beyond military considerations and included economic, political, and social dimensions. Furthermore, the author claims that the security of a nation must be construed in terms of the security of individual citizens — their ability to live in peace, have access to basic necessities of life, fully participate in societal affairs, and enjoy fundamental human rights (Africa, 2015:179).

According to Appiah (2018) and Zondi (2021), the promotion of peace, security, and stability is a prerequisite for implementing Africa's development agenda. This must be considered in light of the fragility and failure to provide essential services for development in most African states. However, fragility is not unique to Africa; it also affects developed countries. State fragility and

failure to meet basic human needs can pose peace and security threats (Tardy, 2019).

In South Africa, the policy proposals of 1994 were also informed by the Kampala Document, emphasising the need to shift from a state-centric to a people-centred approach to security (Africa, 2015). The principles associated with democratic civil-security relations and the broadening of the concept of security permeated negotiation discourses and discussions on the role of security.

Esterhuyse (2016) argues that the history of armed conflict, human rights violations, and societal dysfunctions provided a conducive environment for adopting the human security approach. Accordingly, Section 198 of the Constitution of the Republic of South Africa (RSA, 1996) outlines the principles governing the country's national security. This section makes provision for security to reflect the resolve of South Africans, as individuals and as a nation, to live as equals, in peace and harmony, free from fear and want, and to seek a better life.

In South Africa, national security relates to the state's ability to ensure the well-being of its people, including physical protection, development, freedom, prosperity, and social justice. The responsibility for maintaining and promoting peace, stability, development, and progress lies with both the government and society.

Africa (2015) presents a mixed record regarding human security in South Africa. Massive socio-economic and political gains are noted, such as government programmes that have enabled individual participation in governance and improved the lives of millions. However, weaknesses are observed in implementing the original policy framework.

The policy proposals particularly focused on achieving a proper balance between security and development. Yet, unexpected consequences — including violent protests, service delivery tensions, destruction of infrastructure, and the persistent issues of gender-based violence, homicide, and violence against foreign nationals — seemingly reflect feelings of insecurity in daily life.

Esterhuyse (2016:29) is of the view that the human security paradigm has not prevailed in South Africa and may even be a waning value in the country's political and social fabric. The author further contends that the notion of human security provided the South African military leadership with a safe haven, allowing them to avoid presenting a clearly defined and explicitly motivated military mandate. The leadership's messaging suggests that the problems experienced in the country are primarily socio-economic and non-military in nature.

Human Security as a Lever for Transformative Programmes in Socio-Economic Development

Security, peace, and development are fundamental attributes of society. Jacobs (2016) proposes that a comprehensive approach to peace and human security must take into account economic opportunity and political rights. Orago (2017) recognises that poverty, conflict, social injustices, social exclusion, and marginalisation of certain sectors are sources of insecurity and root causes of conflict.

Socio-economic development is viewed as a cornerstone of social stability, peacebuilding, and peacekeeping. Human security is seen as holistic, comprehensive, and prioritises the security, welfare, safety, and well-being of individuals. Without peace and security, there is no development; and without development, peace and security are threatened. Jacobs (2016) contends that the relationship between peace and development, though subtle, holds the key to effective strategies for addressing the root causes of unrest and violence.

Specifically, security within the socio-economic development context embraces basic social security, including access to basic services, food, shelter, health care, and employment opportunities. This reflects the concepts of freedom from want, freedom from fear, and freedom to live in dignity. The approach aims to promote human well-being by embracing psychological, physical, social, and economic aspects.

Tschirgi (2006) notes the interdependence and interconnectedness between security and

development, stating that this link is self-evident and most directly experienced through physical security and socio-economic development.

On the other hand, Langenhoven (2004) and Orago (2017) regard human insecurity as the greatest obstacle to peace and development, arguing that a commitment to promoting access, protection, and empowerment will enhance development and prevent underdevelopment. Socio-economic insecurity, as an internal threat, exposes individuals to uncertainty, anxiety, and the anticipation of difficult living conditions. Insecurity has the potential to exacerbate inequalities.

Human security is viewed as a lever for transformative programmes due to its approach and the priority it gives to individual security against violence and deprivation, with a focus on basic needs and rights for all. Gasper (2010) and Mawdsley (2019) argue that human security is not merely a single concept but a broader discourse. Accordingly, it provides a comprehensive and holistic perspective, focusing on human needs, human development, and human rights.

The approach is rooted in people-centred principles and promotes cooperation between the nation and the state to achieve mutually beneficial outcomes. It enhances the capabilities of individuals and communities, empowering and protecting them to survive and to cope with threats and conditions that inhibit their ability to live in freedom, peace, and safety.

Jacobs (2016) also maintains that the concept of peace must be based on a comprehensive, integrated, and human-centred approach.

Conclusion and recommendations

Development signifies progress and positive change in the living standards of people. The links between security and development are closely related to the connections between poverty, underdevelopment, and civil strife. Conflict and violent protests erupt when basic human needs are not met and when people are unable to generate livelihoods. Development promotes lasting peace, sustains security, and ensures political stability.

That being said, establishing the nexus is complicated due to the broadness of the concept of 'human security' and the ambiguity inherent in its definition. However, without security and peace, progress in human well-being will never be realised. The narrow view of security is being challenged by ever-increasing and changing socio-economic development systems, and this calls for a multifaceted approach.

Human security, as an approach and lever for transformative programmes, creates opportunities for protection and freedom from pervasive threats to people's rights, safety, and well-being. Human security, as the helm for peace, security, and socio-economic development, entails adopting measures that prevent exposure to risk and vulnerability, and emphasises taking remedial action to prevent conflicts and other social ills. The approach views both the individual and the state as role players in the attainment of security, peace, and development.

Human security prioritises individuals and recognises the role of the state in peacebuilding, conflict management, and resolution. These are seen as critical in processes aimed at developing communities and implementing poverty reduction programmes. As a steering mechanism for peace, security, and socio-economic development, human security is considered a capability-based approach that empowers and enhances people's ability to achieve self-worth and self-respect—the core of human dignity.

However, it is noted that the notion of human security is difficult to put into practice, particularly in policy formulation and implementation. A clear set of guidelines, including measures and indicators, is needed to establish a broader and more effective means of achieving security, such as in health, economics, food, and other basic human needs. Shortcomings noted include the demystification of the concept and the need for a clearer definition. More needs to be done in terms of measurement and monitoring, rather than just theorising about the nature of security.

A sustainable and effective national security strategy must consider human security as a multidimensional and multifaceted approach. Threats to human security are diverse and dynamic, changing with time, space, and context. Therefore, more research still needs to be conducted to determine the value of the human security approach within the peace and socio-economic development context.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

Acharya, A., Singhdeo, S.K. and Rajaretnam, M. 2011. Introduction: Human Security from Concept to Practice. In A. Acharya., S.K. Singhdeo and M. Rajaretnam (eds). *Human Security: From Concept to Practice: Case Studies from Northeast India and Orissa* (pp. 1-12). New Jersey: World Scientific Publishing.

Africa, S. 2015. Human Security in South Africa. *Strategic Review for Southern Africa,* 37 (1): 178-189. Available from : https://repository.up.ac.za/bitstream/handle/2263/52175/Africa_Human_2015.pdf?sequence=1

Ahsan Ullah, A.K.M. 2016. Rohingya crisis in Myanmar: Seeking justice for the "stateless". *Journal of Contemporary Criminal Justice*, *32*(3): 285-301. https://doi.org/10.1177/1043986216660811

Alence, R and Pitcher, A. 2019. Resisting State Capture in South Africa. *Journal of Democracy*, 30 (4): 5-19. https://doi.org/10.1353/jod.2019.0065.

Alkire, S. 2005. Why the capability approach? *Journal of Human Development*, 6 (1): 115-131. Available from : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2118610.

Andersen-Rodgers, D., and Crawford, K. F. (2018). Human Security: Theory and Action. New York: Rowman & Littlefield.

Appiah, J.A. 2018. Africa Peace and Security Architecture: reflections on over a decade of promoting peace and security in Africa. *Africa Insight*, *47*(4): 29-39. Available from : https://www.ajol.info/index.php/ai/article/view/178020.

Asaka, J.O. 2018. *Transformations in Conservation Governance and Implications for Human Security: The Case of Kenya's Northern Rangelands.* (Doctoral dissertation). Boston: University of Massachusetts.

Bhandari, M.P. 2024. What is next for the sustainable development goals, what are the challenges concerning SDG 10—reduced inequalities?. *Sustain Earth Reviews*, 7, 23: 1-5. Available from : https://sustainableearthreviews.biomedcentral.com/articles/10.1186/s42055-024-00093-8.

Boshkoska, M. 2017. Social and Economic Aspects of the Human Security Concept. *Ekonomski horizonti*, 19 (1): 61-74. chrome- Available from : https://scispace.com/pdf/social-and-economic-aspects-of-the-human-security-concept-5a09fbh2bb.pdf.

Brownlee, K., and Cruft, R. 2024. Human Rights. *Oxford Research Encyclopedia of Politics.* Retrieved 19 Mar. 2025, Available from : https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-2035.

Butcher, C. and Hallward, M.C., 2016. Bridging the gap between human rights and peace: An analysis of NGOs and the United Nations Human Rights Council. *International Studies Perspectives*, *18*(1): 81-109. Available from : https://digitalcommons.kennesaw.edu/facpubs/4081/

Cohen, E.A. 2019. *Citizens and soldiers: The dilemmas of military service*. Cornell University Press.

Dinshak, L.D. and Danfulani, W.A. (2018). A Theoretical Framework for Human Security in West Africa: An Assessment of the Critical Human Security Theory. *FULafia Journal of Social Sciences,* 1(3): 59-70. Available from : https://www.researchgate.net/publication/339796381_A_THEORETICAL_FRAMEWORK_FOR_HUMAN_SECURITY_IN_WEST_AFRICA_DINSHAK_LUKA_DAJAHAR_WALNSHAK_ALHERI_DANFULANI

Esterhuyse, A. 2016. Human security and the conceptualisation of South African defence: Time for a reappraisal. *Strategic Review for Southern Africa*, *38*(1): 29-48. https://doi.org/10.35293/srsa.v38i1.276

Fuo, O and Du Plessis, A. (2015). In the face of judicial deference: Taking the "minimum core" of socio-economic rights to the local government sphere. *Law, Democracy and Development*, 19, 01-28.

Gasper, D. 2010. The idea of human security. In K. O'Brien, A.L. St. Clair &B. Kristoffersen (eds.). *Climate Change, Ethics and Human Security* (pp. 23-46). Cambridge: Cambridge University Press.

Habiyaremye, A., King, N.A., and Tregenna, F. (2022). *Innovation and socio-economic development challenges in South Africa: An overview of indicators and trends*. SARChI Industrial Development Working Paper Series WP 2022-03. SARChI Industrial Development, University of Johannesburg.

Hama, H.H. 2017. State Security, Societal Security, and Human Security, *Journal of International Relations*, 21(1), 1–19. https://doi.org/10.1177/0973598417706591.

Harris, B., Goudge, J., Ataguba, J.E., McIntyre, D., Nxumalo, N., Jikwana, S. and Chersich, M. 2011. Inequities in access to health care in South Africa. *Journal of public health policy*, 32(1), 102-123. https://doi.org/10.1057/jphp.2011.35.

Holcombe, S.H and Howard, M. 2019. Drawing Lessons from Reflection and Practice. In S.H. Holcombe and M. Howard (eds). *Practicing Development: Upending Assumptions for Positive Change*. A Kumarian Press Book.

Homolar, A. 2015. Human Security Benchmarks: governing human wellbeing at a distance. *Review of International Studies*. Vol 4: 843-863. https://doi.org/10.1017/s0260210515000352.

International Covenant on Civil and Political Rights, adopted Dec. 19, 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976).

International Covenant on Economic, Social and Cultural Rights, adopted 16 Dec. 1966,993 U.N.T.S.3 (entered into force 3 Jan. 1976), G.A. Res. 2200 (XXI), 21U.N. GAOR Supp. (No.16) at 49, U.N. Doc. A/6316 (1966).

Jacobs, G. 2016. Integrated Approach to Peace and Human Security in the 21st Century. *CADMUS.* Vol. 3 (1): 48-70. Available from : https://www.cadmusjournal.org/node/581.

Jamshidi, Maryam, Whose Security Matters? (August 15, 2022). 116 AJIL UNBOUND 236 (2022), Available at SSRN: Available from : https://ssrn.com/abstract=4190554

Johansson, V. 2015. The Security and Development Nexus: A Policy Analysis.

Jooma, M.B. 2005. We can't eat the constitution. Transformation and the socio-economic reconstruction of Burundi. *Institute for Security Studies Papers*, (106):16-16. Available from : https://issafrica.org/research/papers/we-cant-eat-the-constitution-transformation-and-the-socio-economic-reconstruction-of-burundi

Kaldor, M. and Salmon, A. 2006. Military Force and European Strategy. *Survival*, *48*(1): 19-34. Available from : http://eprints.lse.ac.uk/id/eprint/51685

Langenhove, L.V. 2004. *Regionalising human security in Africa. UNU-CRIS Occasional Papers 0-2004/8.* Available from : https://collections.unu.edu/eserv/unu:7175/O-2004-8.pdf

Leaning, J. and Arie, S. 2000. Human security: A framework for assessment in conflict and transition. *Washington: United States Agency for International Development/Complex Emergency*

Response and Transition Initiative.

Mastrojeni, G. (2017). Peace, security, land and sustainable development. UNCCD Global Land Outlook Working Paper.

Mawdsley, J. 2019. Europe and the human security agenda. *Contemporary European Security*, (1st ed.). Routledge.

Mayosi, B. M. and Benatar, S. R. (2014). Health and health care in South Africa—20 years after Mandela. *New England Journal of Medicine*, 371(14): 1344-1353. Available from : https://www.nejm.org/doi/full/10.1056/NEJMsr1405012

Newman, E. 2021. Covid-19: A human security analysis. *Global Society,* 1-24. Available from : https://www.researchgate.net/publication/357412361_Covid-19_A_Human_Security_Analysis

Ngira, D. 2018. The Nexus Between Human Security and Human Rights: Some Wayside Remarks. Journalofcmsd, 2(2).

O'Brien, R and Williams, M. 2016. Global Political Economy: evolution and dynamics (5th ed). New York: Palgrave (Chapter 14: Security), 279-298. Bloomsbury Publishing.

Orago, N.W. 2017. Socio-economic development and resource redistribution as tools for conflict prevention and post-conflict peace building in fragile societies: A comparative analysis of Burundi and Rwanda. *Global Campus Human Rights Journal*, 226-258.

Pavleski, A. 2023. The nexus between human security and human rights. *Rocznik Administracji Publicznej*, 9, 295–308. Available from : https://www.researchgate.net/publication/374939881_The_nexus_between_human_security_and_human_rights

Republic of South Africa. 1996. *Constitution of the South Africa*. Pretoria: Government Printers.

Robeyns, I. 2017. *Wellbeing, Freedom and Social Justice the Capability Approach Re-Examined*. Cambridge: Open Book Publishers.

Robinson, C. 2006. Whose Security? Integration and Integrity in EU Policies for Security and Development. In S. Klingebiel (Ed). *New Interfaces between Security and Development: changing concepts and approaches.* Bonn: Deutsches Institut für Entwicklungspolitik. Bonn. 69-92.

Scanlon, H. and Murithi, T. 2006. The United Nations and Africa: Peace, Development and Human Security.

Stewart, F., 2004. Development and security. *Conflict, Security & Development*, *4*(3): 261-288. Available from : https://assets.publishing.service.gov.uk/media/57a08cd140f0b652dd00159c/wp3.pdf

Tardy, T. 2019. The European Union and UN Peace Operations: What Global–Regional Peace and Security Partnership?. In C. de Coning & M. Peter (eds). *United Nations Peace Operations in a Changing Global Order* (pp. 231-251). Cham: Palgrave Macmillan.

Taylor, V. 2002. Socio-economic rights: essential for human security: closing address. *ESR Review: Economic and Social Rights in South Africa,* 3(1): 31-32.

Tschirgi, N. 2006. Security and development policies: Untangling the relationship. *New interfaces between security and development*, 39.

United Nations. 1994. *Human Development Report 1994.* New York: United Nations.

United Nations. 2015. *Transforming our World: The 2030 Agenda for Sustainable Development. General Assembley 70 session*. New York: United Nations.

United Nations. 2019. *The Sustainable Development Goals Report 2019.* Available from : https://unstats.un.org/sdgs/indicators/regional-groups. (Accessed on 17 September 2019).

United Nations. 2022. *The Sustainable Development Goals Report 2022.* New York: United Nations.

Vietti, F and Scribner, T. 2013. Human insecurity: Understanding international migration from a human security perspective. *Journal on Migration and Human Security*, 1(1): 17-31. https://doi.org/10.14240/jmhs.v1i1.6.

Williamson, S. (2024). Impact of Political Instability on Social Development. *International Journal of Humanity and Social Sciences*, 3(1), 56-77. https://doi.org/10.47941/ijhss.2080.

Zondi, S. 2017. Comprehensive and holistic human security for a post-colonial southern Africa: a conceptual framework. *Strategic Review for Southern Africa,* 39 (1):185-210. Available from : http://hdl.handle.net/2263/64759

Zondi, S. 2021. The Qualitative Review of Human Security in South Africa: A Four Levels Analysis. *Strategic Review for Southern Africa*, 43(2): 150-175. https://doi.org/10.35293/srsa.v43i2.341

Список використаних джерел

Acharya, A., Singhdeo, S.K. and Rajaretnam, M. 2011. Introduction: Human Security from Concept to Practice. In A. Acharya., S.K. Singhdeo and M. Rajaretnam (eds). *Human Security: From Concept to Practice: Case Studies from Northeast India and Orissa* (pp. 1-12). New Jersey: World Scientific Publishing.

Africa, S. 2015. Human Security in South Africa. *Strategic Review for Southern Africa,* 37 (1): 178-189. Available from : https://repository.up.ac.za/bitstream/handle/2263/52175/Africa_Human_2015.pdf?sequence=1

Ahsan Ullah, A.K.M. 2016. Rohingya crisis in Myanmar: Seeking justice for the "stateless". *Journal of Contemporary Criminal Justice*, *32*(3): 285-301. https://doi.org/10.1177/1043986216660811

Alence, R and Pitcher, A. 2019. Resisting State Capture in South Africa. *Journal of Democracy*, 30 (4): 5-19. https://doi.org/10.1353/jod.2019.0065.

Alkire, S. 2005. Why the capability approach? *Journal of Human Development*, 6 (1): 115-131. Available from : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2118610.

Andersen-Rodgers, D., and Crawford, K. F. (2018). Human Security: Theory and Action. New York: Rowman & Littlefield.

Appiah, J.A. 2018. Africa Peace and Security Architecture: reflections on over a decade of promoting peace and security in Africa. *Africa Insight*, *47*(4): 29-39. Available from : https://www.ajol.info/index.php/ai/article/view/178020.

Asaka, J.O. 2018. *Transformations in Conservation Governance and Implications for Human Security: The Case of Kenya's Northern Rangelands.* (Doctoral dissertation). Boston: University of Massachusetts.

Bhandari, M.P. 2024. What is next for the sustainable development goals, what are the challenges concerning SDG 10—reduced inequalities?. *Sustain Earth Reviews*, 7, 23: 1-5. Available from : https://sustainableearthreviews.biomedcentral.com/articles/10.1186/s42055-024-00093-8.

Boshkoska, M. 2017. Social and Economic Aspects of the Human Security Concept. *Ekonomski horizonti*, 19 (1): 61-74. chrome- Available from : https://scispace.com/pdf/social-and-economic-aspects-of-the-human-security-concept-5a09fbh2bb.pdf.

Brownlee, K., and Cruft, R. 2024. Human Rights. *Oxford Research Encyclopedia of Politics.* Retrieved 19 Mar. 2025, Available from : https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-2035.

Butcher, C. and Hallward, M.C., 2016. Bridging the gap between human rights and peace: An analysis of NGOs and the United Nations Human Rights Council. *International Studies Perspectives*, *18*(1): 81-109. Available from : https://digitalcommons.kennesaw.edu/facpubs/4081/

Cohen, E.A. 2019. *Citizens and soldiers: The dilemmas of military service*. Cornell University Press.

Dinshak, L.D. and Danfulani, W.A. (2018). A Theoretical Framework for Human Security in West Africa: An Assessment of the Critical Human Security Theory. *FULafia Journal of Social Sciences,* 1(3): 59-70. Available from : https://www.researchgate.net/publication/339796381_A_THEORETICAL_FRAMEWORK_FOR_HUMAN_SECURITY_IN_WEST_AFRICA_DINSHAK_LUKA_DAJAHAR_WALNSHAK_ALHERI_DANFULANI

Esterhuyse, A. 2016. Human security and the conceptualisation of South African defence: Time for a reappraisal. *Strategic Review for Southern Africa*, *38*(1): 29-48. https://doi.org/10.35293/srsa.v38i1.276

Fuo, O and Du Plessis, A. (2015). In the face of judicial deference: Taking the "minimum core" of socio-economic rights to the local government sphere. *Law, Democracy and Development*, 19, 01-28.

Gasper, D. 2010. The idea of human security. In K. O'Brien, A.L. St. Clair &B. Kristoffersen (eds.). *Climate Change, Ethics and Human Security* (pp. 23-46). Cambridge: Cambridge University Press.

Habiyaremye, A., King, N.A., and Tregenna, F. (2022). *Innovation and socio-economic development challenges in South Africa: An overview of indicators and trends*. SARChI Industrial Development Working Paper Series WP 2022-03. SARChI Industrial Development, University of Johannesburg.

Hama, H.H. 2017. State Security, Societal Security, and Human Security, *Journal of International Relations*, 21(1), 1–19. https://doi.org/10.1177/0973598417706591.

Harris, B., Goudge, J., Ataguba, J.E., McIntyre, D., Nxumalo, N., Jikwana, S. and Chersich, M. 2011. Inequities in access to health care in South Africa. *Journal of public health policy*, 32(1), 102-123. https://doi.org/10.1057/jphp.2011.35.

Holcombe, S.H and Howard, M. 2019. Drawing Lessons from Reflection and Practice. In S.H. Holcombe and M. Howard (eds). *Practicing Development: Upending Assumptions for Positive Change*. A Kumarian Press Book.

Homolar, A. 2015. Human Security Benchmarks: governing human wellbeing at a distance. *Review of International Studies*. Vol 4: 843-863. https://doi.org/10.1017/s0260210515000352.

International Covenant on Civil and Political Rights, adopted Dec. 19, 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976).

International Covenant on Economic, Social and Cultural Rights, adopted 16 Dec. 1966,993 U.N.T.S.3 (entered into force 3 Jan. 1976), G.A. Res. 2200 (XXI), 21U.N. GAOR Supp. (No.16) at 49, U.N. Doc. A/6316 (1966).

Jacobs, G. 2016. Integrated Approach to Peace and Human Security in the 21st Century. *CADMUS.* Vol. 3 (1): 48-70. Available from : https://www.cadmusjournal.org/node/581.

Jamshidi, Maryam, Whose Security Matters? (August 15, 2022). 116 AJIL UNBOUND 236 (2022), Available at SSRN: Available from : https://ssrn.com/abstract=4190554

Johansson, V. 2015. The Security and Development Nexus: A Policy Analysis.

Jooma, M.B. 2005. We can't eat the constitution. Transformation and the socio-economic reconstruction of Burundi. *Institute for Security Studies Papers*, (106):16-16. Available from : https://issafrica.org/research/papers/we-cant-eat-the-constitution-transformation-and-the-socio-economic-reconstruction-of-burundi

Kaldor, M. and Salmon, A. 2006. Military Force and European Strategy. *Survival*, *48*(1): 19-34. Available from : http://eprints.lse.ac.uk/id/eprint/51685

Langenhove, L.V. 2004. *Regionalising human security in Africa. UNU-CRIS Occasional Papers 0-2004/8.* Available from : https://collections.unu.edu/eserv/unu:7175/O-2004-8.pdf

Leaning, J. and Arie, S. 2000. Human security: A framework for assessment in conflict and transition. *Washington: United States Agency for International Development/Complex Emergency*

Response and Transition Initiative.

Mastrojeni, G. (2017). Peace, security, land and sustainable development. UNCCD Global Land Outlook Working Paper.

Mawdsley, J. 2019. Europe and the human security agenda. *Contemporary European Security*, (1st ed.). Routledge.

Mayosi, B. M. and Benatar, S. R. (2014). Health and health care in South Africa—20 years after Mandela. *New England Journal of Medicine*, 371(14): 1344-1353. Available from : https://www.nejm.org/doi/full/10.1056/NEJMsr1405012

Newman, E. 2021. Covid-19: A human security analysis. *Global Society,* 1-24. Available from : https://www.researchgate.net/publication/357412361_Covid-19_A_Human_Security_Analysis

Ngira, D. 2018. The Nexus Between Human Security and Human Rights: Some Wayside Remarks. Journalofcmsd, 2(2).

O'Brien, R and Williams, M. 2016. Global Political Economy: evolution and dynamics (5th ed). New York: Palgrave (Chapter 14: Security), 279-298. Bloomsbury Publishing.

Orago, N.W. 2017. Socio-economic development and resource redistribution as tools for conflict prevention and post-conflict peace building in fragile societies: A comparative analysis of Burundi and Rwanda. *Global Campus Human Rights Journal*, 226-258.

Pavleski, A. 2023. The nexus between human security and human rights. *Rocznik Administracji Publicznej*, 9, 295–308. Available from : https://www.researchgate.net/publication/374939881_The_nexus_between_human_security_and_human_rights

Republic of South Africa. 1996. *Constitution of the South Africa*. Pretoria: Government Printers.

Robeyns, I. 2017. *Wellbeing, Freedom and Social Justice the Capability Approach Re-Examined*. Cambridge: Open Book Publishers.

Robinson, C. 2006. Whose Security? Integration and Integrity in EU Policies for Security and Development. In S. Klingebiel (Ed). *New Interfaces between Security and Development: changing concepts and approaches.* Bonn: Deutsches Institut für Entwicklungspolitik. Bonn. 69-92.

Scanlon, H. and Murithi, T. 2006. The United Nations and Africa: Peace, Development and Human Security.

Stewart, F., 2004. Development and security. *Conflict, Security & Development*, *4*(3): 261-288. Available from : https://assets.publishing.service.gov.uk/media/57a08cd140f0b652dd00159c/wp3.pdf

Tardy, T. 2019. The European Union and UN Peace Operations: What Global–Regional Peace and Security Partnership?. In C. de Coning & M. Peter (eds). *United Nations Peace Operations in a Changing Global Order* (pp. 231-251). Cham: Palgrave Macmillan.

Taylor, V. 2002. Socio-economic rights: essential for human security: closing address. *ESR Review: Economic and Social Rights in South Africa,* 3(1): 31-32.

Tschirgi, N. 2006. Security and development policies: Untangling the relationship. *New interfaces between security and development*, 39.

United Nations. 1994. *Human Development Report 1994.* New York: United Nations.

United Nations. 2015. *Transforming our World: The 2030 Agenda for Sustainable Development. General Assembley 70 session*. New York: United Nations.

United Nations. 2019. *The Sustainable Development Goals Report 2019.* Available from : https://unstats.un.org/sdgs/indicators/regional-groups. (Accessed on 17 September 2019).

United Nations. 2022. *The Sustainable Development Goals Report 2022.* New York: United Nations.

Vietti, F and Scribner, T. 2013. Human insecurity: Understanding international migration from a human security perspective. *Journal on Migration and Human Security*, 1(1): 17-31. https://doi.org/10.14240/jmhs.v1i1.6.

Williamson, S. (2024). Impact of Political Instability on Social Development. *International Journal of Humanity and Social Sciences*, 3(1), 56-77. https://doi.org/10.47941/ijhss.2080.

Zondi, S. 2017. Comprehensive and holistic human security for a post-colonial southern Africa: a conceptual framework. *Strategic Review for Southern Africa,* 39 (1):185-210. Available from : http://hdl.handle.net/2263/64759

Zondi, S. 2021. The Qualitative Review of Human Security in South Africa: A Four Levels Analysis. *Strategic Review for Southern Africa*, 43(2): 150-175. https://doi.org/10.35293/srsa.v43i2.341

Аналіз нормативно-правових документів з внутрішнього аудиту

Analysis of regulatory and legal documents on internal audit

Олександр Шпиталь
ад'юнкт, e-mail: shpital777@ukr.net, ORCID: 0009-0003-5261-1954
Національний університет оборони України, м. Київ, Україна

Oleksandr Shpytal
PhD student, e-mail: shpital777@ukr.net, ORCID: 0009-0003-5261-1954
National Defense University of Ukraine, Kyiv, Ukraine

Received: April 16, 2025 | Revised: April 28, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.22

Мета роботи: проаналізувати нормативно-правові документи з внутрішнього аудиту на відповідність міжнародним стандартам, виявити проблемні аспекти в нормативному забезпеченні та визначити напрями його вдосконалення.

Метод дослідження: методи системного аналізу, синтезу, дедукції та індукції, аналогії та порівняння.

Результати дослідження: систематизовано та проаналізовано нормативні документи з внутрішнього аудиту, зосереджено увагу на їх відповідності міжнародним стандартам. Виявлено проблемні аспекти нормативного забезпечення внутрішнього аудиту. Визначено напрями вдосконалення нормативного регулювання внутрішнього аудиту в контексті стратегії реформування системи управління державними фінансами.

Теоретична цінність дослідження: результати дослідження сприяють науковому розумінню питань організації та функціонування внутрішнього аудиту, а також фундаментальних принципів міжнародних стандартів, що забезпечують ефективність внутрішнього аудиту. Запропоновано заходи трансформації внутрішнього аудиту, які можуть бути використані для вдосконалення нормативно-правових документів з внутрішнього аудиту.

Практична цінність дослідження: результати дослідження можуть бути використані для аналізу стану організації та функціонування підрозділів внутрішнього аудиту, їх основних внутрішніх документів з питань проведення внутрішнього аудиту

Цінність дослідження: систематизація теоретичних, організаційно-методологічних засад проведення внутрішнього аудиту, виявлення прогалин у нормативно-правовому регулюванні та формування напрямів його вдосконалення, сприяння гармонізації національних і міжнародних стандартів. Матеріали дослідження є цінними для підвищення якості нормативних документів з внутрішнього аудиту. Висновки та рекомендації дослідження можуть бути використані під час розроблення навчальних програм та методичних матеріалів з внутрішнього аудиту для закладів вищої освіти і центрів підвищення кваліфікації.

Обмеження дослідження/Майбутні дослідження: аналіз нормативно-правової бази обмежений періодом до квітня 2025 року, що не дає змоги врахувати можливі майбутні зміни в нормативно-правових документах з внутрішнього аудиту. Перспективним напрямом майбутніх досліджень є удосконалення наявних або розроблення нових методологічних підходів до оцінювання для надання впевненості.

Тип статті: теоретичний.

Purpose: the aim is to analyze regulatory documents on internal audit for compliance with international standards, identify problematic aspects in regulatory support and determine areas for its improvement.

Methods applied: methods of system analysis, synthesis, deduction and induction, analogy and comparison.

Findings: regulatory documents on internal audit were systematized and analyzed, focusing on their compliance with international standards. Problematic aspects of regulatory support for internal audit were identified. Areas for improving regulatory regulation of internal audit were identified in the context of the strategy for reforming the public finance management system.

Theoretical applications: the results of the study contribute to a scientific understanding of the issues of organization and functioning of internal audit, as well as the fundamental principles of international standards that ensure the effectiveness of internal audit. Measures for the transformation of internal audit are proposed, which can be used to improve regulatory documents on internal audit.

Practical applications: the results of the study can be used to analyze the state of the organization and functioning of internal audit units, their main internal documents on internal audit.

Value: systematization of theoretical, organizational and methodological principles of internal audit, identification of gaps in regulatory and legal regulation and formation of directions for its improvement, promotion of harmonization of national and international standards. The study materials are valuable for improving the quality of regulatory documents on internal audit. The conclusions and recommendations of the study can be used when developing curricula and methodological materials on internal audit for higher education institutions and centers for advanced training.

Research limitations/Future research: the analysis of the regulatory and legal framework is limited to the period until April 2025, which does not allow taking into account possible future changes in regulatory and legal documents on internal audit. A promising direction for future research is to improve existing or develop new methodological approaches to assessment to provide assurance.

Papertype: theoretical.

Ключові слова: внутрішній аудит, стандарти внутрішнього аудиту, ефективність.

Key words: internal audit, internal audit standards, efficiency.

Вступ

Забезпечення фінансової стійкості, ефективності використання державних ресурсів, які будуть залучені для гарантування національної безпеки України, завдяки підвищенню прозорості і впровадженню сучасного фінансового менеджменту необхідними складовими реалізації Стратегії національної безпеки України [1].

Побудову ефективної системи управління фінансами в публічному секторі економіки визначено основною метою Стратегії реформування системи управління державними фінансами [2].

Сучасним пріоритетом є створення дієвого та ефективного механізму фінансового контролю в публічному секторі економіки, побудованого на фундаментальних міжнародних принципах і кращих практиках. Це надзвичайно важливий крок у процесі впровадження реформи управління державними фінансами.

Належний нагляд за дотриманням законності, а також ефективне (результативне й економне) використання державних ресурсів забезпечує дієва система внутрішнього фінансового контролю в публічному секторі [3].

Одним із ключових напрямів досягнення стратегічної мети реформування системи державного внутрішнього фінансового контролю вважаємо підвищення ефективності, спроможності і незалежності внутрішнього аудиту. Зазначене передбачає переорієнтацію аудиторської діяльності на системний аналіз та оцінювання ефективності внутрішнього контролю, ступеня виконання завдань (функцій) і забезпечення досягнення поставлених цілей [2].

Таким чином, побудова ефективної системи внутрішнього аудиту є невід'ємною складовою сучасної системи внутрішнього фінансового контролю в публічному секторі економіки України.

Водночас за результатами аналізу звітності стану функціонування внутрішнього аудиту в державних установах за 2023 та 2024 роки Міністерство фінансів України засвідчило наявність недоліків і проблемних питань в організації та проведенні внутрішнього аудиту, що потребує вжиття заходів для їх вирішення [4].

Теоретичні основи дослідження

Теоретичними основами дослідження є нормативно-правові документи з внутрішнього аудиту [5-16].

Фундаментальні теоретичні основи організаційно-правових засад та проблемні аспекти внутрішнього аудиту активно досліджували багато учених, науковців, економістів: Т. Каменська [17;18], О. Пушкарьова [19], А. Семенець [20], О. Філозоп [21], Д. Калінкін [22], О. Редько [23], О. Лебединська [24], Р. Рудніцька [25;26], О. Мельник [27], О. Ружанський [28] та ін. Проте, деякі аспекти щодо посилення ефективності, спроможності та незалежності підрозділів внутрішнього аудиту залишаються неврегульованими та потребують проведенню додаткового дослідження.

Постановка проблеми

Реформування системи державного внутрішнього фінансового контролю передбачає адаптацію національних нормативно-правових документів до міжнародних стандартів і кращих практик. Актуальності набуває питання посилення ефективності внутрішнього аудиту, що має на меті перехід від традиційних підходів до проведення внутрішнього аудиту, орієнтованого виключно на оцінювання відповідності законодавству, до системного аналізу та стратегічного оцінювання ефективності, забезпечення переорієнтації на вдосконалення діяльності державної установи [2].

Внутрішній аудит є ключовим інструментом підвищення ефективності управління державними ресурсами, забезпечення прозорості і посилення управлінської підзвітності.

Незважаючи на значний прогрес у розвитку внутрішнього аудиту, далеко не всі проблемні питання та виявлені недоліки вирішені, що продовжує негативно впливати на його спроможність та ефективність.

Так, за результатами проведеного Мінфіном аналізу звітності про стан функціонування внутрішнього аудиту в державних установах за 2023 та 2024 роки та результатами

проведеного Програмою SIGMA оцінювання стану справ у системі державного управління України у 2023 році підтверджено наявність недоліків і проблем у функціонуванні внутрішнього аудиту, що впливає на його спроможність та ефективність [4], зокрема щодо незабезпечення:

підрозділів внутрішнього аудиту кадрами через неукомплектованість і плинність кадрів відповідної кваліфікації;

функціональної незалежності підрозділів внутрішнього аудиту;

застосування ризик-орієнтованого підходу до планування діяльності з внутрішнього аудиту;

належної якості внутрішнього аудиту через слабкий зв'язок між рекомендаціями та зібраними аудиторськими доказами. Аудиторські дослідження та надані рекомендації не були спрямовані на удосконалення діяльності державних органів, здебільшого орієнтовані на перевірку відповідності законодавству, а не системне оцінювання та аналіз системи внутрішнього контролю.

Зазначені недоліки та проблеми призводять до зниження ефективності функціонування внутрішнього аудиту, формального підходу до проведення аудиторських досліджень і недостатнього впливу результатів аудиту на процеси управління.

Через вплив вказаних недоліків і проблем на спроможність та ефективність внутрішнього аудиту необхідно вжити заходи для підвищення якості і незалежності внутрішнього аудиту в системі державних органів, його подальшого розвитку з урахуванням міжнародних стандартів і кращих практик.

Особливо гострими залишаються питання нормативного забезпечення незалежності внутрішніх аудиторів, методології оцінювання системи управління, процедур проведення аудиторських досліджень, документування їх результатів та контролю за виконанням аудиторських рекомендацій. Реформа державного управління і процеси децентралізації створюють нові виклики для системи внутрішнього аудиту, що потребує оновлення та вдосконалення нормативно-правової бази. Водночас недостатньо дослідженими залишаються питання адаптації принципів міжнародних стандартів та кращих практик внутрішнього аудиту до національних особливостей системи управління.

Таким чином, потрібно проаналізувати нормативно-правові документи внутрішнього аудиту, щоб виявити проблемні аспекти нормативного забезпечення та визначити напрями їх вдосконалення з урахуванням міжнародних стандартів.

Методологія дослідження

У проведеному дослідженні застосовано системний підхід до організації та проведення внутрішнього аудиту, що дає змогу розглядати внутрішній аудит як цілісну систему у структурі державного управління. У процесі аналізу нормативно-правової бази використано такі методи: системного аналізу, синтезу, дедукції, індукції, аналогії та порівняння для обробки, систематизації та критичного осмислення нормативно-правових документів з внутрішнього аудиту, порівняння національних нормативно-правових документів з внутрішнього аудиту із міжнародними стандартами і кращими практиками.

Використання цього методичного підходу дало змогу ґрунтовно вивчити проблемні аспекти системи внутрішнього аудиту, сформулювати висновки і окреслити напрями вдосконалення нормативно-правових документів з внутрішнього аудиту.

Результати

У ході дослідження нормативно-правових документів з внутрішнього аудиту встановлено, що, на відміну від зовнішнього аудиту, правові засади та провадження аудиторської діяльності в Україні визначено Законом України "Про аудит фінансової звітності та аудиторську діяльність",

а діяльність з внутрішнього аудиту на рівні окремого закону не регламентована [5].

Нормативне визначення сутності внутрішнього аудиту і вимоги до відповідальності розпорядників бюджетних коштів в особі їх керівників щодо організації та проведення внутрішнього аудиту у своїх установах на законодавчому рівні передбачено частиною третьою статті 26 “Контроль та аудит у бюджетному процесі” глави 4 “Бюджетний процес та його учасники” Бюджетного кодексу України (редакція від 05.03.2025) [7].

Відповідно до положень статті 26 Бюджетного кодексу України Кабінет Міністрів отримує повноваження щодо визначення основних засад здійснення внутрішнього аудиту і порядку утворення підрозділів внутрішнього аудиту. Міністерство фінансів України уповноважене розробляти і затверджувати організаційно-методологічні засади здійснення внутрішнього аудиту, забезпечуючи формування і реалізацію державної політики у сфері внутрішнього фінансового контролю [7].

Поняття сутності “внутрішній аудит” визначено статтею 26 Бюджетного кодексу України як “незалежна, об’єктивна діяльність, що передбачає здійснення аудиторських досліджень (оцінки з надання впевненості) та аудиторського консультування для сприяння розпоряднику бюджетних коштів у досягненні цілей, завдань і конкретних результатів своєї діяльності. Внутрішній аудит сприяє покращенню ефективності і результативності в діяльності розпорядника бюджетних коштів, а також підприємств, установ та організацій, що належать до сфери його управління, шляхом застосування систематичного, послідовного підходу до оцінки і вдосконалення організації та функціонування системи управління, внутрішнього контролю, управління ризиками” (Рис. 1) [7].

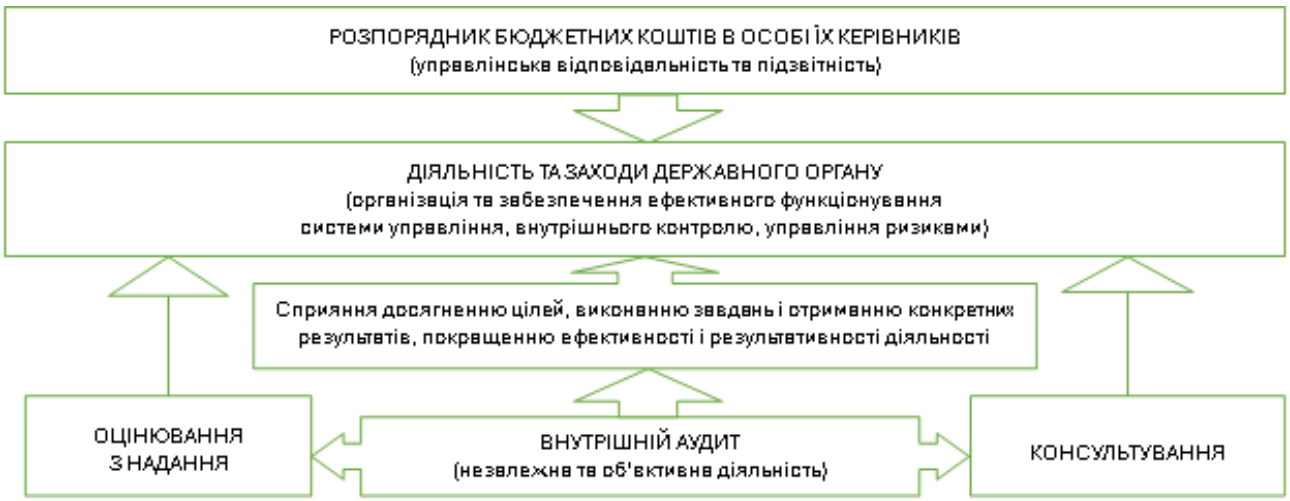


Рисунок 1 – Сутність діяльності з внутрішнього аудиту
Джерело: сформовано автором на основі [7]

Зазначимо, що з 05.03.2025 змінилося трактування сутності внутрішнього аудиту. Аналіз змін у нормативному визначенні порівняно з попередньою редакцією показав, що раніше “внутрішній аудит” було визначено як “діяльність, спрямовану на удосконалення системи управління, внутрішнього контролю, запобігання фактам незаконного, неефективного та нерезультативного використання бюджетних коштів, виникненню помилок чи інших недоліків у діяльності розпорядника бюджетних коштів і підприємств, установ та організацій, що належать до сфери його управління, та яка передбачає надання незалежних висновків і рекомендацій” [7].

Відповідно до оновленої редакції внутрішньому аудиту законодавчо надано статус незалежної та об’єктивної діяльності, у ньому виокремлено два види діяльності внутрішнього

аудиту, а саме “аудиторське дослідження (оцінка з надання впевненості)” та “консультування”, сформовано головну мету внутрішнього аудиту – “сприяння розпоряднику бюджетних коштів у досягненні цілей, завдань і конкретних результатів його діяльності” [7].

Відповідно до Порядку здійснення внутрішнього аудиту та утворення підрозділів внутрішнього аудиту (далі – Порядок) передбачено механізм утворення структурних підрозділів внутрішнього аудиту, окреслено питання їх діяльності, визначено “об’єкт внутрішнього аудиту” як “діяльність державного органу та заходи, які проводять керівники таких органів з метою забезпечення ефективного функціонування системи внутрішнього контролю (дотримання принципів законності й ефективного використання бюджетних коштів та інших активів, досягнення результатів відповідно до встановленої мети, виконання завдань, планів і вимог щодо їх діяльності)” [8].

Водночас відповідно до Міжнародних стандартів внутрішнього аудиту об’єктом внутрішнього аудиту визначено “діяльність, яку перевіряють, предмет завдання внутрішнього аудиту”. Як приклади можна назвати напрям, установу, операцію, функцію, процес чи систему [15].

Порядком визначено основні завдання підрозділу внутрішнього аудиту: “надання керівнику державного органу об'єктивних і незалежних висновків та рекомендацій щодо функціонування системи внутрішнього контролю та її удосконалення; удосконалення системи управління; запобігання фактам незаконного, неефективного та нерезультативного використання бюджетних коштів та інших активів; запобігання виникненню помилок чи інших недоліків у діяльності державного органу, його територіальних органів, підприємств, установ та організацій, що належать до сфери його управління” [8].

Підрозділ внутрішнього аудиту виконує зазначені завдання так: “оцінюванням ефективності функціонування системи внутрішнього контролю; ступеня виконання і досягнення цілей, визначених у стратегічних та річних планах; ефективності планування і виконання бюджетних програм та результатів їх виконання, управління бюджетними коштами; якості надання адміністративних послуг та виконання контрольно-наглядових функцій, завдань, визначених актами законодавства; використання і збереження активів; надійності, ефективності та результативності інформаційних систем і технологій; управління державним майном; правильності ведення бухгалтерського обліку та достовірності фінансової і бюджетної звітності; ризиків, які негативно впливають на виконання функцій і завдань державного органу, його територіальних органів, підприємств, установ та організацій, що належать до сфери його управління” [8].

Провадження внутрішнього аудиту врегульовано обов’язковими правилами та єдиними підходами, що визначені Стандартами внутрішнього аудиту (далі – Стандарти ВА) [9].

Стандарти ВА складаються з двох видів стандартів (рис. 2).

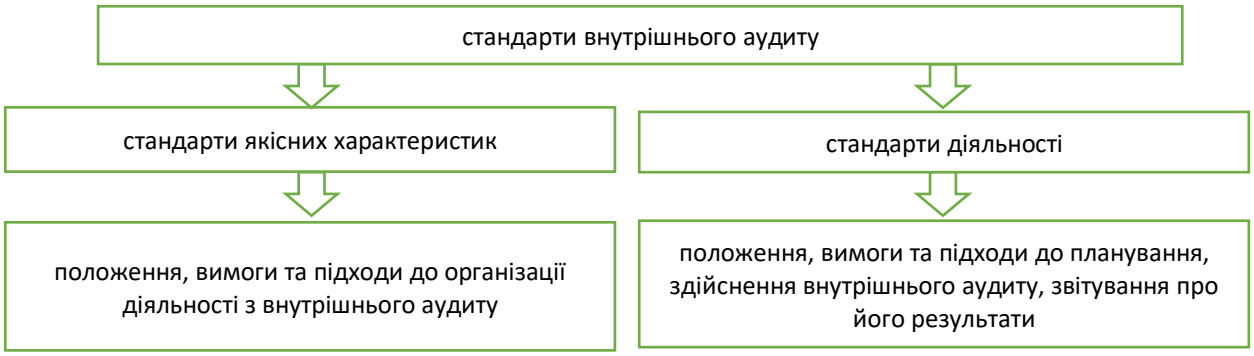


Рисунок 2 – Структура стандартів внутрішнього аудиту
Джерело: сформовано автором на основі [9]

Відповідно до Стандартів ВА повноваження з визначення ключових завдань і функцій підрозділу внутрішнього аудиту, а також встановлення прав та обов'язків його керівника і співробітників разом із вимогами до його незалежності мають бути передбачені внутрішніми документами установи. Ці документи, розроблені безпосередньо керівником підрозділу, мають охоплювати усі аспекти аудиторської діяльності [9].

Аналіз стандартів якісних характеристик показав, що в них міститься детальний перелік вимог до основних нормативних внутрішніх документів з питань аудиту, серед яких “декларація внутрішнього аудиту”, “положення про підрозділ”, “посадові інструкції співробітників”, “програма з підвищення якості аудиту”, а також інших внутрішніх документів, які регулюють аудиторську діяльність [9].

Крім того, вимоги Стандартів ВА надають керівнику підрозділу внутрішнього аудиту повноваження щодо розроблення методологічних документів до проведення внутрішнього аудиту. Під час створення внутрішніх документів враховують специфіку діяльності установи, розмір і структуру підрозділу, складність об’єктів аудиту й особливості виконуваних завдань.

У Стандартах ВА визначено поняття незалежності (організаційної і функціональної) та об'єктивності внутрішнього аудиту.

Порівняно з визначеннями, наданими у Міжнародних стандартах внутрішнього аудиту [15], виявлено помітні розбіжності (табл. 1).

Таблиця 1 – Порівняння визначень термінів “незалежність” та “об’єктивність”

Стандарти внутрішнього аудиту	Глобальні стандарти внутрішнього аудиту
“Організаційна незалежність – пряме підпорядкування та підзвітність підрозділу внутрішнього аудиту керівнику установи”. “Функціональна незалежність – недопущення виконання працівниками підрозділу внутрішнього аудиту функцій, не пов’язаних зі здійсненням внутрішнього аудиту”	“Незалежність – свобода від умов, що можуть порушити здатність функції внутрішнього аудиту виконувати зобов’язання з внутрішнього аудиту неупереджено”
“Об’єктивність вимагає від працівників підрозділу внутрішнього аудиту провадити свою діяльність неупереджено, без формування свого висновку під впливом третіх осіб та уникати конфлікту інтересів”	“Об’єктивність – неупереджене ментальне ставлення, яке дозволяє внутрішнім аудиторам робити професійні судження, виконувати свої обов’язки та досягати мети внутрішнього аудиту без компромісів”

Стандарти діяльності внутрішнього аудиту визначають сутність проведення внутрішнього аудиту (рис. 3).

Моральні та етичні засади професійної діяльності співробітників підрозділу внутрішнього аудиту, а також основні норми їх поведінки закріплено у Кодексі етики працівників підрозділу внутрішнього аудиту [10].

Також передбачена обов’язкова сертифікація працівників підрозділів внутрішнього аудиту [11], яку проводять відповідно до встановленого порядку [12].

Щорічно підрозділ внутрішнього аудиту за встановленою формою звітує перед Міністерством фінансів України про результати своєї діяльності відповідно до встановленої Інструкції [13].

Зовнішнє оцінювання функціювання внутрішнього аудиту (іншими словами, зовнішнє оцінювання якості внутрішнього аудиту) проводить Міністерство фінансів України відповідно до встановлено порядку [14].



Рисунок 3 – Сутність проведення внутрішнього аудиту
Джерело: сформовано автором на основі [9]

Отже, за результатами аналізу систематизовано та побудовано ієрархічну систему нормативно-правових документів з внутрішнього аудиту (рис. 4). Це вказує на сформованість нормативно-правової бази з внутрішнього аудиту в Україні і забезпечення регулювання його діяльності.

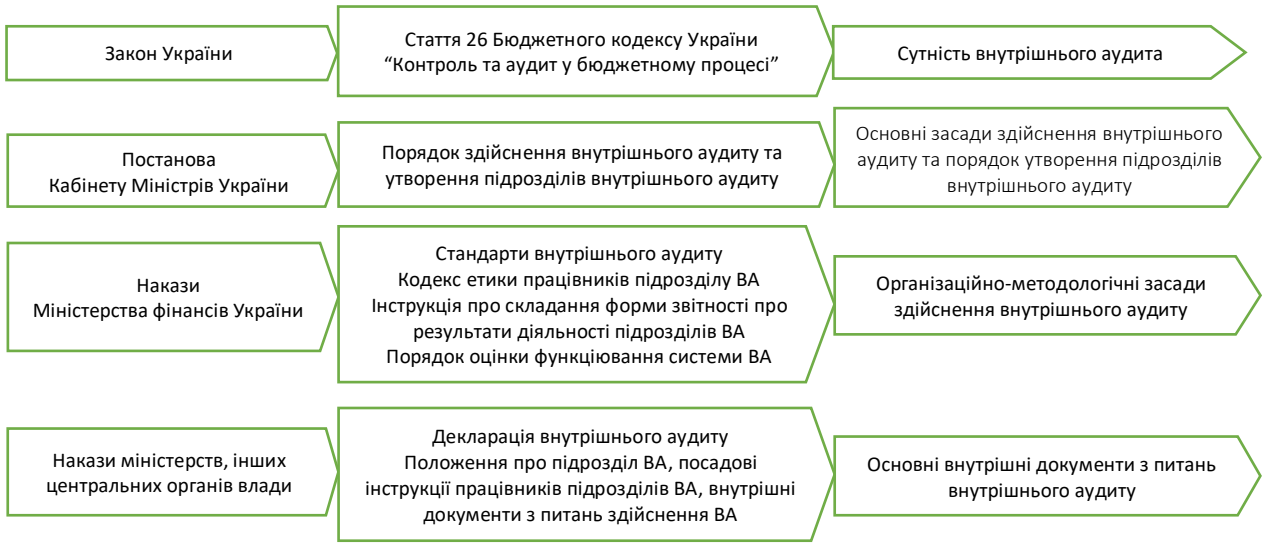


Рисунок 4 – Структура та ієрархія національних нормативних документів з внутрішнього аудиту
Джерело: сформовано автором на основі [7 – 14].

Розвиток системи державного внутрішнього фінансового контролю, у тому числі системи внутрішнього аудиту в публічному секторі економіки, відбувається на підставі

реалізації взятих зобов'язань відповідно до Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, з іншої сторони через гармонізацію з міжнародними стандартами та кращими практиками внутрішнього аудиту [6].

З січня 2025 року набули чинності Глобальні стандарти внутрішнього аудиту [15], які, на відміну від чинних Стандартів ВА, що поділяються на два стандарти (якісних характеристик та діяльності), містять п'ять розділів (принципів – 15 та стандартів – 52), зокрема такі: "Мета внутрішнього аудиту", "Етичне ставлення та професіоналізм", "Нагляд за функцією внутрішнього аудиту", "Управління функцією внутрішнього аудиту" та "Надання послуг внутрішнього аудиту" [15].

Попередня редакція Міжнародних стандартів внутрішнього аудиту структурно включала окремі елементи, наприклад, місію внутрішнього аудиту, кодекс етики та інші компоненти, які викликали плутанину. Сучасні Глобальні стандарти мають уніфіковану структуру, яка допомагає аудиторам послідовно застосовувати найкращі практики у функціях внутрішнього аудиту.

Глобальні стандарти містять нове визначення мети – "внутрішній аудит зміцнює спроможність організації створювати, захищати та підтримувати цінність, надаючи раді та керівництву незалежні, ризик-орієнтовані й об'єктивні аудиторські та консультаційні послуги, аналітичну оцінку та прогнозування" [15], яка надає розуміння цінності внутрішнього аудиту в допомозі організації для успішного досягнення поставлених цілей, перебігу процесів управління, управління ризиками та контролю, ухвалення рішень та забезпечення нагляду, підтримання репутації і довіри серед зацікавлених сторін, а головне – служіння інтересам суспільства.

Ефективності внутрішнього аудиту досягають за умов дотримання вимог та рекомендацій, визначених у Глобальних стандартах внутрішнього аудиту, незалежності внутрішнього аудиту та об'єктивності оцінювання компетентними професіоналами.

На основі зазначеного можна виокремити основні аспекти внутрішнього аудиту: ризик-орієнтований підхід; баланс між аудиторськими й консультаційними послугами; забезпечення досягнення цілей установи через процеси управління, управління ризиками та контролю; сприяння спроможності організації служити інтересам суспільства; професійна компетентність аудиторів; незалежність та об'єктивність аудиту [15].

Термін "внутрішній аудит" відповідно до Глобальних стандартів внутрішнього аудиту визначено як "незалежні, об'єктивні послуги з надання впевненості і консультаційні послуги, що додають вартості організації і покращують її діяльність. Внутрішній аудит допомагає організації досягати поставлених цілей застосуванням систематичного, послідовного підходу до оцінювання і вдосконалення процесів управління, ризик-менеджменту і контролю" [15].

У ході порівняльного аналізу сутності терміна "внутрішній аудит" за Глобальними стандартами внутрішнього аудиту та нормативним визначенням у національному законодавстві виявлено, що концептуальна основа цих підходів збігається. В обох визначеннях наголошено, що внутрішній аудит є незалежною та об'єктивною діяльністю, спрямованою на оцінювання ефективності системи управління, внутрішнього контролю й управління ризиками. Незважаючи на наявність у формулюваннях незначних розбіжностей, суть внутрішнього аудиту, визначена Глобальними стандартами, і передбачена Бюджетним кодексом України, практично ідентична, що забезпечує її відповідність міжнародним стандартами внутрішнього аудиту та кращим практикам.

Також, у розділі "Етичне ставлення та професіоналізм" нових стандартів консолідовано етичні принципи та вимоги до професійної поведінки, інтегровані безпосередньо у процес внутрішнього аудиту. Ця зміна спрощує відповідність і забезпечує дотримання внутрішніми аудиторами найвищих стандартів чесності, об'єктивності, компетентності і конфіденційності.

Окремо зазначимо, що в національному законодавстві спостерігається певна невизначеність щодо низки термінів, які у Глобальних стандартах внутрішнього аудиту мають чітке та структуроване визначення. Зокрема, такі поняття, як “надання впевненості”, “консультаційні послуги”, “компетентність”, “чесність”, “функція внутрішнього аудиту”, “методологія внутрішнього аудиту” та інші, не отримали нормативно-правового підтвердження в державній регуляторній базі. Відсутність формально встановлених визначень спричиняє неоднозначність у тлумаченні аудиторських функцій, ускладнює інтеграцію сучасних міжнародних практик у систему внутрішнього аудиту і може негативно позначитися на якості внутрішнього аудиту.

Глобальні стандарти підкреслюють важливу роль аудиторського комітету в нагляді для забезпечення загальної ефективності внутрішнього аудиту. У розділі “Нагляд за функцією внутрішнього аудиту” роз’яснено обов’язки аудиторського комітету, включно з обговоренням та затвердженням планів внутрішнього аудиту, забезпеченням внутрішнього аудиту достатніми ресурсами для виконання плану, а також переглядом зовнішніх оцінок якості для забезпечення постійного вдосконалення внутрішнього аудиту.

В оновлених стандартах наголошено на продуктивності і постійному вдосконаленні, з акцентом на регулярне оцінювання продуктивності. Визнаючи зростання важливості технологій, нові стандарти наголошують на доцільності використання аналітики даних, штучного інтелекту і засобів автоматизації. Такий фокус дає змогу внутрішнім аудиторам підвищити свою ефективність, поліпшити оцінювання ризиків і надати своєчасну та актуальну інформацію.

У розділі “Управління функцією внутрішнього аудиту” визначено вимоги до відповідальності керівника підрозділу внутрішнього аудиту, зокрема щодо управління діяльністю, яка включає планування, залучення та розподіл ресурсів, налагодження взаємовідносин, спілкування із заінтересованими особами, а також забезпечення і підвищення якості й ефективності внутрішнього аудиту.

Особливістю Глобальних стандартів є включення вимог, які містять конкретні вказівки щодо аудиту складних сфер, таких як кібербезпека та управління ризиками шахрайства. Функції внутрішнього аудиту мають відповідати цим вимогам, коли стосуються обсягів аудиторського завдання.

У стандартах також запропоновано конкретні вказівки, розроблені для невеликих аудиторських функцій та організацій державного сектору, визначено унікальні проблеми, з якими зіштовхуються ці організації, і запропоновано практичні рішення для досягнення відповідності при збереженні ефективності.

Проведений аналіз показав, що в Стандартах ВА і Глобальних стандартах внутрішнього аудиту чітко окреслено межі аудиторської діяльності, проте змістове наповнення, зокрема застосування певних прийомів і процедур, покладено на відповідних керівників підрозділів внутрішнього аудиту. Це означає, що для підвищення ефективності і спроможностей внутрішнього аудиту обов’язково потрібно ретельно добирати кадри з високою кваліфікацією, а також ввести кодекс етики як складову Стандартів ВА.

Висновки

Дослідження дає змогу констатувати, що нормативно-правові документи з внутрішнього аудиту в Україні сформовані, але практика постійно вдосконалюється та змінюється у відповідь на виклики сьогодення.

Нормативне визначення терміна “внутрішній аудит” в національному законодавстві приведено до міжнародно визнаних стандартів, при цьому набули чинності нові Глобальні стандарти внутрішнього аудиту, що потребуватиме трансформації та приведення чинних

Стандартів ВА у відповідність до міжнародних норм і визначень, а також трансформації методологічного забезпечення підрозділів внутрішнього аудиту.

У ході аналізу виявлено такі проблемні аспекти нормативно-правового забезпечення внутрішнього аудиту:

фрагментація нормативної бази – діяльність внутрішнього аудиту регламентована численними нормативно-правовими документами, що призводить до розгалуженості і фрагментації законодавчої бази;

невизначеність термінології – на національному рівні існує невизначеність щодо ряду термінів, які за Глобальними стандартами мають чітке та структуроване визначення;

неповна імплементація стандартів –Міжнародні стандарти внутрішнього аудиту досі не імплементовано, що негативно впливає на гармонізацію кращих практик;

відсутність нормативного регулювання застосування сучасних технологій – питання використання аналітики даних, штучного інтелекту та автоматизованих засобів аналізу даних у процесах внутрішнього аудиту залишаються неврегульованими.

На нашу думку, з метою посилення ефективності, спроможності і незалежності внутрішнього аудиту необхідно:

систематизувати нормативно-правові документи з внутрішнього аудиту через їх консолідацію в єдиний документ, наприклад, розробити й ухвалити спеціальний закон, в якому були б об’єднані норми, вимоги, принципи та терміни, які містяться в різних нормативних документах і визначають правові засади провадження внутрішнього аудиту, а також регулюють відносини, що виникають під час його провадження;

забезпечити повну імплементацію Міжнародних стандартів та адаптацію термінології Інституту внутрішніх аудиторів (IIA) до національних реалій;

забезпечити розвиток нормативно-правової бази для застосування сучасних технологій у процесах внутрішнього аудиту.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Стратегія національної безпеки України: Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#n149 (дата звернення: 28.04.2025).
2. Стратегія реформування системи управління державними фінансами на 2022-2025 роки: Розпорядження Кабінету Міністрів України від 29.12.2021 р. № 1805-р. URL: https://zakon.rada.gov.ua/laws/show/1805-2021-%D1%80?find=1&text=%D0%B0%D1%83%D0%B4%D0%B8%D1%82#w1_52 (дата звернення: 28.04.2025).
3. Концепція реалізації державної політики у сфері реформування системи державного фінансового контролю. Розпорядження Кабінету Міністрів України від 10.05.2018 р. № 310-р. URL: https://zakon.rada.gov.ua/laws/show/310-2018-%D1%80#Text (дата звернення: 28.04.2025).
4. Звітна інформація про стан функціонування державного внутрішнього фінансового контролю у 2023 році та 2024 році / Міністерство фінансів України. URL: https://www.mof.gov.ua/uk/informacija-pro-stan-vnutrishnogo-kontrolju-ta-vnutrishnogo-

auditu (дата звернення: 28.04.2025).
5. Закон України "Про аудит фінансової звітності та аудиторську діяльність" від 21.12.2017 р. № 2258-VIII. URL: https://zakon.rada.gov.ua/laws/show/2258-19#Text (дата звернення: 28.04.2025).
6. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. Закон України від 16.09.2014 р. № 1678-VII. URL: https://zakon.rada.gov.ua/laws/show/984_011?find=1&text=%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8C#w1_22 (дата звернення: 28.04.2025).
7. Стаття 26 "Контроль та аудит у бюджетному процесі" глава 4 "Бюджетний процес та його учасники" // Бюджетний кодекс України від 09.07.2010 р. № 2478-VI. URL: https://zakon.rada.gov.ua/laws/show/2542-14#Text (дата звернення: 28.04.2025).
8. Порядок утворення структурних підрозділів внутрішнього аудиту та проведення такого аудиту в міністерствах, інших центральних органах виконавчої влади, їх територіальних органах та бюджетних установах, які належать до сфери управління міністерств, інших центральних органів виконавчої влади: Постанова Кабінету Міністрів України від 28.09.2011 р. № 1001. URL: https://zakon.rada.gov.ua/laws/show/1001-2011-%D0%BF#Text (дата звернення: 28.04.2025).
9. Про затвердження Стандартів внутрішнього аудиту: Наказ Міністерства фінансів України від 04.10.2011 р. № 1247. URL: https://zakon.rada.gov.ua/laws/show/z1219-11#Text (дата звернення: 28.04.2025).
10. Про затвердження Кодексу етики працівників підрозділу внутрішнього аудиту: Наказ Міністерства фінансів України від 29.09.2011 р. № 1217. URL: https://zakon.rada.gov.ua/laws/show/z1195-11#Text (дата звернення: 28.04.2025).
11. Про запровадження сертифікації працівників підрозділів внутрішнього аудиту: Постанова Кабінету Міністрів України від 12.01.2022 р. № 12. URL: https://zakon.rada.gov.ua/laws/show/12-2022-%D0%BF#Text (дата звернення: 28.04.2025).
12. Порядок проведення сертифікації працівників підрозділів внутрішнього аудиту: Наказ Міністерства фінансів України від 18.05.2022 р. № 144. URL: https://zakon.rada.gov.ua/laws/show/z0676-22#Text (дата звернення: 28.04.2025).
13. Інструкція про складання форми звітності про результати діяльності підрозділів внутрішнього аудиту: Наказ Міністерства фінансів України від 27.03.2014 р. № 347. URL: https://zakon.rada.gov.ua/laws/show/z0410-14#Text (дата звернення: 28.04.2025).
14. Порядок здійснення Міністерством фінансів України оцінки функціонування системи внутрішнього аудиту: Наказ Міністерства фінансів України від 03.05.2017 р. № 480. URL: https://zakon.rada.gov.ua/laws/show/z0663-17#Text (дата звернення: 28.04.2025).
15. Глобальні стандарти внутрішнього аудиту. URL: https://theiia.org.ua/wp-content/uploads/2024/12/global-internal-audit-standards-ukrainian.pdf (дата звернення: 28.04.2025).
16. Порядок проведення внутрішнього аудиту в системі Міністерства оборони України від 15.12.2020 р. № 475. Наказ Міністерства оборони України URL: http://www.mil.gov.ua/diyalnist/vnutrishnij-audit/normativno-pravova-baza.html (дата звернення: 28.04.2025).
17. Каменська Т. О. Внутрішній аудит: методологія та організація дис. … доктора наук: 19.04.2011. Київ, 2011. 560 с. URL: https://uacademic.info/ua/document/0511U000334#! (дата звернення: 28.04.2025).
18. Каменська Т. О. Внутрішній аудит: виникнення та розвиток / Т. О. Каменська // Статистика України. – 2015. – № 4. – С. 60-68. URL: http://nbuv.gov.ua/UJRN/su_2015_4_10 (дата

звернення: 28.04.2025).
19. Пушкарьова О. Ю. Організаційно-методичне забезпечення внутрішнього аудиту в системі державного фінансового контролю. дис. … канд. наук: 12.11.2020. Київ, 2020. 293 с. URL: https://uacademic.info/ua/document/0420U102140#! (дата звернення: 28.04.2025).
20. Семенець А. О. Методологія внутрішнього аудиту в системі управління торговельними підприємствами. дис. … доктора наук: 10.10.2019. Харків, 2019. 361 с. URL: https://uacademic.info/ua/document/0519U001645#! (дата звернення: 28.04.2025).
21. Філозоп О. В. Розвиток внутрішнього аудиту в Україні: організація і методика: дис. … канд. наук: 06.10.2010. Житомир, 2010. 315 с.
22. Калінкін Д. В. Внутрішній аудит бюджетних установ в умовах реформування системи державного фінансового контролю: дис. … канд. наук: 10.03.2016. Харків, 2016. 279 с.
23. Редько О. Ю. Методологія та організація професійного аудиту в Україні. Стан та перспективи розвитку: дис. … доктора наук: 28.04.2009. Київ, 2009. 453 с.
24. Лебединська О. Ю. Адміністративно-правове регулювання державного аудиту в Україні: дис. … доктора філософії: 23.12.2020. Київ, 2020. 533 с.
25. Рудніцька Р.М. Роль аудиту в оцінюванні ефективності державного управління: світовий досвід розвитку. Державне управління та місцеве самоврядування. Вип.2 (17). 2013. С. 72–79.
26. Рудніцька Р.М. Міжнародні та вітчизняні стандарти аудиту в державному управлінні – спільні та відмінні риси. Демократичне врядування. Науковий вісник. 2012. Вип. 10. 6 с.
27. Мельник О.П. Внутрішній аудит в системі державного внутрішнього фінансового контролю. Збірник наукових праць Ірпінської фінансово-юридичної академії (економіка, право). 2013. Вип. 2. 6 с.
28. Ружанський О. Нормативно-правове забезпечення внутрішнього аудиту в публічному управлінні системою Державної служби України з надзвичайних ситуацій // Науковий вісник: “Державне управління”. 2023. № 1 (13). https://doi.org/10.33269/2618-0065-2023-1(13)-123-137 (дата звернення: 28.04.2025).

References

1. Stratehiya natsional’noyi bezpeky Ukrayiny: Ukaz Prezydenta Ukrayiny vid 14.09.2020 r. № 392/2020. Available from : https://zakon.rada.gov.ua/laws/show/392/2020#n149 (data zvernennya: 28.04.2025).
2. Stratehiya reformuvannya systemy upravlinnya derzhavnymy finansamy na 2022-2025 roky: Rozporyadzhennya Kabinetu Ministriv Ukrayiny vid 29.12.2021 r. № 1805-r. Available from : https://zakon.rada.gov.ua/laws/show/1805-2021-%D1%80?find=1&text=%D0%B0%D1%83%D0%B4%D0%B8%D1%82#w1_52 (data zvernennya: 28.04.2025).
3. Kontseptsiya realizatsiyi derzhavnoyi polityky u sferi reformuvannya systemy derzhavnoho finansovoho kontrolyu. Rozporyadzhennya Kabinetu Ministriv Ukrayiny vid 10.05.2018 r. № 310-r. Available from : https://zakon.rada.gov.ua/laws/show/310-2018-%D1%80#Text (data zvernennya: 28.04.2025).
4. Zvitna informatsiya pro stan funktsionuvannya derzhavnoho vnutrishn’oho finansovoho kontrolyu u 2023 rotsi ta 2024 rotsi / Ministerstvo finansiv Ukrayiny. Available from : https://www.mof.gov.ua/uk/informacija-pro-stan-vnutrishnogo-kontrolju-ta-vnutrishnogo-auditu (data zvernennya: 28.04.2025).
5. Zakon Ukrayiny “Pro audyt finansovoyi zvitnosti ta audytors’ku diyal’nist’” vid 21.12.2017 r. № 2258-VIII. Available from : https://zakon.rada.gov.ua/laws/show/2258-19#Text (data zvernennya: 28.04.2025).

6. Uhoda pro asotsiatsiyu mizh Ukrayinoyu, z odniyeyi storony, ta Yevropeys'kym Soyuzom, Yevropeys'kym spivtovarystvom z atomnoyi enerhiyi i yikhnimy derzhavamy-chlenamy, z inshoyi storony. Zakon Ukrayiny vid 16.09.2014 r. № 1678-VII. Available from : https://zakon.rada.gov.ua/laws/show/984_011?find=1&text=%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8C#w1_22 (data zvernennya: 28.04.2025).
7. Stattya 26 "Kontrol' ta audyt u byudzhetnomu protsesi" hlava 4 "Byudzhetnyy protses ta yoho uchasnyky" // Byudzhetnyy kodeks Ukrayiny vid 09.07.2010 r. № 2478-VI. Available from : https://zakon.rada.gov.ua/laws/show/2542-14#Text (data zvernennya: 28.04.2025).
8. Poryadok utvorennya strukturnykh pidrozdiliv vnutrishn'oho audytu ta provedennya takoho audytu v ministerstvakh, inshykh tsentral'nykh orhanakh vykonavchoyi vlady, yikh terytorial'nykh orhanakh ta byudzhetnykh ustanovakh, yaki nalezhat' do sfery upravlinnya ministerstv, inshykh tsentral'nykh orhaniv vykonavchoyi vlady: Postanova Kabinetu Ministriv Ukrayiny vid 28.09.2011 r. № 1001. Available from : https://zakon.rada.gov.ua/laws/show/1001-2011-%D0%BF#Text (data zvernennya: 28.04.2025).
9. Pro zatverdzhennya Standartiv vnutrishn'oho audytu: Nakaz Ministerstva finansiv Ukrayiny vid 04.10.2011 r. № 1247. Available from : https://zakon.rada.gov.ua/laws/show/z1219-11#Text (data zvernennya: 28.04.2025).
10. Pro zatverdzhennya Kodeksu etyky pratsivnykiv pidrozdilu vnutrishn'oho audytu: Nakaz Ministerstva finansiv Ukrayiny vid 29.09.2011 r. № 1217. Available from : https://zakon.rada.gov.ua/laws/show/z1195-11#Text (data zvernennya: 28.04.2025).
11. Pro zaprovadzhennya sertyfikatsiyi pratsivnykiv pidrozdiliv vnutrishn'oho audytu: Postanova Kabinetu Ministriv Ukrayiny vid 12.01.2022 r. № 12. Available from : https://zakon.rada.gov.ua/laws/show/12-2022-%D0%BF#Text (data zvernennya: 28.04.2025).
12. Poryadok provedennya sertyfikatsiyi pratsivnykiv pidrozdiliv vnutrishn'oho audytu: Nakaz Ministerstva finansiv Ukrayiny vid 18.05.2022 r. № 144. Available from : https://zakon.rada.gov.ua/laws/show/z0676-22#Text (data zvernennya: 28.04.2025).
13. Instruktsiya pro skladannya formy zvitnosti pro rezul'taty diyal'nosti pidrozdiliv vnutrishn'oho audytu: Nakaz Ministerstva finansiv Ukrayiny vid 27.03.2014 r. № 347. Available from : https://zakon.rada.gov.ua/laws/show/z0410-14#Text (data zvernennya: 28.04.2025).
14. Poryadok zdiysnennya Ministerstvom finansiv Ukrayiny otsinky funktsionuvannya systemy vnutrishn'oho audytu: Nakaz Ministerstva finansiv Ukrayiny vid 03.05.2017 r. № 480. Available from : https://zakon.rada.gov.ua/laws/show/z0663-17#Text (data zvernennya: 28.04.2025).
15. Hlobal'ni standarty vnutrishn'oho audytu. Available from : https://theiia.org.ua/wp-content/uploads/2024/12/global-internal-audit-standards-ukrainian.pdf (data zvernennya: 28.04.2025).
16. Poryadok provedennya vnutrishn'oho audytu v systemi Ministerstva oborony Ukrayiny vid 15.12.2020 r. № 475. Nakaz Ministerstva oborony Ukrayiny Available from : http://www.mil.gov.ua/diyalnist/vnutrishnij-audit/normativno-pravova-baza.html (data zvernennya: 28.04.2025).
17. Kamens'ka T. O. Vnutrishniy audyt: metodolohiya ta orhanizatsiya dys. … doktora nauk: 19.04.2011. Kyyiv, 2011. 560 s. Available from : https://uacademic.info/ua/document/0511U000334#! (data zvernennya: 28.04.2025).
18. Kamens'ka T. O. Vnutrishniy audyt: vynyknennya ta rozvytok / T. O. Kamens'ka // Statystyka Ukrayiny. 2015. № 4. S. 60-68. Available from : http://nbuv.gov.ua/UJRN/su_2015_4_10 (data zvernennya: 28.04.2025).

19. Pushkar'ova O. YU. Orhanizatsiyno-metodychne zabezpechennya vnutrishn'oho audytu v systemi derzhavnoho finansovoho kontrolyu. dys. … kand. nauk: 12.11.2020. Kyyiv, 2020. 293 s. Available from : https://uacademic.info/ua/document/0420U102140#! (data zvernennya: 28.04.2025).
20. Semenets' A. O. Metodolohiya vnutrishn'oho audytu v systemi upravlinnya torhovel'nymy pidpryyemstvamy. dys. … doktora nauk: 10.10.2019. Kharkiv, 2019. 361 s. Available from : https://uacademic.info/ua/document/0519U001645#! (data zvernennya: 28.04.2025).
21. Filozop O. V. Rozvytok vnutrishn'oho audytu v Ukrayini: orhanizatsiya i metodyka: dys. … kand. nauk: 06.10.2010. Zhytomyr, 2010. 315 s.
22. Kalinkin D. V. Vnutrishniy audyt byudzhetnykh ustanov v umovakh reformuvannya systemy derzhavnoho finansovoho kontrolyu: dys. … kand. nauk: 10.03.2016. Kharkiv, 2016. 279 s.
23. Red'ko O. YU. Metodolohiya ta orhanizatsiya profesiynoho audytu v Ukrayini. Stan ta perspektyvy rozvytku: dys. … doktora nauk: 28.04.2009. Kyiv, 2009. 453 s.
24. Lebedyns'ka O. YU. Administratyvno-pravove rehulyuvannya derzhavnoho audytu v Ukrayini: dys. … doktora filosofiyi: 23.12.2020. Kyiv, 2020. 533 s.
25. Rudnits'ka R.M. Rol' audytu v otsinyuvanni efektyvnosti derzhavnoho upravlinnya: svitovyy dosvid rozvytku // Derzhavne upravlinnya ta mistseve samovryaduvannya. Vyp.2 (17). 2013. S. 72–79.
26. Rudnits'ka R.M. Mizhnarodni ta vitchyznyani standarty audytu v derzhavnomu upravlinni – spil'ni ta vidminni rysy // Demokratychne vryaduvannya. Naukovyy visnyk. 2012. Vyp. 10. 6 s.
27. Mel'nyk O.P. Vnutrishniy audyt v systemi derzhavnoho vnutrishn'oho finansovoho kontrolyu // Zbirnyk naukovykh prats' Irpins'koyi finansovo-yurydychnoyi akademiyi (ekonomika, pravo). 2013. Vyp. 2. 6 s.
28. Ruzhans'kyy O. Normatyvno-pravove zabezpechennya vnutrishn'oho audytu v publichnomu upravlinni systemoyu Derzhavnoyi sluzhby Ukrayiny z nadzvychaynykh sytuatsiy // Naukovyy visnyk: "Derzhavne upravlinnya". 2023. № 1 (13). https://doi.org/10.33269/2618-0065-2023-1(13)-123-137 (data zvernennya: 28.04.2025).

Удосконалення методу оцінювання рівня воєнної небезпеки з урахуванням досвіду російсько-української війни

Improving the method of assessing the level of military threat based on the experience of the russian-ukrainian war

Микола Ткач [A]
Corresponding author: д.економ.н., доцент, начальник центру, e-mail: nyck1985@ukr.net, ORCID: 0000-0002-8832-1268
Станіслав Слободяник [A]
к.економ.н., СНС, e-mail: 8s.8@ukr.net, ORCID: 0000-0001-5537-2723
Ігор Хабло [A]
Магістр, e-mail: habib@i.ua
Наталія Гончарук [A]
ад'юнкт, e-mail: onofreichyk@ukr.net, ORCID: 0009-0002-3464-0623
Павло Макошенець [A]
ад'юнкт, e-mail: nyck1985@ukr.net

Mykola Tkach [A]
Corresponding author: Dr of Economics, Associate Professor, e-mail: nyck1985@ukr.net, ORCID: 0000-0002-8832-1268
Stanislav Slobodianyk [A]
Candidate of Economic Sciences, Senior Researcher, e-mail: 8s.8@ukr.net, ORCID: 0000-0001-5537-2723
Igor Hablo [A]
Master's student, e-mail: habib@i.ua
Natalia Honcharuk [A]
PhD student, e-mail: onofreichyk@ukr.net, ORCID: 0009-0002-3464-0623
Pavlo Makoshenets [A]
PhD student, e-mail: nyck1985@ukr.net

[A] Національний університет оборони України, м. Київ, Україна
[A] National Defense University of Ukraine, Kyiv, Ukraine

Received: April 16, 2025 | Revised: April 28, 2025 | Accepted: April 30, 2025

JEL Classification: F52, C81, C82.

DOI: 10.33445/sds.2025.15.2.23

Мета роботи: розроблення рекомендацій щодо підвищення якості оцінювання рівня воєнної небезпеки для України з врахуванням досвіду російсько-Української війни.

Метод дослідження: для реалізації мети дослідження використано такі методи наукових досліджень, як аналіз, експертний метод, метод індукції та дедукції, статистичний аналіз та метод порівнянь.

Результати дослідження: на основі отриманих знань в дослідження сформовано пропозиції щодо розвитку підходів з оцінювання рівня воєнної небезпеки держави.

Теоретична цінність дослідження: результати дослідження доповнюють існуючі теоретичні дослідження в сфері оцінювання та прогнозування воєнної небезпеки держави, а також враховують практичний досвід російсько-Української війни.

Практична цінність дослідження: в межах дослідження наведений досвід російсько-Української війни та запропоновано практичні кроки щодо підвищення якості оцінювання та прогнозування воєнної загрози державі.

Оригінальність/Цінність дослідження: в даному дослідженні запропоновано показники рівня воєнної небезпеки держави з врахуванням досвіду підготовки російською федерацією, а також російсько-Української війни.

Обмеження дослідження/Майбутні дослідження: обмеження дослідження полягає у використанні джерел, що знаходяться у відкритому доступі. Майбутні дослідження будуть спрямовані на формуванні прогнозів щодо подальшого перебігу війни та формуванні пропозицій щодо протидії майбутнім загрозам для України.

Тип статті: теоретичний, практичний.

Purpose: The purpose of the article is to develop recommendations for improving the quality of assessing the level of military threat for Ukraine, taking into account the experience of the Russian-Ukrainian war.

Method: To achieve the research goal, the following scientific research methods were used: analysis, expert method, induction and deduction method, statistical analysis, and comparison method.

Findings: Based on the knowledge gained, the study formulated proposals for the development of approaches to assessing the level of military threat to the state.

Theoretical implications: The results of the study complement existing theoretical research in the field of assessing and forecasting the military danger of the state and also take into account the practical experience of the Russian-Ukrainian war.

Practical implications: The study presents the experience of the Russian-Ukrainian war and proposes practical steps to improve the quality of assessing and forecasting the military threat to the state.

Originality/Value: This study proposes indicators of the level of military danger of the state, taking into account the experience of the Russian Federation's preparation, as well as the Russian-Ukrainian war.

Research limitations/Future research: The limitation of the study is the use of publicly available sources. Future research will be aimed at forming forecasts for the further course of the war and formulating proposals for countering future threats to Ukraine.

Papertype: theoretical and practical.

Ключові слова: небезпека, воєнна небезпека, національна безпека, війна, національні інтереси, воєнне стратегічне навчання.

Key words: danger, military danger, national security, war, national interests, military strategic training.

Вступ

Прогнозування рівня воєнної небезпеки є одним з основних аспектів національної безпеки будь-якої держави, і особливо важливим воно є для України, яка стикається з постійними загрозами з боку російської федерації (рф). Оскільки рф активно проводить гібридну війну, а в 2014 році здійснила незаконну анексію Криму та почала підтримку сепаратистських рухів на сході України, перед українською державою постає необхідність удосконалення механізмів оцінки воєнної небезпеки. Особливо це актуально в контексті останніх подій, пов'язаних з повномасштабним військовим вторгненням РФ у 2022 році. Враховуючи нестабільну ситуацію в Південно-Східному регіоні країни, прогнозування рівня воєнної небезпеки є не лише важливим інструментом для державних структур, а й важливим кроком у збереженні територіальної цілісності та забезпеченні безпеки.

Теоретичні основи дослідження

Стратегічною метою воєнної політики є забезпечення воєнної безпеки держави. Воєнна безпека визначається як захищеність національних інтересів, суверенітету, територіальної цілісності та недоторканності країни від будь-яких посягань із застосуванням воєнної сили. Для забезпечення належного рівня воєнної безпеки необхідним є комплексне використання економічного, соціального, політичного, військового, науково-технологічного, демографічного, ресурсного, інформаційного та морально-психологічного потенціалів держави з метою зниження рівня воєнної небезпеки в будь-яких умовах.

У науковій літературі поняття воєнної небезпеки розглядається як постійна потенційна можливість застосування воєнної сили однією державою або групою держав для вирішення міждержавних політичних, економічних, військових, етнічних та інших протиріч. Важливість цього поняття підкреслюється необхідністю врахування існуючих чинників, які створюють ризики для національних інтересів України та можуть призвести до збройних конфліктів.

Воєнна небезпека визначається низкою показників, які характеризують напруженість воєнно-політичних відносин між країнами та ступінь можливості збройного конфлікту.

Методологічний підхід до оцінювання воєнної небезпеки передбачає комплексний аналіз зазначених факторів з урахуванням їх взаємозв'язку та впливу на загальну ситуацію безпеки. Це дозволяє формувати адекватні управлінські рішення для забезпечення необхідного рівня обороноздатності країни та запобігання розвитку кризових сценаріїв.

У сучасних умовах існує велика кількість методик оцінювання рівня воєнної небезпеки [1-8]:

методика оцінювання воєнно-економічної стійкості держави, яка базується на експертному аналізі загроз за критеріями ймовірності, впливу та можливості контролю, із розрахунком інтегрального показника стійкості;

методика оцінки загроз енергетичній безпеці, яка акцентує увагу на комплексному аналізі внутрішніх та зовнішніх чинників, що впливають на енергетичну стійкість держави;

таксономічна методика оцінювання рівня воєнної небезпеки, яка використовує математичні методи багатовимірного порівняльного аналізу для отримання кількісних оцінок рівня загроз;

методика оцінювання можливостей відновлення озброєння та військової техніки, що враховує фактори інтенсивності бойових дій, логістичного забезпечення та кваліфікації персоналу;

методичні підходи оцінювання воєнно-економічного потенціалу, які аналізують економічні показники, інфраструктурні можливості та ресурсну базу;

концепція забезпечення воєнної безпеки на основі оцінювання ризиків реалізації кризових сценаріїв, яка передбачає превентивні стратегії та інтеграцію військових і

невійськових учасників системи безпеки;

національний стратегічний абакус ризиків, цей інструмент допомагає планувальникам оцінити прийнятність ризиків, пов'язаних з різними інструментами національної влади (дипломатичними, інформаційними, військовими, економічними);

національна радарна діаграма стратегічних ризиків, ця діаграма пропонує візуальне представлення ризиків за кількома вимірами, що дозволяє планувальникам виявляти області підвищеної вразливості та ефективно повідомляти про ці ризики особам, що приймають рішення.

Використання цих інструментів, під час прогнозування та стратегічного планування, дозволяє краще передбачати стратегічні наслідки своїх дій, що призводить до більш обґрунтованих процесів прийняття рішень.

Усі наведені методики мають як переваги, так і недоліки, що підкреслює необхідність їх комплексного використання з подальшою емпіричною валідацією. Таким чином, аналіз теоретичних основ оцінювання воєнної небезпеки дозволяє сформувати ґрунтовний базис для подальших досліджень та вдосконалення методик забезпечення національної безпеки України в умовах сучасних воєнно-політичних викликів.

Постановка проблеми

Сучасна геополітична ситуація характеризується динамічним зростанням воєнних та гібридних загроз для національної безпеки України, особливо у зв’язку із тривалою агресією з боку російської федерації. Незважаючи на численні наукові дослідження та розробки методик оцінювання рівня воєнної небезпеки, питання комплексного, своєчасного та ефективного прогнозування таких загроз залишається недостатньо вирішеним.

Існуючі методичні підходи до оцінювання воєнної безпеки, хоча й дозволяють визначати рівні загроз та ризиків, характеризуються певними недоліками, зокрема суб'єктивністю експертних оцінок, обмеженістю набору критеріїв, недостатнім використанням сучасних технологій аналізу даних та прогностичних інструментів. Крім того, в умовах гібридної війни особливо гостро постає потреба у створенні новітніх методик, які б забезпечували комплексну оцінку багатовимірних факторів загроз та дозволяли автоматизувати процеси моніторингу і прогнозування.

Таким чином, виникає необхідність у розробці комплексного науково-методичного підходу, що базувався би на використанні сучасних інформаційних технологій, штучного інтелекту, Big Data, а також інтегральних багатокритеріальних методик оцінювання воєнної небезпеки. Особливу увагу при цьому слід приділити поглибленню міжнародного співробітництва, підвищенню якості прогнозування загроз на ранніх стадіях їх виникнення, та створенню єдиної автоматизованої системи стратегічного попередження для органів державного управління.

Отже, проблема подальших досліджень полягає у формуванні нових, ефективних методів та засобів прогнозування воєнних загроз для України, які дозволять підвищити рівень готовності держави до своєчасного реагування на різноманітні виклики та зменшити ризики збройних конфліктів та гібридних загроз.

Метою статті є розроблення рекомендацій щодо підвищення якості оцінювання рівня воєнної небезпеки для України з врахуванням досвіду російсько-Української війни.

Методологія дослідження

Методологія проведення дослідження базується на використанні комплексного підходу, що передбачає поєднання загальнонаукових, теоретичних та прикладних методів аналізу й оцінювання воєнної небезпеки, а також сучасних інформаційних технологій для прогнозування та управління загрозами. Враховуючи складність та багатовимірність досліджуваного об'єкта, методологія охоплює такі основні компоненти:

системний підхід, який передбачає розгляд воєнної безпеки як цілісної системи, що складається з взаємопов'язаних політичних, військових, економічних, соціальних, технологічних та інформаційних елементів;

комплексний підхід, що передбачає всебічний аналіз факторів, які впливають на рівень воєнної небезпеки, а також дозволяє враховувати їхні взаємні впливи та взаємозалежність;

аналіз і синтез, для визначення основних показників, що формують рівень воєнної небезпеки, а також для узагальнення отриманих результатів та розробки інтегральних підходів до оцінювання;

порівняльний метод, для зіставлення міжнародних методик та досвіду у сфері оцінювання та прогнозування загроз національній безпеці;

експертний метод, проведення опитувань і анкетувань серед військових, аналітиків, фахівців з питань безпеки з метою ідентифікації ключових загроз, визначення їхньої важливості та формування пріоритетів.

Результати

1 Воєнно-політична та воєнна-стратегічна обстановка навколо України напередодні вторгнення

У другій половині 2021 року світ почав висловлювати свою занепокоєність діями рф навколо України:

квітень 2021 року – Європейське командування США підвищує рівень спостереження за ситуацією з "потенційної кризи";

30.10.2021 – The Washington Post опублікувало статтю про загрозливе збільшення кількості російських військ поблизу кордонів України [9];

листопад 2021 року – очільник ЦРУ США Вільям Бернс відвідав москву, після чого зателефонував Президенту України;

листопад 2021 року – Директор національної розвідки США (Ервіл Гейнс) доповіла про плани вторгнення Північноатлантичній раді НАТО;

15.11.2021 – спільна заява голів МЗС Німеччини та Франції із попередженням росії про наслідки у разі нової спроби підриву територіальної цілісності України;

04.12.2021 – видання Bild публікує можливі сценарії вторгнення рф в Україну [10];

16.12.2021 – Північноатлантична рада у своїй заяві попередила росію про наслідки у разі агресії проти України;

17 грудня 2021 року – росія вимагала юридично обов'язкових гарантій припинення НАТО будь-якої військової діяльності в Східній Європі та Україні. Ці вимоги були частиною ширшого набору гарантій безпеки, які росія хотіла отримати [11];

26 січня 2022 року – США та НАТО передали росії письмову відповідь на її "пропозиції" щодо "гарантій безпеки" в Європі з відмовою;

04.02.2022 – спільна заява лідерів КНР та рф у Пекіні про міжнародні відносини, які вступають в нову епоху, та глобальний стійкий розвиток. Жодна держава не може і не повинна забезпечувати свою безпеку у відриві від безпеки всього світу та за рахунок безпеки інших держав", — йдеться в домовленостях. Китай та росія наголошують, що вони "глибоко стурбовані серйозними викликами у сфері міжнародної безпеки" і заявляють, що "долі народів усіх країн взаємопов'язані" [12];

7 лютого президент Франції Еммануель Макрон відвідав росію та провів перемовини з путіним. Сторони домовилися продовжити співпрацю у Нормандському форматі [13];

17.02.2022 року – на Радбезі ООН Державний Секретар Блінкен заявив про наближення вторгнення в Україну з боку рф [14];

18.02.2022 року – заява президента США Дж. Байдена щодо ухвалення путіним рішення про вторгнення до України. Сенат США затвердив резолюцію про непохитну підтримку США

безпечної, демократичної та незалежної України [15].

На передодні вторгнення росії в Україну 24 лютого 2022 року світова безпекова ситуація перебувала в умовах суттєвих змін, що зумовило перегляд стратегічних розрахунків як західних, так і російських керівників. Завершення місії Збройних сил США в Афганістані, про що свідчить аналітичний звіт Національного інституту стратегічних досліджень (НІСД, 2021), стало важливим сигналом у глобальній безпековій системі, який, зокрема, вплинув на настрій росії перед початком повномасштабного вторгнення в Україну.

За даними звіту НІСД, виведення американських військ з Афганістану підсумувало двадцятирічну кампанію, метою якої було знищення терористичних угруповань і встановлення стабільності в регіоні. Хоча військові операції завершилися відносним успіхом у бойовому плані, політичні цілі, такі як створення стабільного, демократичного уряду та трансформація традиційного суспільства, залишилися невиконаними. Аналіз НІСД вказує на те, що результати кампанії продемонстрували обмеження військової сили у досягненні комплексних політичних змін, а також на слабкість західних механізмів постконфліктного врегулювання. Ці уроки, зауважено в документі, є надзвичайно важливими для аналізу глобальної безпеки, оскільки вони свідчать про можливість невизначеності у зобов'язаннях головних світових гравців. Для росії, яка протягом багатьох років активно використовувала стратегію гібридної війни та прагнула до перегляду статусу-кво в пострадянському просторі, виведення військ США з Афганістану стало своєрідним каталізатором для перегляду власних стратегічних розрахунків [16].

Перед вторгненням рф в Україну 24 лютого 2022 року кібератаки стали однією з невід'ємних складових загальної стратегії гібридної війни, спрямованої на дестабілізацію оперативної готовності українських державних структур та зниження ефективності систем управління. У цей період спостерігалося різке зростання інтенсивності кібератак, що включало спроби проникнення у внутрішні мережі урядових установ, Збройних сил і критичної інфраструктури країни. Російські кібероперації мали на меті не тільки збирання розвідувальної інформації, але й створення хаосу в інформаційному середовищі, що ускладнювало оперативне реагування та координацію дій українських сил.

Таким чином, інтенсивність кібератак перед вторгненням у 2022 році стала одним із важливих чинників, що відображали готовність росії застосовувати гібридні методи ведення війни. Ці операції сприяли підриву стабільності в Україні, створюючи передумови для широкомасштабного військового наступу та свідчачи про здатність кремля інтегрувати сучасні технологічні інструменти в традиційну військову стратегію. Такий підхід підкреслює необхідність для України не лише посилити свою обороноздатність у фізичному вимірі, а й розвивати кібербезпеку та захищеність інформаційних систем як частину системи національної безпеки.

Згідно зі звітом Microsoft, російські хакери готувалися до воєнної агресії проти України щонайменше з березня 2021 року. У березні 2021 року одна з груп розпочала фішингову кампанію, спрямовану на ускладнення отримання Україною міжнародної допомоги для протидії російській агресії. У середині 2021 року російські хакерські угруповання здійснювали численні спроби кібератак методом "атака через ланцюжок постачання" (supply-chain attack). Наприклад, було скомпрометовано мережу IT-компанії, яка розробляла систему управління ресурсами для Міністерства оборони України, а також програми для організацій транспортного й комунікаційного секторів. Інша хакерська група здійснила схожі кібератаки проти IT-компаній, які надавали аналогічні послуги державним замовникам у країнах НАТО. У серпні 2021 року проведено фішингову кампанію для отримання доступу до акаунтів українських іноземних військових радників та гуманітарних працівників.

Отже, кіберзагроза стала невід'ємною складовою сучасних військових конфліктів, і її зростаюча інтенсивність свідчить про необхідність розширення систем кібербезпеки як в національному, так і в міжнародному контексті.

До повномасштабного вторгнення росії в Україну в лютому 2022 року, рф активно проводила інформаційну війну з метою впливу на внутрішню та зовнішню ситуацію в Україні. Ця кампанія включала різноманітні методи, спрямовані на дестабілізацію суспільно-політичної ситуації та підрив довіри до державних інститутів.

У контексті роботи, аналіз наративів російської пропаганди за пів року до повномасштабного вторгнення росії в Україну є важливим аспектом для розуміння інформаційного впливу, що здійснювався на українське суспільство та міжнародну аудиторію. Ці наративи сприяли формуванню суспільної думки, яка підтримувала російські геополітичні інтереси та намагалася ослабити українську державність, створюючи підґрунтя для агресії.

Після введення міжнародних санкцій та зростання напруженості у відносинах із Заходом, росія зосередила свою увагу на зміцненні зв'язків з іншими державами, що виявили готовність підтримати її інтереси в умовах міжнародної ізоляції. Важливою складовою цієї стратегії стало укладення нових стратегічних угод із країнами, які не поділяли позиції Заходу щодо росії. Однією з найбільш важливих угод стала співпраця з Китаєм. У 2021 році дві держави підписали низку домовленостей у сферах енергетики, безпеки та інфраструктури, що дозволило росії зменшити свою економічну залежність від західних країн.

Зокрема, росія активно розвивала спільні енергетичні проекти з Китаєм, зокрема через газопроводи, такі як "Сила Сибіру". Ці угоди дозволили москві зберегти свою роль постачальника енергоносіїв для китайського ринку, що є важливим для економічної стабільності країни. Також росія продовжила зміцнення співпраці з Іраном і Туреччиною в рамках різноманітних стратегічних ініціатив, зокрема у галузях енергетики, оборони та інфраструктури. Водночас ці угоди стали основою для створення нових політичних альянсів, що дозволяли росії зберігати вплив на міжнародній арені, зокрема в контексті протистояння з Заходом.

Як показує досвід одним з важливих факторів впливу на воєнну небезпеку є кількість проведених військових навчань сусідньою країною (в нашому випадку рф), змісту таких навчань, а також їхня географічна близькість до кордонів України. Якщо розглянути військові навчання рф та її союзників (в основному Республіка Білорусь) починаючи з 2017 року, то можна констатувати, що вони все більше нагадували підготовку до повномасштабного вторгнення в Україну. Проаналізуємо деякі з військових навчань.

Навчання "Захід-2017" були масштабними стратегічними військовими навчаннями, які проводилися Росією спільно з Білоруссю з 14 по 20 вересня 2017 року. Основними цілями цих навчань було перевірити готовність та координацію військових сил обох країн в умовах можливого конфлікту з зовнішнім агресором, що, за заявами, відображало агресивні дії НАТО.

Навчання "Схід-2018", які відбулися з 11 по 15 вересня 2018 року, також були масштабними військовими навчаннями, організованими Росією. Ці навчання включали в себе широкий спектр військових дій і стратегічне планування, зокрема перекидання військ із центральних районів Росії до кордонів з Україною та проведення маневрів уздовж кордонів.

Навчання "Центр-2019" відбулися в серпні-вересні 2019 року і були одними з найбільших військових навчань, які проводила рф того року. Ці навчання свідчили про зростаючу військову активність росії та її прагнення підвищити військову готовність у стратегічно важливих регіонах, що межують з Європою та іншими сусідніми країнами.

Навчання "Щит Союзу-2019". Російські ЗМІ нарочито підкреслюють, що маневри "Щит Союзу-2019" цього року матимуть виключно оборонний характер, хоча насправді перелік техніки й тематика заходів вказують на протилежне [17].

Навчання "Кавказ-2020", які відбулися у вересні 2020 року, були спрямовані на підвищення військової готовності та вдосконалення стратегічного планування в регіоні Південного Кавказу.

Навчання у Південному військовому окрузі (грудень 2021 року), які розпочалися 1 грудня 2021 року. Росія розпочала навчання в Південному військовому окрузі, що межує з

Україною. У них взяли участь понад 10 тисяч військовослужбовців, які здійснили марші до загальновійськових полігонів у Ростовській, Волгоградській, Астраханській областях, Північній Осетії, Інгушетії, на Ставропіллі та в окупованому Криму.

Ці навчання свідчать про постійну зосередженість російської федерації на підвищенні своєї військової готовності в ключових регіонах, а також підвищення воєнної небезпеки для України.

Захід-2021 — спільне стратегічне навчання (ССН) Збройних сил російської федерації і республіки білорусь, які відбулися з 10 по 16 вересня 2021 року. У навчаннях мали взяти участь близько 200 тис. військових, до 760 одиниць техніки і 15 кораблів. За словами американського генерала та голови Об'єднаного комітету начальників штабів США Марка Міллі, спостереження за "Західом-2021" допомогли американській розвідці передбачити неминучість російського вторгнення в Україну. Це сталося тому, що навчання були набагато більшими за масштабом, обсягом, складом і тривалістю, ніж попередні навчання. Після навчань Міллі провів брифінг із президентом США Джо Байденом щодо серйозності російської загрози щодо України.

Навчання "Союзна рішучість-2022" — спільні навчання Збройних сил російської федерації та Республіки Білорусь, які проводилися з 10 по 20 лютого 2022 року, фактично були подовжені до 24 лютого та стали підґрунтям для подальшого російського вторгнення в Україну.

18 січня 2022 року на брифінгу для іноземних військових аташе заступник міністра оборони рф Олександр Фомін повідомив, що цілями навчань є проведення позапланової перевірки військ та відпрацювання різних варіантів спільних дій щодо нейтралізації загроз та стабілізації обставин на кордонах Союзної держави росії та білорусі. Підготовка військ і сил до дій не тільки у своїх межах відповідальності, але й до розв'язання задач, що раптово виникають, з локалізації кризових ситуацій на будь-яких напрямках.

Важлива частина навчань — оцінка можливостей транспортної інфраструктури із забезпечення перевезення військ під час перекидання російських частин на територію Білорусі. У зв'язку з цим у навчаннях від росії беруть участь органи управління та підрозділи Східного військового округу (Далекий Схід та Східний Сибір)[12].

Аналіз задіяних сил і засобів зс рф у військових навчаннях показує, що кількість особового складу та техніки постійно зростає, а географія місць проведення рухається на захід, ближче до кордонів з Україною (рис. 1).

Таким чином, за рахунок військових навчань рф випробувала основні сценарії агресії проти України, провела злагодження військ та штабів на всіх рівнях управління, підготувала логістичні потужності, накопичила необхідні військові запаси на кордоні з Україною, провела мобілізаційні приготування, зосередила на кордоні з Україною необхідну кількість сил та засобів.

Проведений аналіз дозволяє зробити висновок, що показник кількості, масштабів, географії та змісту військових навчань на території держави потенційного агресора є одним з ключових показників, який впливає на рівень воєнної небезпеки.

2. Показники рівня воєнної небезпеки

Оцінка рівнів військової загрози включає різні методології, які враховують численні показники, включаючи військовий потенціал, геополітичні наміри та потенційну вразливість. Нижче наведено деякі відомі підходи та ресурси з детальним описом цих методологій [18-22].

Аналіз центру ваги (COG), цей метод визначає критичні компоненти сили супротивника, які, якщо їх нейтралізувати, значно послаблять його загальні можливості. Аналіз передбачає визначення критичних можливостей, вимог і вразливостей для ефективного націлювання.

Модель аналізу ризиків безпеки на морі (MSRAM). Розроблена Береговою охороною США, MSRAM оцінює ризики терористичних атак на морські цілі шляхом оцінки факторів загрози, наслідків і вразливості. Він підтримує прийняття рішень щодо розподілу ресурсів для пом'якшення виявлених ризиків.



Рисунок 1 – Стратегічні військові навчання рф та її союзників на кордоні з Україною

Проект індикаторів раннього попередження Варшавського договору. Ця історична методологія була зосереджена на моніторингу індикаторів, які могли сигналізувати про потенційні військові дії супротивників, сприяючи ранньому попередженню та прийняттю стратегічних рішень.

Кількісний розрахунок і прогнозування ситуаційної обізнаності на основі ризиків (QR-SACP). Нещодавнє дослідження пропонує кількісний метод розрахунку та проектування ситуаційної обізнаності в мережах на основі обміну інформацією про загрози, наголошуючи на важливості розуміння поширення загрози та потенційних наслідків.

Рівні загрози Великобританії. Сполучене Королівство використовує структуровану систему для класифікації рівнів терористичної загрози, починаючи від низького до критичного, спрямовуючи урядові та громадські дії щодо різного ступеня загрози.

Таким чином, з аналізу чинників, що впливають на рівень воєнної небезпеки, випливає, що вони здійснюють комплексний вплив, а тому у цілому визначення рівня воєнної небезпеки повинно базуватися на ґрунтовно обраній системі показників, які всебічно характеризують загальну обстановку в регіоні, напруженість у воєнно-політичних стосунках сторін, співвідношення потенційних можливостей збройних сил, наявність інтересів до України, для реалізації яких може знадобитись воєнна сила, а також впевненість воєнно-політичного керівництва сусідніх держав у доцільності збройного насильства як засобу досягнення політичних цілей.

На основі аналізу існуючих показників можна зробити висновок, що вони охоплюють важливі, але не всі аспекти оцінки рівня воєнної небезпеки. Зокрема, існують кілька ключових причин, чому ці показники потребують доповнення та уточнення:

обмеження у відображенні сучасних гібридних загроз. Сьогоднішні воєнні небезпеки значно ширші за традиційні військові дії. Оцінювати рівень загрози лише через співвідношення воєнних потенціалів чи підтримку сепаратистів недостатньо. Не враховано, наприклад, масштаб і частоту кібератак, дезінформаційних кампаній, впливу санкційних обмежень, які істотно впливають на обороноздатність і стійкість держави;

відсутність показників економічної стійкості. Хоча наведено рівень боротьби за ринки

збуту, це лише один із багатьох економічних чинників. Не враховано залежність від енергетичних ресурсів, логістичну вразливість, макроекономічну стабільність, які можуть суттєво впливати на здатність держави протистояти воєнним загрозам;

не враховано внутрішньополітичну стабільність. Ступінь соціальної напруженості у сусідніх країнах — це важливий показник, але потрібна більш широка оцінка внутрішніх політичних процесів. Наприклад, рівень політичної єдності, довіра до уряду, готовність населення до оборони — всі ці аспекти формують основу для національної безпеки;

інформаційний вплив та медійна вразливість. У списку відсутні показники, що оцінюють масштаби інформаційної агресії, медійної вразливості, поширення пропаганди і фейкових новин. Ці аспекти є невід'ємною частиною сучасних гібридних конфліктів, які можуть суттєво впливати на здатність держави протистояти загрозам.

глобальний контекст та зовнішні союзники. Важливо враховувати не лише рівень співробітництва з іншими державами, але й залежність від міжнародної допомоги, вплив глобальних військових конфліктів, геополітичну ситуацію в регіоні. Без таких показників картина воєнної небезпеки буде неповною.

Наведені показники є корисними для базового аналізу, але їх недостатньо для глибокої та повної оцінки рівня воєнної небезпеки.

Необхідність подальших досліджень в оцінці рівня воєнної небезпеки обумовлена низкою причин:

динамічний характер загроз. Воєнна небезпека є змінною величиною, яка залежить від багатьох факторів. Зміна військових технологій, розвиток гібридних методів впливу, поява нових геополітичних викликів вимагають постійного оновлення даних і підходів. Лише регулярні дослідження можуть забезпечити актуальність і точність оцінок;

неповнота поточних показників. Використані показники, хоча і відображають важливі аспекти, не охоплюють всієї складності сучасних конфліктів. Наприклад, кібератаки, інформаційна війна, економічні санкції, енергетична залежність — це важливі аспекти, які потребують додаткового дослідження для комплексної оцінки рівня загроз;

розширення аналітичного інструментарію. Існуючі методики можуть бути вдосконалені. Впровадження більш сучасних методів аналізу, таких як математичне моделювання, прогнозування на основі штучного інтелекту, багатофакторний аналіз ризиків, вимагає проведення глибоких досліджень та розробки нових підходів.

зміна регіональної та міжнародної обстановки. Геополітична ситуація в регіоні та світі постійно змінюється. З'являються нові актори, змінюються альянси, вводяться нові санкції чи розробляються нові оборонні стратегії. Вивчення цих змін є важливим для розуміння їхнього впливу на рівень воєнної небезпеки.

формування ефективних управлінських рішень. Без додаткових досліджень неможливо отримати глибоке розуміння причинно-наслідкових зв'язків між різними чинниками. Це обмежує здатність розробляти стратегії, які не лише реагують на вже існуючі загрози, але й запобігають новим.

Подальші дослідження необхідні для отримання повнішої картини воєнних загроз, удосконалення методик аналізу та прийняття більш обґрунтованих управлінських рішень. Вони дозволять швидше адаптуватися до змінної обстановки, вчасно виявляти нові загрози та ефективно їх нейтралізувати.

Проведений аналіз дозволяє запропонувати наступні показники рівня воєнної небезпеки, які враховуватимуть специфіку російсько-українського конфлікту:

1) Співвідношення воєнних потенціалів України та потенційного агресора;
2) Ступінь підтримки сепаратистських сил в Україні;
3) Наявність територіальних претензій до України з боку потенційного агресора (рф);
4) Заяви й акції, які дискредитують внутрішню і зовнішню політику України;

5) Рівень військового співробітництва потенційного агресора;

6) Ступінь впливу військової еліти на внутрішню і зовнішню політику держав потенційного агресора;

7) Рівень зацікавленості у стратегічних сировинних ресурсах України;

8) Рівень впливу релігійних центрів на конфесії в Україні;

9) Політична та дипломатична активність потенційного агресора, розвиток партнерства та союзів;

10) Рівень інформаційного тиску з боку потенційного агресора;

11) Військова активність потенційного агресора (військові навчання);

12) Ступінь соціальної напруженості в Україні;

13) Рівень боротьби за українські ринки збуту;

14) Інтенсивність кібератак, з боку потенційного агресора, які можуть вплинути на оперативну готовність сил оборони України.

3. Оцінювання рівня воєнної небезпеки для України на передодні повномасштабного вторгнення рф

Для визначення кількісних значень обраних показників оцінювання рівня воєнної небезпеки були використані як загальні статистичні данні, так і результати експертного опитування. В загальному в опитуванні взяли участь 10 експертів, які надали свою оцінку кожному з показників від 0 до 1. Де, 0 – відсутність впливу показника, а 1– максимальний вплив показника на стан воєнної небезпеки для України.

Узагальнені статистичні дані для усієї сукупності показників за роками, що розглядаються, а також результати експертного опитування наведені у (табл.1).

Таблиця 1 – Вихідні дані для оцінювання рівня воєнної небезпеки для України з боку рф

№ з/п	Показники	2017	2018	2019	2020	2021	2022
1	Наявність територіальних претензій до України з боку рф	1	1	1	1	1	1
2	Ступінь підтримки сепаратистських сил в Україні з боку рф	1	1	1	1	1	1
3	Співвідношення воєнних потенціалів України та рф	0,18	0,2	0,22	0,23	0,25	0,25
4	Рівень зацікавленості у стратегічних сировинних ресурсах України	0,6	0,7	0,8	0,8	0,8	0,9
5	Рівень боротьби за українські ринки збуту	0,7	0,8	0,7	0,7	0,8	0,85
6	Рівень впливу релігійних центрів на конфесії в Україні	0,6	0,5	0,4	0,4	0,5	0,55
7	Заяви й акції, які дискредитують внутрішню і зовнішню політику України	1	1	1	1	1	1
8	Ступінь соціальної напруженості в Україні	0,3	0,35	0,4	0,4	0,35	0,8
9	Рівень військового співробітництва	0,5	0,5	0,5	0,5	0,6	0,6
10	Ступінь впливу військової еліти на внутрішню і зовнішню політику держави	0,3	0,35	0,4	0,37	0,35	0,3
11	Військова активність потенційного агресора (навчання)	0,3	0,9	0,45	0,4	0,87	1
12	Інтенсивність кібератак, які можуть вплинути на оперативну готовність.	0,6	0,7	0,7	0,8	0,9	1
13	Рівень інформаційного тиску	0,8	0,9	0,8	0,9	0,9	1
14	Політична та дипломатична активність потенційного ворога, розвиток партнерства та союзів	0,7	0,7	0,9	0,8	0,9	1

Для обрахунку загального рівня воєнної небезпеки на основі вказаних показників і років, можна скористатися методом вагового сумування. Присвоєння вагових коефіцієнтів – нормалізуємо значення показників на шкалі від 0 до 1 і присвоюємо їм вагові коефіцієнти відповідно до їх важливості для визначення загального рівня воєнної небезпеки.

Розрахунок вагового сумарного балу за кожен рік розраховується шляхом множення значення кожного показника на його ваговий коефіцієнт і сумується для кожного року. Це дасть нам загальний рівень воєнної небезпеки за кожен рік.

Агрегація рівнів воєнної небезпеки за роками здійснюється сумуванням значення рівня воєнної небезпеки за кожен рік для отримання загального рівня воєнної небезпеки протягом усього періоду.



Рисунок 2 – Рівень воєнної небезпеки для України в період 2017-2022 років.

Як видно з графіка у 2018 році рівень воєнної небезпеки для України з боку рф зріс, але вже у 2019 та 2020 роках він дещо почав зменшуватися. Починаючи з 2021 року та на початку 2022 року рівень воєнної небезпеки почав знову різко зростати, що пов'язано з нарощуванням військового потенціалу рф на кордонах з Україною.

Виходячи з отриманих результатів авторами пропонується така класифікація рівнів воєнної небезпеки (табл. 2).

Станом на початок 2022 року рівень воєнної небезпеки зріс з "Середній рівень загрози" до рівня "Високий рівень загрози", що характеризувалося посиленням військової присутності агресора біля кордонів, проведення військових навчань, активна підтримка сепаратистських сил, використання політичного та інформаційного тиску. Така динаміка свідчила про те, що безпекова ситуація рухається до "Критичного рівня загрози" високої ймовірності збройного конфлікту.

Аналіз показав, що протягом 2017-2019 років рівень воєнної небезпеки залишався на відносно стабільному середньому рівні, хоча спостерігалося поступове зростання за деякими параметрами. Однак у 2021-2022 роках ситуація різко погіршилася, що свідчить про підготовку агресії.

Таблиця 2 – Класифікація рівнів воєнної небезпеки

Рівень військової небезпеки	Значення інтегрального показника	Характеристика рівня загрози
Критичний рівень загрози	≥ 30,0	Висока ймовірність збройного конфлікту, пряма військова загроза. Максимальна військова активність противника, проведення масштабних операцій, інформаційні атаки, кібератаки та економічний тиск.
Високий рівень загрози	25,0≤ ВНБ <30,0	Посилення військової присутності агресора біля кордонів, проведення військових навчань, активна підтримка сепаратистських сил, використання політичного та інформаційного тиску.
Середній рівень загрози	20,0≤ ВНБ <25,0	Підготовка до можливих військових дій, дипломатичний та політичний тиск, кібератаки середньої інтенсивності, військове навчання в прикордонних регіонах.
Низький рівень загрози	15,0≤ ВНБ <20,0	Відсутність іншої військової загрози, але активна інформаційна війна, економічні та політичні маніпуляції, часткове залучення гібридних загроз.
Мінімальний рівень загрози	<15,0	Відносно стабільна ситуація, наявні політичні та економічні проблеми, але відсутні критичні воєнні ризики.

Основними факторами, які спричинили погіршення ситуації у 2021-2022 роках є наступні:

нарощування військового потенціалу рф – співвідношення воєнних сил поступово змінювалося не на користь України;

збільшення військової активності – проведення рф масштабних військових навчань у прикордонних з Україною регіонах;

посилення кібератак – значне зростання атак на критичну інфраструктуру України, що свідчило про тестування тактики кібернетичних операцій;

інформаційний тиск – активізація російської пропаганди щодо “небезпечності” України, що стало частиною гібридної війни;

дипломатичний та економічний тиск – блокування стратегічних угод України, спроби дестабілізації української економіки;

висока активність дипломатичних маніпуляцій свідчила про спроби підготовки ґрунту для виправдання агресії.

Для формування обґрунтованих пропозицій щодо покращення прогнозованості та ефективного реагування на підвищення рівня воєнної небезпеки також використано метод кількісної оцінки ваги критеріїв для ухвалення рішень. Згідно проведених розрахунків до найбільш важливих показників оцінювання рівня воєнної небезпеки для України з боку рф належать наступні (рис. 4):

співвідношення воєнних потенціалів України та рф – 8,75;

ступінь підтримки сепаратистських сил в Україні з боку рф –8,75;

наявність територіальних претензій до України з боку рф – 7,25;

заяви й акції, які дискредитують внутрішню і зовнішню політику України –7,25;

рівень військового співробітництва – 7,25;

ступінь впливу військової еліти на внутрішню і зовнішню політику держави –7,02;

рівень зацікавленості у стратегічних сировинних ресурсах України – 6,25;

рівень впливу релігійних центрів на конфесії в Україні –6,21;

політична та дипломатична активність потенційного ворога, розвиток партнерства та союзів –5,79;

рівень інформаційного тиску –5,55;
військова активність потенційного агресора (навчання) –5,52;
ступінь соціальної напруженості в Україні –5,41;
рівень боротьби за українські ринки збуту –5,36;
інтенсивність кібератак, які можуть вплинути на оперативну готовність –5,18.

Провівши синтез отриманих нами суджень, об'єднавши надані оцінки загроз, можна сформулювати загальні пріоритети ієрархії для оцінки рівня воєнної небезпеки (табл. 4).

Таблиця 4 – Шкала пріоритетів показників для оцінки показників рівня воєнної небезпеки

Рівень пріоритету	Обґрунтування рівня	Діапазон показника
Критичний рівень загрози	Цей рівень відображає **безпосередню загрозу збройної агресії або стратегічного домінування противника**, що може призвести до серйозних наслідків для безпеки держави. Показники, що потрапляють у цей діапазон, мають визначальний вплив на можливість воєнного конфлікту, знищення критичної інфраструктури або зміну політичного курсу країни через військовий тиск. **Характеристика:** - противник має значну військову перевагу та можливість оперативного розгортання наступальних сил; - підтримка сепаратистських рухів та гібридних елементів досягла критичної позначки, що дозволяє швидко розпочати дестабілізаційні дії; - територіальні претензії активно використовуються як привід для ескалації конфлікту.	**≥ 7**
Високий рівень загрози	Цей рівень вказує на **суттєві ризики для безпеки, що можуть стати критичними у разі їх подальшого загострення**. Він охоплює **інформаційні, дипломатичні та військово-економічні методи тиску**, які використовуються агресором для послаблення обороноздатності країни. **Характеристика:** - активні інформаційні операції із метою дискредитації України на міжнародній арені та всередині країни; - посилення дипломатичної ізоляції шляхом міжнародного тиску; - використання військових союзників та посилення військового співробітництва рф для підготовки до можливих агресивних дій.	**6–7**
Середній рівень загрози	На цьому рівні загрози ще не досягли критичного масштабу, але **становлять потенційну небезпеку**, особливо в умовах ескалації або недостатнього реагування. - агресор здійснює економічний і ресурсний тиск, що може послабити стійкість країни; - м’які методи впливу (релігійні, соціальні, культурні, інформаційні) використовуються для поступового розхитування ситуації; - гібридні атаки, як-от кібератаки або локальні військові навчання, що маскують реальні наміри агресора.	**5 - 6**
Низький рівень загрози	Цей рівень означає, що **воєнна загроза має опосередкований характер, але її прояви можуть створити умови для майбутньої ескалації**. **Характеристика:** - інформаційний тиск, спроби дестабілізації суспільства (створення паніки, політичних криз, соціального незадоволення); - локальні провокації, економічний саботаж, тестування готовності сил безпеки України; - низькоінтенсивні кібератаки на державні установи та військові об’єкти.	**< 5**

Отримані пріоритети дозволяють сформувати рекомендації з підвищення рівня прогнозованості воєнної небезпеки для України, які пропонується розділити на декілька пунктів:

1) Посилення моніторингу та аналітики (збирання та аналіз інформації):

створення Національного центру стратегічного прогнозування. Об'єднання можливостей воєнної, зовнішньої та військової розвідки, а також цивільних аналітичних та дипломатичних структур, з метою оперативного моніторингу та аналізу загроз національній безпеці України;

запровадити систему постійного автоматизованого моніторингу. Впровадження автоматизованих систем, які в режимі реального часу здійснюють збір, аналіз та прогнозування загроз на основі методів штучного інтелекту, Big Data та машинного навчання;

використання штучного інтелекту (AI) та машинного навчання (ML). Впровадження технологій прогнозування воєнних загроз через AI та ML для виявлення аномалій у поведінці противника, раннього попередження про зростання напруженості, визначення характеру та ступеня загрози на ранній стадії.

2) Розширення міжнародної співпраці з партнерами:

збільшення обсягу розвідувального обміну інформацією з НАТО та ЄС. Регулярне оновлення бази даних спільних загроз, проведення регулярних консультацій і обміну аналітичною інформацією для кращого розуміння планів та намірів агресора;

запуск спільних програм раннього попередження. Створення з країнами-партнерами системи раннього попередження про можливі загрози, що дозволить забезпечити додатковий час для реагування;

використання міжнародних експертних платформ та конференцій. Організація постійно діючих міжнародних експертних груп з аналізу загроз та проведення спільних тренінгів, семінарів із залученням провідних міжнародних експертів.

3) Створення необхідних структур та інституцій:

створення державної автоматизованої системи раннього попередження (Early Warning System), яка включатиме моніторинг воєнних, економічних, соціальних, інформаційних загроз, автоматизовані системи оцінювання ризиків і прогнозування потенційних кризових ситуацій;

розвиток центрів із стратегічних комунікацій. Протидія інформаційним атакам і фейкам, оперативне інформування населення, міжнародних партнерів щодо загроз безпеці;

організація аналітичних центрів при регіональних військово-цивільних адміністраціях. Локальний моніторинг та прогнозування рівня загроз, оперативне реагування у регіонах з урахуванням місцевих особливостей.

4) Автоматизація процесів прогнозування та аналізу:

впровадження інтегрованих цифрових платформ єдина цифрова система обробки і аналізу даних, що об'єднує інформацію з розвідувальних служб, військових підрозділів, правоохоронних органів та міжнародних партнерів;

моніторинг соціальних мереж з використанням автоматичних систем аналізу контенту в соцмережах та ЗМІ для раннього виявлення інформаційних операцій, пропаганди, провокацій, які можуть передувати військовій агресії.

5) Використання новітніх технологій:

супутникові та геопросторові технології. Активізація використання супутникових знімків для моніторингу переміщень військ, військової інфраструктури, концентрації сил противника, раннього виявлення ознак підготовки до агресії;

безпілотні літальні апарати (БПЛА). Використання БПЛА для розвідки та збору даних в реальному часі, автоматизована ідентифікація та аналіз переміщень противника;

біометричні та аналітичні системи контролю. Впровадження технологій для контролю міграційних потоків, виявлення агентури, диверсійних груп, потенційних терористів.

6) Використання нових методик оцінювання:

метод сценарного аналізу (Scenario Planning). Використання сценарного аналізу для прогнозування різних варіантів поведінки противника, підготовка конкретних планів реагування на кожен із сценаріїв;

метод динамічного моделювання загроз. Побудова цифрових моделей розвитку потенційних військових конфліктів із подальшим імітаційним моделюванням сценаріїв розвитку ситуації;

використання інтегральних та багатокритеріальних моделей. Інтеграція різних методик кількісної та якісної оцінки рівнів воєнної небезпеки із формуванням інтегрального показника воєнної безпеки держави.

7) Вивчення та застосування міжнародного досвіду:

вивчення досвіду держав НАТО, використання кращих практик створення оборонних і прогнозних систем, досвіду боротьби з гібридними загрозами;

регулярне проведення міжнародних навчань та тренінгів. Обмін практичним досвідом у сфері протидії гібридним загрозам, військовим та кризовим сценаріям, проведення спільних навчань із партнерами;

залучення міжнародних консультантів та експертів. Використання консультативної допомоги експертів з країн, що мають досвід протидії воєнним та гібридним загрозам для постійного вдосконалення системи прогнозування.

8) Систематичне навчання та підвищення кваліфікації кадрів:

створення спеціалізованих навчальних програм для аналітиків, розвідників та офіцерів, підготовка фахівців із прогнозування, розвідки, обробки та аналізу інформації;

організація навчань із кризового реагування, регулярні тренування з моделювання сценаріїв реагування на загрози, міжвідомчі штабні навчання для покращення координації дій у кризових умовах.

Таким чином, запропоновані заходи комплексно забезпечать Україні можливість оперативно прогнозувати, своєчасно реагувати та ефективно протидіяти загрозам воєнної безпеки з боку інших держав, особливо рф, і значно підвищать обороноздатність і стійкість країни в умовах сучасних загроз.

Висновки

У ході проведеного дослідження було здійснено кількісний аналіз рівня воєнної небезпеки для України з боку російської федерації за період 2017–2022 рр. Виявлено, що воєнна небезпека демонструвала тенденцію до зростання, особливо критично це проявилося у 2021–2022 роках, що свідчило про підготовку до повномасштабної військової агресії.

Ключовими факторами загострення ситуації стали: суттєве нарощення військового потенціалу РФ, інтенсифікація військових навчань біля кордонів України, посилення кібератак, інформаційний та дипломатичний тиск. Найбільшу вагу серед аналізованих факторів отримали такі показники, як співвідношення воєнних потенціалів (8,75), ступінь підтримки сепаратистських сил (8,75), територіальні претензії (7,25) та заходи щодо дискредитації України (7,25).

На основі отриманих даних було запропоновано ієрархічну структуру загроз, яка дозволяє визначити пріоритети реагування залежно від критичності показників. Запропонована методика визначення пріоритетів дає змогу концентрувати ресурси та увагу на найбільш значущих загрозах, оптимізуючи прийняття рішень в умовах обмежених ресурсів.

Для підвищення ефективності прогнозування та своєчасного реагування на загрози рекомендовано впровадження автоматизованих систем моніторингу на основі штучного інтелекту, створення Національного центру стратегічного прогнозування, інтеграцію в

міжнародні системи раннього попередження та регулярний обмін аналітичною інформацією з країнами-партнерами.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Assessing Risk at the National Strategic Level: Visualization Tools for Military Planners. URL : https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=3078&context=parameters&utm_source=chatgpt.com. [Дата звернення: 17.03.2025].
2. Семененко, О., Ткач, І., Чернега, Т., Абрамова, М., Чугуй, Г., & Герасименко, О. (2025). Підхід до оцінювання рівня воєнно-економічної стійкості держави з урахуванням оцінок загроз національній безпеці. *Social Development and Security*, *15*(1), 44-58. https://doi.org/10.33445/sds.2025.15.1.5.
3. Суходоля О. Визначення рівня та оцінювання загроз енергетичній безпеці. Науковий журнал "Енергетична безпека України". – 2022. – № 1. – С. 45–62. – URL : https://www.researchgate.net/publication/366285653_Viznacenna_rivna_ta_ocinuvanna_zagroz_energeticnij_bezpeci. [Дата звернення: 17.02.2025].
4. Гогонянц С.Ю., Грицай П.М., Шапран О.О. Загальні положення методики оцінювання рівня воєнної небезпеки на основі таксономічних методів [Електронний ресурс] // Науковий журнал "Система інформаційної безпеки та управління". – 2019. – № 4. – С. 65–79. – URL : https://www.researchgate.net/publication/337461466_Zagalni_polozenna_metodiki_ocinuvanna_rivna_voennoi_nebezpeki_na_osnovi_taksonomicnih_metodiv. [Дата звернення: 17.02.2025].
5. Старцев В.В., Третяк В.Ф., Міхальова Л.В., Коломійцев О.В., Борщ В.В., Олійник Р.М. Основні положення методики оцінювання можливостей відновлення озброєння та військової техніки Повітряних Сил Збройних Сил України, пошкоджених під час ведення бойових дій. Збірник наукових праць "Дослідження та перспективи розвитку озброєння і військової техніки". – 2023. – № 1 (23). – С. 112–127. – URL : https://dndivsovt.com/index.php/journal/article/view/219. [Дата звернення: 17.01.2025].
6. Ткач, М., Ткач, І., Ясенко, С., Брітченко, І., & Лошонці, П. (2022). Методичні підходи щодо оцінювання воєнно-економічної спроможності країни. *Social Development and Security*, *12*(3), 81-97. https://doi.org/10.33445/sds.2022.12.3.8.
7. Богданович В., Муженко В., Луцький О. Концепція забезпечення воєнної безпеки України на основі оцінювання та прогнозування ризиків реалізації кризових сценаріїв. Збірник наукових праць. Серія: Військові та технічні науки. – 2023. – №4(93). – С. 4–16.
8. Косевцов В. О., Бінько І. Ф., Матвієвський О. М. Методичний підхід до аналізу й оцінки рівня національної безпеки та її складових. Наука і оборона. – 1995. – № 1. – С. 74-77.
9. Russian troop movements near Ukraine border prompt concern in U.S., Europe. URL : https://www.washingtonpost.com/world/russian-troop-movements-near-ukraine-border-prompt-concern-in-us-europe/2021/10/30/c122e57c-3983-11ec-9662-399cfa75efee_story.html?utm_source=chatgpt.com. [Дата звернення: 10.03.2025].
10. So könnte Putin die Ukraine vernichten. URL : https://www.bild.de/politik/ausland/politik-ausland/bild-exklusiv-russlands-kriegsplaene-so-koennte-putin-die-ukraine-vernichten-

78425518.bild.html. [Дата звернення: 10.03.2025].
11. Росія офіційно запропонувала НАТО відмовитися від подальшого розширення, в тому числі приєднання України. URL : https://lb.ua/news/2021/12/17/501196_rosiya_ofitsiyno_zaproponuvala_nato.html [Дата звернення: 17.02.2025].
12. Стратегічні зовнішньополітичні цілі рф щодо США, ЄС, Китаю та держав-партнерів України (Польща, Країни Балтії). URL : https://analytics.intsecurity.org/russia-foreign-policy-goals/. [Дата звернення: 10.02.2025].
13. З Москви до Києва: чого очікувати від візиту президента Франції Макрона в Україну. URL : https://suspilne.media/205026-z-moskvi-do-kieva-cogo-ocikuvati-vid-vizitu-prezidenta-francii-makrona-v-ukrainu/. [Дата звернення: 03.03.2025].
14. Блінкен у Радбезі ООН розповів, як Росія може створити привід для нападу на Україну. URL : https://www.eurointegration.com.ua/news/2022/02/17/7134182/13. [Дата звернення: 11.03.2025].
15. Звернення президента США Байдена щодо загроз для України. URL : https://www.radiosvoboda.org/a/zvernennya-baydena-ukrayina-rosiya/31710714.html. [Дата звернення: 17.12.2024].
16. США виводять війська з Афганістану: чому це важливо для України. URL : https://niss.gov.ua/news/statti/ssha-vyvodyat-viyska-z-afhanistanu-chomu-tse-vazhlyvo-dlya-ukrayiny. [Дата звернення: 17.12.2024].
17. В Україні та РФ одночасно розпочалися масштабні військові маневри. URL : https://informnapalm.org/ua/v-ukraini-ta-rf-odnochasno-rozpochalysia/. [Дата звернення: 17.03.2025].
18. Center of Gravity (COG) Analysis. Wikipedia. – URL : https://en.wikipedia.org/wiki/Center_of_gravity_(military). [Дата звернення: 15.03.2025].
19. Maritime Security Risk Analysis Model (MSRAM). Wikipedia. URL : https://en.wikipedia.org/wiki/Maritime_Security_Risk_Analysis_Model. [Дата звернення: 01.04.2025].
20. Warsaw Pact Early Warning Indicator Project. Wikipedia. URL : https://en.wikipedia.org/wiki/Warsaw_Pact_Early_Warning_Indicator_Project. [Дата звернення: 05.02.2025].
21. Quantitative Risk-based Situational Awareness Calculation and Projection (QR-SACP). Arxiv. URL : https://arxiv.org/abs/2304.14952. [Дата звернення: 10.03.2025].
22. UK Threat Levels. Wikipedia URL : https://en.wikipedia.org/wiki/UK_Threat_Levels. [Дата звернення: 21.02.2025].

References

1. Assessing Risk at the National Strategic Level: Visualization Tools for Military Planners. Available from : https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=3078&context=parameters&utm_source=chatgpt.com. [Data zvernennya: 17.03.2025].
2. Semenenko, O., Tkach, I., Cherneha, T., Abramova, M., Chuhui, H., & Herasymenko, O. (2025). The methodology for assessing the level of a state's military-economic sustainability considering national security threat evaluations. *Social Development and Security*, *15*(1), 44-58. https://doi.org/10.33445/sds.2025.15.1.5.
3. Sukhodolya O. Vyznachennya rivnya ta otsinyuvannya zahroz enerhetychniy bezpetsi. Naukovyy zhurnal "Enerhetychna bezpeka Ukrayiny". – 2022. – № 1. – S. 45–62. – Available from : https://www.researchgate.net/publication/366285653_Viznacenna_rivna_ta_ocinuvanna_zagroz_energeticnij_bezpeci. [Data zvernennya: 17.02.2025].

4. Hohonyants S.YU., Hrytsay P.M., Shapran O.O. Zahal'ni polozhennya metodyky otsinyuvannya rivnya voyennoyi nebezpeky na osnovi taksonomichnykh metodiv [Elektronnyy resurs] // Naukovyy zhurnal "Systema informatsiynoyi bezpeky ta upravlinnya". – 2019. – № 4. – S. 65–79. – Available from : https://www.researchgate.net/publication/337461466_Zagalni_polozenna_metodiki_ocinuvanna_rivna_voennoi_nebezpeki_na_osnovi_taksonomicnih_metodiv. [Data zvernennya: 17.02.2025].
5. Startsev V.V., Tretyak V.F., Mikhal'ova L.V., Kolomiytsev O.V., Borshch V.V., Oliynyk R.M. Osnovni polozhennya metodyky otsinyuvannya mozhlyvostey vidnovlennya ozbroyennya ta viys'kovoyi tekhniky Povitryanykh Syl Zbroynykh Syl Ukrayiny, poshkodzhenykh pid chas vedennya boyovykh diy. Zbirnyk naukovykh prats' "Doslidzhennya ta perspektyvy rozvytku ozbroyennya i viys'kovoyi tekhniky". – 2023. – № 1 (23). – S. 112–127. – Available from : https://dndivsovt.com/index.php/journal/article/view/219. [Data zvernennya: 17.01.2025].
6. Tkach, M., Tkach, I., Yasenko, S., Britchenko, I., & Lošonczi, P. (2022). Methodical approaches to assessing the military and economic capacity of the country. *Social Development and Security*, *12*(3), 81-97. https://doi.org/10.33445/sds.2022.12.3.8.
7. Bohdanovych V., Muzhenko V., Luts'kyy O. Kontseptsiya zabezpechennya voyennoyi bezpeky Ukrayiny na osnovi otsinyuvannya ta prohnozuvannya ryzykiv realizatsiyi kryzovykh stsenariyiv. Zbirnyk naukovykh prats'. Seriya: Viys'kovi ta tekhnichni nauky. – 2023. – №4(93). – S. 4–16.
8. Kosevtsov V. O., Bin'ko I. F., Matviyevs'kyy O. M. Metodychnyy pidkhid do analizu y otsinky rivnya natsional'noyi bezpeky ta yiyi skladovykh. Nauka i oborona. – 1995. – № 1. – S. 74-77.
9. Russian troop movements near Ukraine border prompt concern in U.S., Europe. Available from : https://www.washingtonpost.com/world/russian-troop-movements-near-ukraine-border-prompt-concern-in-us-europe/2021/10/30/c122e57c-3983-11ec-9662-399cfa75efee_story.html?utm_source=chatgpt.com. [Data zvernennya: 10.03.2025].
10. So könnte Putin die Ukraine vernichten. Available from : https://www.bild.de/politik/ausland/politik-ausland/bild-exklusiv-russlands-kriegsplaene-so-koennte-putin-die-ukraine-vernichten-78425518.bild.html. [Data zvernennya: 10.03.2025].
11. Rosiya ofitsiyno zaproponuvala NATO vidmovytysya vid podal'shoho rozshyrennya, v tomu chysli pryyednannya Ukrayiny. Available from : https://lb.ua/news/2021/12/17/501196_rosiya_ofitsiyno_zaproponuvala_nato.html [Data zvernennya: 17.02.2025].
12. Stratehichni zovnishn'opolitychni tsili rf shchodo SSHA, YES, Kytayu ta derzhav-partneriv Ukrayiny (Pol'shcha, Krayiny Baltiyi). Available from : https://analytics.intsecurity.org/russia-foreign-policy-goals/. [Data zvernennya: 10.02.2025].
13. Z Moskvy do Kyyeva: choho ochikuvaty vid vizytu prezydenta Frantsiyi Makrona v Ukrayinu. Available from : https://suspilne.media/205026-z-moskvi-do-kieva-cogo-ocikuvati-vid-vizitu-prezidenta-francii-makrona-v-ukrainu/. [Data zvernennya: 03.03.2025].
14. Blinken u Radbezi OON rozpoviv, yak Rosiya mozhe stvoryty pryvid dlya napadu na Ukrayinu. Available from : https://www.eurointegration.com.ua/news/2022/02/17/7134182/. [Data zvernennya: 11.03.2025].
15. Zvernennya prezydenta SSHA Baydena shchodo zahroz dlya Ukrayiny. Available from : https://www.radiosvoboda.org/a/zvernennya-baydena-ukrayina-rosiya/31710714.html. [Data zvernennya: 17.12.2024].
16. SSHA vyvodyat' viys'ka z Afhanistanu: chomu tse vazhlyvo dlya Ukrayiny. Available from : https://niss.gov.ua/news/statti/ssha-vyvodyat-viyska-z-afhanistanu-chomu-tse-vazhlyvo-dlya-ukrayiny. [Data zvernennya: 17.12.2024].

17. V Ukrayini ta RF odnochasno rozpochalysya masshtabni viys'kovi manevry. Available from : https://informnapalm.org/ua/v-ukraini-ta-rf-odnochasno-rozpochalysia/. [Data zvernennya: 17.03.2025].
18. Center of Gravity (COG) Analysis. Wikipedia. – Available from : https://en.wikipedia.org/wiki/Center_of_gravity_(military). [Data zvernennya: 15.03.2025].
19. Maritime Security Risk Analysis Model (MSRAM). Wikipedia. Available from : https://en.wikipedia.org/wiki/Maritime_Security_Risk_Analysis_Model. [Data zvernennya: 01.04.2025].
20. Warsaw Pact Early Warning Indicator Project. Wikipedia. Available from : https://en.wikipedia.org/wiki/Warsaw_Pact_Early_Warning_Indicator_Project. [Data zvernennya: 05.02.2025].
21. Quantitative Risk-based Situational Awareness Calculation and Projection (QR-SACP). Arxiv. Available from : https://arxiv.org/abs/2304.14952. [Data zvernennya: 10.03.2025].
22. UK Threat Levels. Wikipedia. Available from : https://en.wikipedia.org/wiki/UK_Threat_Levels. [Data zvernennya: 21.02.2025].

Резильєнтність і стійкість економіки: ключові теоретико-практичні наративи та воєнно-економічні уроки

Resilience and Sustainability: Key Theoretical-Practical Narratives and War-Economic Lessons

Олег Семененко [A]

Corresponding author: д. військ. наук, 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, старший науковий співробітник, e-mail: elaira3@gmail.com, ORCID: 0000-0001-7644-9988

Олег Тарасов [B]

к.військ.н., доцент, Кафедра військової підготовки, e-mail: tarasovo@ukr.net, ORCID:0000-0002-6763-8653

Сергій Митченко [C]

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

Роман Дзюбчук [D]

к. тех. наук, старший науковий співробітник, професор кафедри факультету лідерства, e-mail: rd_zt@ukr.net, ORCID: 0000-0001-6224-456X

Денис Фомкін [F]

науковий співробітник, e-mail: dfomkin@gmail.com, ORCID: 0000-0003-0128-9355

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]

Candidate of Economic Sciences, Senior Researcher, Senior Research Fellow, e-mail: Elaira3@gmail.com, ORCID: 0000-0001-7644-9988

Oleh Tarasov [B]

Candidate of Military Sciences, Associate Professor, e-mail: tarasovo@ukr.net, ORCID: 0000-0002-6763-8653

Serhii Mytchenko [C]

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

Roman Dziubchuk [D]

Candidate of Technical Sciences, Senior Researcher, Professor, Department of Leadership, e-mail: rd_zt@ukr.net, ORCID: 0000-0001-6224-456X

Denys Fomkin [F]

науковий співробітник, e-mail: dfomkin@gmail.com, ORCID: 0000-0003-0128-9355

[A] Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна
[B] Кафедра військової підготовки Національного авіаційного університету, Київ, Україна
[C] Національний університет оборони України, м. Київ, Україна
[D] Житомирський військовий інститут імені С.П. Корольова, Житомир, Україна
[F] Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна

[A] Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine
[B] Department of Military Training of the National Aviation University, Kyiv, Ukraine
[C] National Defense University of Ukraine, Kyiv, Ukraine
[D] Korolyov Zhytomyr military institute, Zhytomyr, Ukraine
[F] Military Institute of Telecommunications and Informatization named after Heroes of Kruty, Kyiv, Ukraine

Received: April 20, 2025 | Revised: April 28, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.24

Мета роботи: аналіз ключових теоретичних аспектів використання понятійних апаратів "стійкості" та "резильєнтності" економіки, їх взаємозв'язку та впливу на здатність економічних систем адаптуватися до змін і відновлюватися після криз.

Метод дослідження: аналізу; синтезу; порівняння; формалізації та оцінювання матеріалу; абстрагування та кон'юнктурного аналізу (мислення).

Результати дослідження: встановлено, що "резильєнтність" економіки є динамічним процесом, який забезпечує швидке відновлення національного господарства після шоків шляхом адаптації та структурних змін, тоді як "стійкість" економіки відображає здатність системи протистояти зовнішнім потрясінням без суттєвої трансформації; також визначено, що їх поєднання є критичним для підтримки воєнної могутності (ВМ) держав та забезпечення довгострокового економічного розвитку, а також висвітлено, що розвиток транснаціональних процесів може як сприяти відновленню (резильєнтності), так і створювати додаткові ризики стабільному розвитку ВМ.

Теоретична цінність дослідження: полягає в уточненні концептуальних відмінностей між понятійними апаратами "стійкості" та "резильєнтності" економіки, розкритті їх взаємодії, у контексті адаптації до криз та відновлення економічного потенціалу, а також у визначенні ключових чинників, що сприяють довгостроковій стабільності та розвитку економік.

Тип статті: теоретичний**,** описовий, практичний, методичний.

Purpose: to analyse the main theoretical aspects of the formation of the conceptual apparatus of "sustainability" and "resilience" of the economy, their interrelationship and their impact on the ability of economic systems to adapt to change and recover from crises.

Method: analysis; synthesis; comparison; formalization and evaluation of the material; abstraction and conjunctural analysis (thinking).

Findings: the authors notes that the "resilience" of the economy is a dynamic process that ensures rapid recovery of the national economy aftershocks through adaptation and structural changes, while the "sustainability" of the economy reflects the ability of the system to withstand external shocks without significant transformation; he also notes that their combination is crucial for maintaining the military power of states and ensuring long-term economic development, and emphasizes that the development of transnational processes can contribute both to recovery (resilience) and to sustainability (sustainability).

Theoretical implications: is to clarify the conceptual differences between the conceptual apparatus of "sustainability" and "resilience" of the economy, to reveal their interaction in the context of crisis adaptation and recovery of economic potential, and to identify key factors that contribute to the long-term stability and development of economies.

Paper type: theoretical, descriptive, practical, methodical.

Ключові слова: резильєнтність, стійкість, транснаціональні процеси, воєнна могутність, відновлення, економіка, розвиток.

Key words: resilience, sustainability, transnational processes, military power, recovery, economy, development.

Вступ

Нині національні господарства функціонують в умовах динамічних змін та глобальних викликів, що вимагає від них спроможності не лише протистояти зовнішнім змінам, а й швидко адаптуватися до нових умов. Тому розуміння розмежування специфіки "стійкості" та "резильєнтності" економік стають ключовими для аналізу визначення механізмів економічного відновлення та забезпечення довгострокової стабільності. А дослідження цих категорій дозволяє визначити напрямки, що сприяють економічній адаптивності, та формулюванню ефективних стратегем подолання кризових ситуацій. Особливу увагу варто приділити зв'язку між економічною резильєнтністю та ВМ держави, що є критично важливим у сучасному геополітичному контексті впливу російсько-української війни на регіональну стабільність.

Теоретичні основи дослідження

Дослідження понятійного апарату "resilience" (відновлення) та "sustainability" (стійкості) набули значного поширення у багатьох наукових дисциплінах, зокрема в екології, економіці, соціології, психології та управлінні. Теоретичні основи цих концепцій закладалися поступово, об'єднуючи знання з різних галузей для розуміння механізмів адаптації, відновлення та довготривалого функціонування систем.

"Resilience", зазвичай, розглядається в контексті здатності систем (природних, соціальних, економічних) адаптуватися до змін, зберігаючи свої ключові функції. Вперше цей термін широко почав використовуватися в екології завдяки роботам К. Голлінга у 1970-х роках. Надалі концепція поширилася на інші сфери, наприклад, у соціальних науках "resilience" описує, як спільноти або окремі особи долають кризи та адаптуються до нових умов. "Sustainability", своєю чергою, розглядається як здатність систем підтримувати стабільний стан у довготривалій перспективі, не виснажуючи природні ресурси та не порушуючи рівновагу між соціальними, економічними та екологічними потребами. Концепція набрала актуальності після публікації доповіді "Наше спільне майбутнє" (1987), де було сформульовано визначення сталого розвитку. Дослідження цих двох концепцій мають велике значення для управління ризиками, екологічної політики, урбаністики та економічного розвитку. "Resilience" та "sustainability" часто взаємопов'язані: перша забезпечує адаптивність у короткостроковій перспективі, а друга – стабільність у довгостроковій. Вивчення цих категорій дозволяє створювати більш ефективні стратегії розвитку суспільств, бізнесу та природних систем, що є особливо важливим в умовах глобальних криз та кліматичних змін.

Постановка проблеми

Дослідження стійкості та відновлення економіки є важливими етапами для забезпечення довгострокового зростання, мінімізації наслідків криз та розробки ефективних стратегій економічного розвитку. Сьогодні постає необхідність розмежування понять "стійкості" та "резильєнтності" у контексті дослідження економічних процесів, оскільки в науковій літературі та практиці ці терміни часто використовуються взаємозамінно, хоча мають різне значення. Тому потреба у формуванні цілісного підходу до аналізу резильєнтності економіки, яка, на відміну від стійкості, передбачає не просто здатність протистояти зовнішнім впливам, а й активне пристосування до нових умов спрямована на визначення ключових факторів, що впливають на здатність економіки до швидкого відновлення, а також аналіз їх взаємозв'язку з ВМ держави. Таким чином, є доцільним дослідити специфіку застосування термінології резильєнтності економіки у контексті сучасних викликів та загроз, включаючи глобальні кризи, структурні трансформації та адаптацію до змінних економічних умов.

Результати

Для розкриття понятійного апарату “резильєнтності” є доцільним звернути увагу на те, що розуміння структурних і граматичних відмінностей між англійською та українською мовами є вирішальним для ефективного перекладу, особливо коли йдеться про спеціалізовану термінологію. Орієнтування у відсутності прямих еквівалентів для спеціалізованої або новоствореної термінології є ще однією серйозною проблемою, тому в деяких випадках англомовні терміни не мають прямого перекладу, що змушує перекладачів створювати нові понятійні апарати українською мовою або адаптувати існуючі відповідно до контексту. Наприклад, “оборонний менеджмент” та “оборонне управління” англійською мовою звучать однаково – “defense management”, однак відповідно до реалій України – це два різних за суттю процеси. Такі адаптації потребують глибокого розуміння вихідної та цільової мов, а також предмета, щоб гарантувати, що нові або змінені терміни точно відображали необхідне значення.

Щодо поняття “резильєнтності” – її концепцію в 1973 р. було запропоновано С. Холлінгом як основу для екологічних досліджень, але з часом її стали застосовувати до соціальних та економічних сфер, хоча, як відмічає Дж. Сімі, узгодженої й однозначної операційної концепції досі не існує та поняття “резильєнтності” є близьким до таких понять, як “стійкість”, “стабільність”, “опір”, але основний його зміст пов’язаний з “пружністю”, “еластичністю”, “гнучкістю” та зазвичай відображає швидкість, з якою система повертається у свій початковий стан після удару (шоку), поглинає негативні імпульси (табл. 1).

Наприклад, К. Холлінг поняття “резильєнтності” трактує як показник динаміки, що відображає швидкість, з якою система повертається в стабільний стан після шоку. Е. Вернер розглядає його як здатність будь-якої системи, яка перебувала у кризовому стані, до постшокового відновлення та адаптації до середовища, що змінилося. С. Халагейт визначає сутність “резильєнтності” як забезпечення знаходження системи у стані стабільності, стійкості, невразливості. Дж. Брістоу розуміє резильєнтність як збереження можливостей для подальшого розвитку. Натомість Д. Маккінон впевнений, що це здатність системи поглинати збурення та реорганізовуватися під час змін, щоб зберегти свої функції, структуру, ідентичність та зворотні зв’язки.

Отже, зазвичай “резильєнтність” розглядається як потенціал системи для збереження її конфігурацій і функцій, а також здатність структури до самореорганізації. Згідно з визначенням, що було надано Р. Вінком, “резильєнтність” розглядається як здатність уникати криз, протистояти їм або адаптуватися до них і допомогти стати можливостями, необхідними того, щоб впоратися з негативним шоком і несприятливими умовами. Е. Браун визначав “резильєнтність” як внутрішню властивість системи до протистояння зовнішнім ризикам, що створені глобальними потоками інвестицій, екологічними та економічними кризами. У стратегічних документах таких міжнародних організацій, як ОЕСР, ЄС, ООН та ін., сутність поняття “резильєнтність” трактується як визначальна ознака безпеки в ситуації потрясінь, а також як здатність рекомбінувати ресурси для досягнення динамічної рівноваги на старому або на новому рівні розвитку, порушеної спонтанними внутрішніми або зовнішніми шоками.

Аналізуючи наведені визначення сутності поняття “резильєнтність”, можна виділити два підходи до його розуміння. За першим підходом “резильєнтність”, розглядається, як повернення до вже існуючої точки рівноваги; за другим – як постійна адаптація до мінливих умов. Критерієм резильєнтності за першим підходом є норма повернення в початковий стан (значну роль у цьому процесі відіграє “сила” шоку – інтенсивність і тривалість впливу на економічну систему), за другим підходом – еластичність економічної системи. Але обидва підходи визначають, що резильєнтність передбачає внутрішню здатність економічної системи змінюватися (“згинатися”) та відновлюватися після негативного впливу (шоку) внаслідок структурної адаптації (рис. 1).

Таблиця 1 – Еволюція понятійного апарату “резильєнтності”(“resilience”) у світовій практиці

Автор(-и), рік	Сутність поняття
М. Раттер, 1985	Феномен взаємодії захисних факторів, факторів ризику (індивідуальних, сімейних і соціокультурних впливів)
Е. Вернер, 1993	Балансування факторів ризику та захисних факторів
А. Міллер, 2003	Здатність швидко відновлювати ресурси
Г. Бонанно, 2004	Динамічний процес встановлення позитивної адаптації в контексті несприятливих явищ; адаптація ресурсів до мінливих обставин і непередбачених умов навколишнього середовища
Г. Річардсон, 2007	Процес боротьби з шоками, змінами та несприятливими фа
L. Briguillo, 2006	Здатність економіки відновлюватися або адаптуватися до впливу несприятливих потрясінь
R. Дюваль, 2007	Здатність економіки підтримувати обсяги виробництва близькими до потенційних у відповідь на шоки та потрясіння
І. Роза, 2007	Здатність системи підтримувати функціонування в умовах шоку
А. Хілл, 2008	Здатність економіки успішно відновлюватися після потрясінь, які викликають або уповільнення зростання, або його істотно обмежують
R. Мартін., 2012	Здатність економіки у відповідь на потрясіння адаптувати свою структуру за для підтримки прийнятного зростання виробництва, зайнятості та добробуту з плином часу
І. Роуз, А. Краусманн, 2013	Здатність економіки до швидкого відновлення після шоку
N. Хендерсон, 2013	Внутрішні захисні фактори, що сприяють підвищенню стійкості
D. Маккіннон, К. Д. Деріксон, 2013	Фундаментальна основа того, як найкраще підтримувати функціонування існуючої системи перед обличчям зовнішніх проблем
D. Де Вертей, О. Голубчиков, 2016	Здатність підтримувати альтернативні та вже існуючі практики, зачерпувати виживання, діючи як попередник до трансформаційних дій, шоків
С. Галагейт, 2016	На макрорівні визначається як комбінація миттєвої стійкості, тобто здатності обмежити суму негайних втрат доходу заданою сумою втрати капіталу, та динамічної стійкості, тобто здатності швидко відновлюватися; швидко поглинати удари та відновлювати характеристики системи
OECD, SIDA, 2017	Здатність системи перебудовувати свої елементи та ключові ресурси мобільним способом для досягнення динамічної стійкості на новому рівні розвитку як відповідь на раптові внутрішні або зовнішні збурення
Ш. Аккерман, 2019	Здатність і тенденція “приходити в норму”
Н. Смородинська, V. Малигін, 2021	Новий підхід до забезпечення стійкості національних економік в умовах входження світу в епоху складності, нелінійності та радикальної невизначеності
Cambridge Business English Dictionary, 2022	Здатність швидко повертатися до попереднього позитивного стану після проблем
Oxford Advanced Learner's Dictionary, 2022	Здатність людей або речей швидко відновлюватися після чогось неприємного, такого як шок тощо

Джерело: узагальнено на основі [1 – 24]

Якщо стан стійкості економічної системи можна розглядати як дії передподієвого характеру, що спрямовані на нівелювання чи “пом’якшення” наслідків майбутніх криз. Тоді, “резильєнтність” – це властивість економічної системи, яка має постподієвий характер, що дозволяє поглинати або пом’якшувати втрати, перелаштовувати, відновлювати її стан завдяки внутрішнім адаптивним властивостям після впливу шоків різного характеру.

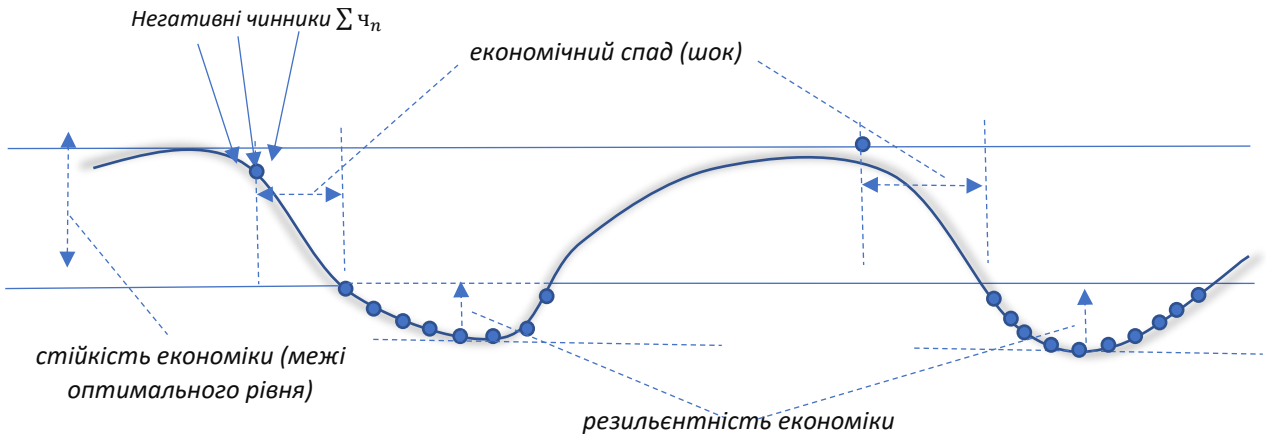


Рисунок 1 – Схематичне відображення реакції економіки на вплив негативних чинників ззовні – економічна резильєнтність (“economic resilience”)

Джерело: позиція авторів

Наведене вище визначення поняття “резильєнтність” дозволяє виділити дві групи чинників усередині самої системи, що її забезпечують:

“природні” чинники економічної системи: структура економіки, стан і тенденції її розвитку, ресурсний потенціал, здатність заміщати втрачені ресурси, стан та особливості ринку праці, здатність промислових ринків перерозподіляти ресурси та ін.;

“набуті” чинники, що характеризують адаптивність економічної системи: здатність пом’якшувати наслідки шоків та кризових ситуацій завдяки додатковим зусиллям (наприклад, державній політиці, національній інноваційній системі, наявному фінансуванню та ін.).

В даній роботі “резильєнтність економіки” розглядається як здатність відновлення спроможностей економік країн досягти меж оптимального рівня свого функціонування за рахунок власних фінансових, матеріальних та виробничих можливостей.

Однак разом із резильєнтністю економіки виділяють й її стійкість. Вона відіграє ключову роль у зміцненні потенціалу національної безпеки, забезпечуючи міцний фундамент для оборонного сектору країни. За стійкої економіки зберігається доступ до ресурсів, необхідних для підтримки і модернізації військової інфраструктури. Це дозволяє фінансувати та інвестувати в оборонні технології на достатньому рівні, здійснювати підготовку особового складу та стратегічні операції, тим самим зміцнюючи національну безпеку. Крім того, економічна стійкість часто призводить до політичної стабільності, яка є не менш важливою для підтримання надійної оборонної системи. Політична стабільність зменшує ймовірність внутрішніх конфліктів і забезпечує чіткий стратегічний напрямок оборонної політики. По суті, стійка економіка створює середовище, в якому може процвітати національна безпека, таким чином посилюючи взаємозв’язок між економічним відновленням і підвищенням ВМ країни.

Із-за наявної проблематики розмежування понять “стійкості” та “резильєнтності” у вітчизняному науковому світі пропонується звернутися до першоджерел, а саме тлумачень мовних понять (табл. 2).

Отже якщо брати за основу поняття, що використовується дослідниками University of Cambridge, а також Oxford University у сфері економіки та бізнесу, тоді терміну “resilience” (“здатності швидко повертатися до попереднього позитивного стану після проблем” та “здатність людей або речей швидко відновлюватися після чогось неприємного”) більш притаманний переклад “відновлення” в українській інтерпретації.

Таблиця 2 – Понятійний апарат “стійкості” (“sustainability”) у світовій практиці

Автор(-и), рік	Сутність поняття
Cambridge Advanced Learner's Dictionary & Thesaurus, 2002	ситуація, в якій навряд чи щось переміститься або зміниться, стан міцно фіксований або малоймовірний рух або зміна
Тлумачний словник української мови: у 2 т., 2000	Здатний твердо стояти, триматися, не падаючи, не коливаючись; протиле жне хисткий
Український тлумачний словник, 1997	Здатність зберігати первісний стан рівноваги при дії на них зовнішніх сил
Сучасний тлумачний словник української мови, 2009	Сталий, усталений, незмінний, повсякчасний, завсідний, твердий, тривкий, тривалий, витривалий, непохитний
Словник української мови у 20 томах, 2010–2023	Здатний зберігати даний стан, незважаючи на дію різних сил; не схильний до коливань, постійний, стійкий

Джерело: узагальнено на основі [24 – 33]

Складний зв’язок між економічною стійкістю та підвищенням ВМ був предметом значного інтересу серед науковців. На збереження економічної стійкості позитивно має вплив низький рівень інфляції, безробіття та збалансованість бюджету, які разом сприяють розвитку середовища для залучення інвестицій. Її забезпечення має першочергове значення для створення міцної військової влади, оскільки забезпечує фінансову основу, необхідну для належного фінансування оборонних витрат і нарощення військового потенціалу (рис. 2).

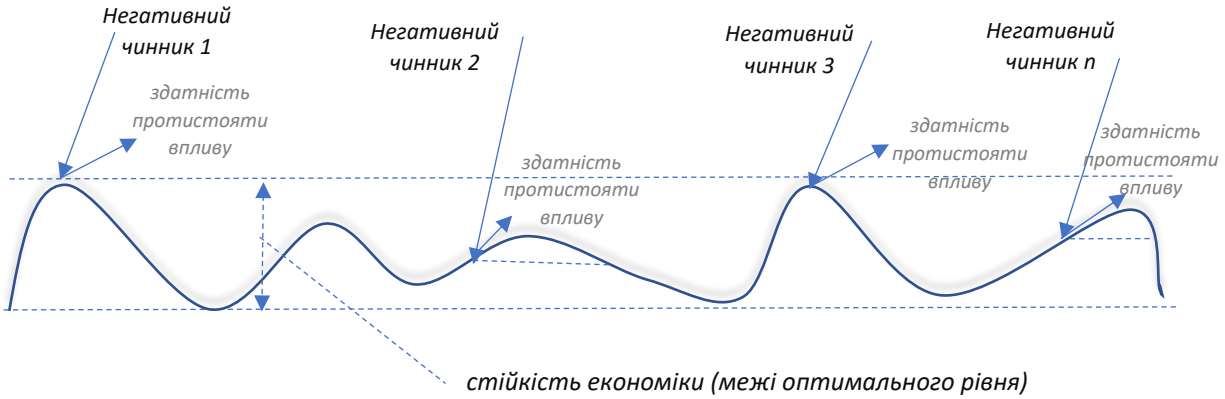


Рисунок 2 – Схематичне відображення реакції економіки на вплив негативних чинників ззовні – економічна стійкість (“economic sustainability”).

Джерело: позиція авторів

Економічне зростання безпосередньо залежить і від здатності інвестувати у власні ЗС, закуповуючи передові технології та підтримуючи боєготовність для забезпечення обороноздатності країни. Наприклад, протягом 1950-х і 1960-х років США пережили значне економічне зростання, що дозволило отримати безпрецедентне військове фінансування, що призвело до створення передового технологічного арсеналу, включаючи розробку ядерної зброї та авіації. Подібним чином військовий розвиток Радянського Союзу під час “холодної війни” був підтриманий його масштабними зусиллями з індустріалізації. Однак надзвичайно важливо визнати, що економічна стійкість не може ґрунтуватися лише на багатстві, її забезпечення також вимагає ефективного політичного управління та розумної фіскальної політики, яка визначає пріоритетні витрати на оборону.

Вплив економічних ресурсів на обсяги військового фінансування додатково ілюструють такі країни, як Німеччина та Японія, які після Другої світової війни відбудували свої економіки та згодом створили сильні, на той час, військові сили. Економічна стійкість цих країн, яка характеризувалася потужними промисловими секторами та технологічними інноваціями, заклала основу для оборонного потенціалу, який можна було мобілізувати під час кризи. Таким чином, економічна стійкість слугує основою, на якій будується військова міць, гарантуючи, що країни можуть підтримувати свою обороноздатність за умов невизначеності.

Економічні спади часто призводять до скорочення бюджету, що безпосередньо впливає на військове фінансування, що призводить до зниження можливостей і готовності. Наприклад, під час фінансової кризи 2008 року кілька країн, зокрема Велика Британія та Греція, зіткнулися із жорсткими заходами економії, які вимагали значного скорочення оборонних бюджетів. Ці скорочення не тільки перешкоджали зусиллям з модернізації військ, але й створювали проблеми з підтримання рівня особового складу та оперативної готовності. Взаємозв'язок між економічними кризами та викликами національній безпеці стає очевидним при розгляді випадку Греції, яка, зіткнувшись з економічною нестабільністю, за якої її військовий потенціал зменшився, що зрештою вплинуло на її здатність ефективно реагувати на регіональні загрози. Історичні прецеденти, такі як міжвоєнний період після Першої світової війни, додатково ілюструють, як економічна нестабільність може спровокувати військові невдачі. Такі країни, як Німеччина, які зіткнулися з гіперінфляцією та економічним колапсом, пережили глибоке зниження своєї військової ефективності, що сприяло зростанню екстремістських рухів і прокладало шлях до Другої світової війни. Уроки, отримані з цих прикладів, підкреслюють критичну необхідність для націй підтримувати збалансований підхід до управління економікою та військової готовності, оскільки наслідки ігнорування однієї сфери можуть призвести до жахливих наслідків для національної безпеки та глобальної стабільності.

Наявно чимало історичних прикладів, які ілюструють заплутаний зв'язок між економічним відновленням і підвищенням ВМ вказуючи на те як економічне пожвавлення може посилити військовий потенціал, тоді як військова міць може одночасно сприяти економічному зростанню або, навпаки, виснажувати національні ресурси. За своєю суттю ВМ складається з кількох найважливіших компонентів, включаючи живу силу, технологічний прогрес, матеріально-технічну потужність і стратегічний потенціал. Міцна економіка забезпечує необхідні ресурси для фінансування військових ініціатив, розробки нових технологій і підтримки боєздатних ЗС. Створення НАТО продемонструвало, як економічне відновлення в Західній Європі було нерозривно пов'язане з військовими альянсами, оскільки механізми колективної оборони забезпечували безпеку, дозволяючи країнам зосередитися на економічній відбудові.

Декілька країн продемонстрували симбіотичний зв'язок між економічним відновленням і військовою експансією, продемонструвавши, як економічне зростання може сприяти модернізації військ. США, наприклад, пережили значне економічне відродження після Другої світової війни, яке супроводжувалося значним військовим розширенням. Післявоєнний бум дозволив уряду США інвестувати значні кошти в оборонні технології, сприяючи створенню передової зброї, встановленню глобальної військової присутності та формуванню стратегічних альянсів. Подібним чином економічні реформи Китаю, розпочаті наприкінці 1970-х років, мали глибокі наслідки для його військової модернізації. Коли Китай перейшов до ринково-орієнтованої економіки, він пережив безпрецедентне економічне зростання, що дозволило суттєво збільшити витрати на оборону. Ця економічна потужність дозволила Китаю посилити свій військовий потенціал за рахунок розвитку передових технологій, таких як кібервійна та проектування військово-морської сили.

Одним із наслідків впливу економічних криз є необхідність відновлення (резильєнтності) економіки з урахуванням збереження військового потенціал країни характеризується раптовими порушеннями економічної діяльності, такими як серйозні спади виробництва, високий рівень безробіття та різке падіння ВВП. Це може призвести до бюджетних обмежень, які безпосередньо вплинуть на військові витрати та потенціал. Багато історичних прикладів, таких як Велика депресія 1930-х років, під час якої такі країни, як Німеччина та США, зіткнулися з різким скороченням військових витрат та економічного потенціалу.

Цікаво, що зв'язок між забезпеченням ВМ та економічним відновленням наявна парадоксальна динаміка. Під час економічного спаду фінансування військових потреб може спричинити навантаження на національні бюджети, відволікаючи необхідні ресурси від секторів, які можуть стимулювати економічне зростання, таких як освіта та інфраструктура. Фінансова криза 2008 року є яскравим прикладом того, як економічні потрясіння можуть змінити військові пріоритети. Після кризи США зазнали значних скорочень бюджету в різних секторах, включаючи оборону, що призвело до скорочення військових витрат приблизно на 20% протягом кількох років. Це зменшення фінансових ресурсів не тільки зупинило нові військові проєкти, але й змусило Пентагон переглянути свої глобальні військові зобов'язання, що вплинуло на здатність США демонструвати свою владу на міжнародному рівні. Подібним чином криза в єврозоні підкреслила крихкість європейської військової співпраці, оскільки такі країни, як Греція та Іспанія, зіткнулися з економічними заходами економії, які змусили їх різко скоротити оборонні бюджети. Ці скорочення перешкоджали спільним військовим ініціативам і створювали напругу в альянсах всередині НАТО. На Близькому Сході постійна економічна нестабільність, посилена конфліктами та політичними заворушеннями, призвела до ослаблення військового потенціалу кількох держав.

Отже між резильєнтністю, стійкістю та ВМ існує прямий зв'язок (рис. 3).

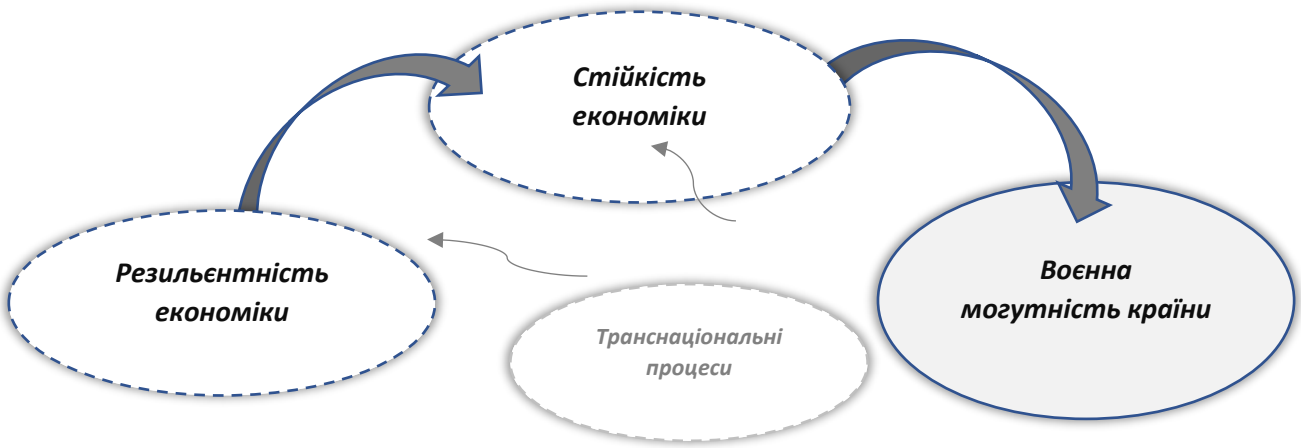


Рисунок 3 – Схематична інтерпретація зв'язку воєнної могутності країни із резильєнтністю та стійкістю її економіки.

Джерело: позиція авторів

Без відновлення економіки до дошокового рівня – стійкість її довгострокового сталого функціонування стає під загрозою, а звідси – знижуються спроможності країни забезпечувати на належному рівні свою власну ВМ із-за відволікання фінансових ресурсів на подолання наслідків шоку (кризи).

За таких обставин є важливим врахування наслідків дії транснаціональних процесів, що виходять за рамки національних кордонів та служать джерелами ресурсів, знань і технологічних досягнень, які є критично важливими в умовах економічного відновлення.

Розуміння ролі цих процесів має вирішальне значення для аналізу того, як країни оговтуються від криз, оскільки вони сприяють переміщенню товарів, послуг і капіталу через кордони тощо.

Наприклад, реакція на фінансову кризу 2008 року наголосила на важливості глобальних ланцюгів постачання для стабілізації економіки. Країни, які змогли використати ці мережі, такі як Німеччина та Південна Корея, відчули відносно швидке відновлення завдяки тісній інтеграції у світові ринки.

Можливість доступу до сировини та комплектуючих з різних країн дозволила цим країнам підтримувати рівень виробництва, тим самим уникаючи серйозніших наслідків кризи, яка вдарила по менш інтегрованих економіках. Крім того, транснаціональна співпраця, прикладом якої є скоординована відповідь G20 на рецесію, спричинену пандемією, ілюструє, як країни можуть об'єднатися, щоб сформулювати політику, яка підвищить економічну резильєнтність. Обмінюючись ресурсами, знаннями та передовим досвідом, країни можуть не тільки швидше відновлюватися, але й створювати надійніші рамки для майбутніх криз.

Міжнародні організації відіграють вирішальну роль у зміцненні економік та сприянні економічному відновленню, особливо в країнах, які серйозно постраждали від криз. В тому числі такі установи, як МВФ і Світовий банк, відіграють важливу роль у наданні фінансової допомоги та програмах підтримки, адаптованих до конкретних потреб постраждалих країн. Наприклад, під час пандемії COVID-19 МВФ активував механізми екстреного фінансування, які виділили кошти більш ніж 80 країнам, дозволяючи їм вирішувати негайні проблеми охорони здоров'я та економіки. Крім того, ініціативи Світового банку, такі як кредити Міжнародної асоціації розвитку (IDA), надають пільгові позики та гранти найбіднішим країнам, гарантуючи, що вони мають необхідні ресурси для стабілізації своєї економіки. Крім фінансової допомоги, ці організації також беруть участь у технічній допомозі та ініціативах з розбудови потенціалу, спрямованих на посилення місцевого управління та інституційних структур.

Оснащуючи країни інструментами, необхідними для реалізації ефективної політики та ефективного управління ресурсами, ці організації сприяють довгостроковій стійкості. Однак ефективність цих ініціатив часто залежить від політичної волі та структурної спроможності країн-реципієнтів, що робить важливим адаптувати програми підтримки до місцевих умов для досягнення оптимального впливу. За допомогою цих багатогранних підходів міжнародні організації не тільки допомагають країнам оговтатися від економічних невдач, але й закладають основу для сталого розвитку.

Незважаючи на потенційні переваги транснаціональних процесів економічного відновлення, деякі виклики можуть підірвати їх ефективність і призвести до несприятливих результатів. Одним із значних занепокоєнь є ризик залежності від іноземної допомоги та інвестицій, що може створити коло вразливості для країн-реципієнтів. Наприклад, країни, які значною мірою покладаються на зовнішню допомогу, можуть опинитися в нестабільному становищі, нездатні проводити незалежну економічну політику або робити довгострокові інвестиції у національну промисловість.

Ця залежність може пригнічувати місцеві інновації та підприємництво, оскільки ресурси перенаправляються на задоволення потреб іноземних інвесторів або організацій з надання допомоги. Крім того, транснаціональне втручання може мати негативний вплив на місцеву економіку та ринки праці. Приплив іноземного капіталу може призвести до втрати робочих місць у традиційних секторах, оскільки багатонаціональні корпорації віддають перевагу максимізації прибутку над місцевою зайнятістю.

Аполітична та соціальна напруга, яка виникає внаслідок цих втручань, може посилити існуючу нерівність і сприяти обуренню серед місцевого населення. Випадок із Замбією, де гірничодобувні компанії критикували за погіршення навколишнього середовища та експлуатацію робочої сили, є прикладом того, як присутність іноземних організацій може призвести до соціальних заворушень. Така динаміка ілюструє складність процесів

транснаціонального економічного відновлення, підкреслюючи необхідність збалансованого підходу, який враховує як переваги глобальної співпраці, так і захист місцевих інтересів.

Висновки

Резильєнтність економіки є ключовою характеристикою, що відображає здатність економічної системи адаптуватися до змін і швидко відновлювати свої функції після негативного впливу. Вона відрізняється від стійкості, яка визначає здатність системи протистояти зовнішнім шокам і зберігати баланс без суттєвих трансформацій. Аналіз наукових теорії свідчить, що резильєнтність можна трактувати як динамічний процес, що включає здатність до гнучкого пристосування, тоді як стійкість більшою мірою акцентує увагу на збереженні поточного стану системи. З історичної перспективи можна простежити, що резильєнтність економіки сприяє забезпеченню національної безпеки, оскільки міцна економічна основа дає змогу країні підтримувати свою ВМ, при цьому економічні кризи та спади призводять до скорочення військових витрат, що може послаблювати обороноздатність. Водночас країни, що швидко адаптуються до змін, за допомогою ефективної економічної політики можуть не лише відновлювати економічне зростання, але й використовувати кризи як можливості для модернізації та технологічного прориву.

Роль транснаціональних процесів у забезпеченні резильєнтності економік також є важливим аспектом дослідження, а інтеграція у світові ринки, доступ до міжнародних інвестицій та технологій сприяють швидшому відновленню після криз. Однак надмірна залежність від зовнішньої підтримки може створювати додаткові ризики, пов’язані із вразливістю до глобальних фінансових та політичних потрясінь.

Таким чином, формування політики економічної резильєнтності має спиратися на комплексний підхід, що включає розвиток внутрішніх адаптивних механізмів, збереження стратегічного балансу між стійкістю та гнучкістю, а також раціональне використання міжнародних ресурсів. Це дозволить забезпечити довгострокову стабільність економічного розвитку та підвищити здатність країн ефективно реагувати на виклики сучасного глобалізованого світу.

Перспективами подальших досліджень доцільно встановити розроблення методики оцінювання зв’язку між резильєнтністю економіки та ВМ, дослідити механізми адаптації економічних систем до криз і вивчити роль міжнародних організацій у підтримці економічної стабільності іноземних держав.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Wink, R. (2014). Regional economic resilience: Policy experiences and issues in Europe. *Raumforschung und Raumordnung: Spatial Research and Planning, 72(2)*, 85–91. https://doi.org/10.1007/s13147-013-0265-4.
2. Brown, E. D., & Williams, B. K. (2015). Resilience and resource management. *Environmental Management, 56(6)*, 1416–1427. https://doi.org/10.1007/s00267-015-0582-1.
3. Walker, B. (2020). Resilience: What it is and is not. *Ecology and Society, 25(2),* Article 11. https://doi.org/10.5751/ES-11647-250211.
4. Jonas, A. E. G. (2012). Region and place: Regionalism in question. *Progress in Human Geography,*

36(2), 263–272. https://doi.org/10.1177/03091325103941.
5. National Infrastructure Advisory Council (U.S.). (2009). *Critical infrastructure resilience: Final report and recommendations.* National Infrastructure Advisory Council.
6. Haldon, J., et al. (2021). Between resilience and adaptation: A historical framework for understanding stability and transformation of societies into shocks and stress. In *COVID-19: Systemic risk and resilience* (pp. 235–268). Springer. https://doi.org/10.1007/978-3-030-71587-8_14.
7. Bristow, G., & Healy, A. (2017). Innovation and regional economic resilience: An exploratory analysis. *The Annals of Regional Science, 60(5)*, 265–284. https://doi.org/10.1007/s00168-017-0841-6.
8. MacKinnon, D., & Derickson, K. D. (2013). From resilience to re-resourcefulness: A critique of resilience policy and activism. *Progress in Human Geography, 37(2)*, 53–70. https://doi.org/10.1177/03091325124547.
9. De Verteuil, G., & Golubchikov, O. (2016). Can resilience be redeemed? *City, 20(1)*, 143–151. https://doi.org/10.1080/13604813.2015.1125714.
10. Hallegatte, S. (2016). *Economic resilience: Definition and measurement.* World Bank. https://doi.org/10.1596/1813-9450-6852.
11. Вінк, Р. (ред.). (2021). *Економічна резильєнтність у регіонах та організаціях.* Springer.
12. Rutter, M. (2005). Resilience in the face of adversity: Protective factors and resistance to psychiatric disorder. *The British Journal of Psychiatry, 147*, 598–611. https://doi.org/10.1192/bjp.147.6.598.
13. Werner, E. (2003). Risk, resilience, and recovery: Perspectives from the Kauai longitudinal study. *Development and Psychopathology, 5(4)*, 503–515. https://doi.org/10.1017/S095457940000612X.
14. Bonanno, G. A. (2004). Loss, trauma, and human resilience: Have we underestimated the human capacity to thrive after extremely adverse events? *American Psychologist, 59(1)*, 20–28. https://doi.org/10.1037/0003-066X.59.1.20.
15. Cambridge University Press. (2022). *Cambridge business English dictionary.* Cambridge University Press.
16. Hornby, A. S. (Ed.). (2022). *Oxford advanced learner's dictionary.* Oxford University Press.
17. Бусел, В. Т. (Ред.). (2000). *Тлумачний словник української мови (Том 1).* Перун.
18. Єрмоленко, С. Я., Шевченко, Л. О., & Симоненко, Т. В. (1997). *Український тлумачний словник.* Абрис.
19. Дудко, Т., & Панько, О. (2009). *Сучасний тлумачний словник української мови.* Торсінг.
20. Наукова думка. (2010–2023). *Словник української мови у 20 томах.* НАН України, Інститут мовознавства ім. О. О. Потебні.
21. Tymchyshyn-Chemerys, J. (2019). Features of economic security of the region as a composition of national economic security. *International Scientific Journal "Internauka," (4).* https://doi.org/10.25313/2520-2057-2019-4-4826.
22. Onofriichuk, A. (2024). Роль і місце процесів забезпечення воєнно-економічної стійкості держави в системі національної безпеки: Теоретичні аспекти. *Міжнародний науковий журнал «Military Science», 2(3),* 64–74. https://doi.org/10.62524/msj.2024.2.3.05.
23. Ivanov, S. (2024). Peculiarities of economic resilience as an important scientific category for ensuring national security. *Bulletin of Taras Shevchenko National University of Kyiv. Public Administration, 19(1),* 74–79. https://doi.org/10.17721/2616-9193.2024/19-13/22.
24. Скляр, Н. (2021). Поняття комплексної потужності держави при оцінці воєнно-економічної складової сектору безпеки і оборони. *Економіка та суспільство, (27).* https://doi.org/10.32782/2524-0072/2021-27-19.
25. Study.com. (2023). Political risk in international business / Examples & analysis. https://study.com/academy/lesson/international-corporate-finance-political-risk.html
26. Food Standards Agency. (2023). *Consumer insights tracker report March 2022 – March 2023.*

https://doi.org/10.46756/sci.fsa.her886.
27. Wilson, J. (n.d.). The impact of the global supply chain crisis. *Imperial College London.* URL : https://www.imperial.ac.uk/stories/global-supply-chain-crisis
28. The White House. (2009). *The economic impact of the American Recovery and Reinvestment Act of 2009: First quarterly report.* URL : https://obamawhitehouse.archives.gov/administration/eop/cea/Economic-Impact
29. Alsen, A., & Veiga, F. J. (2011). How does political instability affect economic growth? *International Monetary Fund.*
30. Malloryk, A. (n.d.). Great responsibilities and new global power. *The National WWII Museum, New Orleans.* URL : https://www.nationalww2museum.org/war/articles/new-global-power-after-world-war-ii-1945
31. McCormick, J. M. (2000). Clinton and foreign policy. *Postmodern Presidency*, 60–84. https://doi.org/10.2307/jj.11660139.6.
32. U.S. Department of State. (n.d.). *Diplomacy in action.* URL : https://2009-2017.state.gov/r/pa/ei/rls/dos/107330.htm
33. Ng, M. (2022). State of trade 2022: The benefits of free trade agreements. *Office of the Chief Economist.* URL : https://www.international.gc.ca/transparency-transparence/state-trade-commerce-international/2022.aspx?lang=eng

References

1. Wink, R. (2014). Regional economic resilience: Policy experiences and issues in Europe. *Raumforschung und Raumordnung: Spatial Research and Planning, 72(2)*, 85–91. https://doi.org/10.1007/s13147-013-0265-4.
2. Brown, E. D., & Williams, B. K. (2015). Resilience and resource management. *Environmental Management, 56(6)*, 1416–1427. https://doi.org/10.1007/s00267-015-0582-1.
3. Walker, B. (2020). Resilience: What it is and is not. *Ecology and Society, 25(2),* Article 11. https://doi.org/10.5751/ES-11647-250211.
4. Jonas, A. E. G. (2012). Region and place: Regionalism in question. *Progress in Human Geography, 36(2)*, 263–272. https://doi.org/10.1177/03091325103941.
5. National Infrastructure Advisory Council (U.S.). (2009). *Critical infrastructure resilience: Final report and recommendations.* National Infrastructure Advisory Council.
6. Haldon, J., et al. (2021). Between resilience and adaptation: A historical framework for understanding stability and transformation of societies into shocks and stress. In *COVID-19: Systemic risk and resilience* (pp. 235–268). Springer. https://doi.org/10.1007/978-3-030-71587-8_14.
7. Bristow, G., & Healy, A. (2017). Innovation and regional economic resilience: An exploratory analysis. *The Annals of Regional Science, 60(5)*, 265–284. https://doi.org/10.1007/s00168-017-0841-6.
8. MacKinnon, D., & Derickson, K. D. (2013). From resilience to re-resourcefulness: A critique of resilience policy and activism. *Progress in Human Geography, 37(2)*, 53–70. https://doi.org/10.1177/03091325124547.
9. De Verteuil, G., & Golubchikov, O. (2016). Can resilience be redeemed? *City, 20(1)*, 143–151. https://doi.org/10.1080/13604813.2015.1125714.
10. Hallegatte, S. (2016). *Economic resilience: Definition and measurement.* World Bank. https://doi.org/10.1596/1813-9450-6852.
11. Вінк, Р. (ред.). (2021). *Економічна резильєнтність у регіонах та організаціях.* Springer.
12. Rutter, M. (2005). Resilience in the face of adversity: Protective factors and resistance to psychiatric disorder. *The British Journal of Psychiatry, 147*, 598–611. https://doi.org/10.1192/bjp.147.6.598.
13. Werner, E. (2003). Risk, resilience, and recovery: Perspectives from the Kauai longitudinal study. *Development and Psychopathology, 5(4)*, 503–515.

https://doi.org/10.1017/S095457940000612X.
14. Bonanno, G. A. (2004). Loss, trauma, and human resilience: Have we underestimated the human capacity to thrive after extremely adverse events? *American Psychologist, 59(1)*, 20–28. https://doi.org/10.1037/0003-066X.59.1.20.
15. Cambridge University Press. (2022). *Cambridge business English dictionary.* Cambridge University Press.
16. Hornby, A. S. (Ed.). (2022). *Oxford advanced learner's dictionary.* Oxford University Press.
17. Бусел, В. Т. (Ред.). (2000). *Тлумачний словник української мови (Том 1).* Перун.
18. Єрмоленко, С. Я., Шевченко, Л. О., & Симоненко, Т. В. (1997). *Український тлумачний словник.* Абрис.
19. Дудко, Т., & Панько, О. (2009). *Сучасний тлумачний словник української мови.* Торсінг.
20. Наукова думка. (2010–2023). *Словник української мови у 20 томах.* НАН України, Інститут мовознавства ім. О. О. Потебні.
21. Tymchyshyn-Chemerys, J. (2019). Features of economic security of the region as a composition of national economic security. *International Scientific Journal "Internauka," (4).* https://doi.org/10.25313/2520-2057-2019-4-4826.
22. Onofriichuk, A. (2024). Роль і місце процесів забезпечення воєнно-економічної стійкості держави в системі національної безпеки: Теоретичні аспекти. *Міжнародний науковий журнал «Military Science», 2(3),* 64–74. https://doi.org/10.62524/msj.2024.2.3.05.
23. Ivanov, S. (2024). Peculiarities of economic resilience as an important scientific category for ensuring national security. *Bulletin of Taras Shevchenko National University of Kyiv. Public Administration, 19(1),* 74–79. https://doi.org/10.17721/2616-9193.2024/19-13/22.
24. Скляр, Н. (2021). Поняття комплексної потужності держави при оцінці воєнно-економічної складової сектору безпеки і оборони. *Економіка та суспільство, (27).* https://doi.org/10.32782/2524-0072/2021-27-19.
25. Study.com. (2023). Political risk in international business | Examples & analysis. https://study.com/academy/lesson/international-corporate-finance-political-risk.html
26. Food Standards Agency. (2023). *Consumer insights tracker report March 2022 – March 2023.* https://doi.org/10.46756/sci.fsa.her886.
27. Wilson, J. (n.d.). The impact of the global supply chain crisis. *Imperial College London.* URL : https://www.imperial.ac.uk/stories/global-supply-chain-crisis
28. The White House. (2009). *The economic impact of the American Recovery and Reinvestment Act of 2009: First quarterly report.* URL : https://obamawhitehouse.archives.gov/administration/eop/cea/Economic-Impact
29. Alsen, A., & Veiga, F. J. (2011). How does political instability affect economic growth? *International Monetary Fund.*
30. Malloryk, A. (n.d.). Great responsibilities and new global power. *The National WWII Museum, New Orleans.* URL : https://www.nationalww2museum.org/war/articles/new-global-power-after-world-war-ii-1945
31. McCormick, J. M. (2000). Clinton and foreign policy. *Postmodern Presidency*, 60–84. https://doi.org/10.2307/jj.11660139.6.
32. U.S. Department of State. (n.d.). *Diplomacy in action.* URL : https://2009-2017.state.gov/r/pa/ei/rls/dos/107330.htm
33. Ng, M. (2022). State of trade 2022: The benefits of free trade agreements. *Office of the Chief Economist.* URL : https://www.international.gc.ca/transparency-transparence/state-trade-commerce-international/2022.aspx?lang=eng

Психолого-педагогічна підтримка дітей і молоді в умовах воєнного стану. Фокус: емоційне відновлення, безпека в освіті, адаптація до змін

Psychological and Pedagogical Support for Children and Youth in Martial Law. Focus: Emotional Recovery, Safety in Education, Adaptation to Change

Олег Семененко [A]

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

Лілія Семененко [B]

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

Олександр Водчиць [C]

к.тех.наук, доцент, начальник кафедри військової підготовки, e-mail: agv64agv@gmil.com, ORCID: 0000-0002-3294-76323

Марія Ярмольчик [C]

доктор філософії, начальник науково-дослідної лабораторії, e-mail: LinkinFan357@ukr.net, ORCID: 0000-0001-9917-0189

Станіслав Петренко [C]

викладач, e-mail: aosemenenko@ukr.net, ORCID: 0000-0001-5369-1683

Максим Поливода [C]

старший викладач, e-mail: polivodamo@ukr.net, ORCID: 0000-0002-4673-008X

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

Lilia Semenenko [B]

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

Oleksandr Vodchyts [C]

Candidate of Technical Sciences, Associate Professor, Head of the Department of Military Training, e-mail: avg64avg@gmail.com, ORCID: 0000-0002-3294-7632

Mariia Yarmolchyk [C]

Doctor of Philosophy, Head of the Research Laboratory, e-mail: LinkinFan357@ukr.net, ORCID: 0000-0001-9917-0189

Stanislav Petrenko [C]

Lecturer, e-mail: aosemenenko@ukr.net, ORCID: 0000-0001-5369-1683

Maksym Polyvoda [C]

Senior Lecturer, e-mail: polivodamo@ukr.net, ORCID:0000-0002-4673-008X

[A] Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна
[B] Національний університет оборони України, м. Київ, Україна
[C] Кафедра військової підготовки Національного авіаційного університету, Київ, Україна

[A] Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine
[B] National Defense University of Ukraine, Kyiv, Ukraine
[C] Department of Military Training of the National Aviation University, Kyiv, Ukrain

Received: April 20, 2025 | Revised: April 28, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.25

Мета роботи: розглянути основні особливості психолого-педагогічної підтримки українських дітей і молоді в умовах воєнного стану. Головний фокус дослідження сконцентрувати на емоційному відновленні дітей і молоді під час війни, забезпеченні безпеки в освіті, та адаптації до змін.

Метод дослідження: робота базується на аналізі ефективних інструментів емоційного відновлення, розробленні механізмів забезпечення психологічної безпеки в освітніх закладах та сприянні формуванню життєстійкості дітей і підлітків у сучасних умовах нестабільності.

Результати дослідження: проведено аналіз сучасних досліджень з теми психолого-педагогічної підтримки дітей і молоді в умовах воєнного стану; визначено ключові напрями виміру психолого-педагогічної підтримки дітей і молоді в умовах воєнного стану; проведено аналіз складових кожного виміру та визначено проблеми – особливості – шляхи вирішення цих проблем; розроблено практичні рекомендації для підвищення психолого-емоційного відновлення дітей і молоді в умовах триваючого воєнного стану в Україні.

Теоретична цінність дослідження: стаття розширює наукові уявлення про психолого-педагогічну підтримку українських дітей і молоді в умовах воєнного стану. Запропоновані підходи та рекомендації можуть бути

Purpose: to consider the main features of psychological and pedagogical support for Ukrainian children and youth in martial law. The main focus of the study is to concentrate on the emotional recovery of children and youth during the war, ensuring safety in education, and adaptation to change.

Method: The work is based on the analysis of effective tools for emotional recovery, the development of mechanisms for ensuring psychological safety in educational institutions, and the promotion of the resilience of children and adolescents in modern conditions of instability.

Findings: an analysis of modern research on the topic of psychological and pedagogical support for children and youth in martial law conditions was conducted; key areas of measurement of psychological and pedagogical support for children and youth in martial law conditions were identified; an analysis of the components of each dimension was conducted and problems - features - ways to solve these problems were identified; practical recommendations were developed to improve the psychological and emotional recovery of children and youth in the conditions of ongoing martial law in Ukraine.

Theoretical implications: The article expands scientific ideas about psychological and pedagogical support for Ukrainian children and youth under martial law. The proposed approaches and recommendations can be used to improve state policy in the

використані для вдосконалення державної політики у сфері освітньої діяльності та розробки освітніх програм.
Тип статті: теоретичний, описовий, практичний, методичний.

field of educational activities and the development of educational programs.
Paper type: theoretical, descriptive, practical, methodical.

Ключові слова: воєнний стан, гуманітарна місія, діти та молодь, психологічна боротьба, освіта, психолого-педагогічна підтримка, військова освіта, психологічна безпека в освіті, емоційне відновлення, професійна підготовка, освітні технології.

Key words: martial law, humanitarian mission, children and youth, psychological struggle, education, psychological and pedagogical support, military education, psychological safety in education, emotional recovery, professional training, educational technologies.

Вступ

Сучасні реалії воєнного стану в Україні, спричинені повномасштабною агресією російської федерації, кардинально змінюють не лише геополітичну ситуацію у світі, але й щоденне життя кожної української родини, зокрема дітей і молоді. Війна проникає в освітній простір, сімейні стосунки, психоемоційне середовище, залишаючи глибокий слід у психіці, поведінці та системі цінностей неповнолітніх громадян [1].

У таких умовах питання психолого-педагогічної підтримки дітей і молоді набуває виняткового значення. Це не лише гуманітарний, а й стратегічний напрям, що визначає майбутнє країни. Розв'язання проблем емоційного відновлення, гарантування безпечного освітнього середовища, формування здатності до адаптації у змінених обставинах є ключовими чинниками збереження психологічного здоров'я, соціальної стійкості та освітнього потенціалу підростаючого покоління [2].

Особливої актуальності дана тематика набуває у контексті триваючої російсько-української війни, в умовах якої Україна вимушено стала полігоном не лише воєнного протистояння, але й психологічної боротьби за свідомість і добробут власних громадян. Діти та молодь переживають численні травмуючі фактори: втрату близьких, вимушене переміщення, дезінтеграцію соціальних зв'язків, нестабільність і загрози в навчальному процесі, що вимагає комплексної психолого-педагогічної відповіді [3].

Попри те, що інші країни лише починають переймати український досвід реагування на ці виклики, сама Україна змушена в оперативному порядку формувати національні підходи, моделі й методики підтримки дітей і молоді. Саме тому наукове вивчення психолого-педагогічної підтримки в умовах воєнного стану є не лише своєчасним, але й вкрай необхідним для забезпечення цілісного розвитку особистості, підтримки емоційного балансу та стабільності освітнього процесу [4].

Теоретичні основи дослідження

Аналіз сучасних досліджень з теми психолого-педагогічної підтримки дітей і молоді в умовах воєнного стану [1–14] виявляє значну увагу до трьох ключових напрямів, а саме: емоційного відновлення, забезпечення психологічної безпеки в освіті та сприяння адаптації до змін. Огляд основних джерел, що висвітлюють ці аспекти, показує, що така проблематика надзвичайно актуальна у світі, бо війни продовжуються, а масштаби та їх наслідки тільки зростають, що негативно відбивається на психологічному та емоційному стані не тільки дітей та молоді, але й їх батьків. Психолого-емоційний баланс у світі порушений, а наслідки його ще нас чекають в майбутньому.

Проведемо аналіз основних сучасних джерел, які тим чи іншим чином торкаються тематики дослідження. Розглянемо, які аспекти вони розкривають, а які залишилися без уваги авторів.

Наприклад, розглянемо тему дослідження за напрямами:

1. Емоційне відновлення: робота з травмою та стресом.

У [5] показано значне зростання внутрішніх (тривога, депресія) та зовнішніх (поведінкові) проблем у дітей після початку повномасштабної війни в Україні. Основними факторами ризику виявлено прямий досвід війни та стрес батьків. Необхідні подальші

дослідження щодо довгострокових наслідків війни на психічне здоров'я дітей та підвищення ефективності втручань.

У [6] описано зростання кількості дітей, які звертаються за психологічною допомогою, та підкреслюється важливість арт-терапії та інших методів для емоційного відновлення. Визначено необхідність систематичних досліджень ефективності різних терапевтичних методів у контексті війни.

2. Психологічна безпека в освіті: школа як простір підтримки.

Порівняльне дослідження в Україні та Польщі у [7] аналізує готовність майбутніх учителів працювати з дітьми, які постраждали від війни. Виявлено потребу в розвитку стійкості та медіаграмотності педагогів. Необхідно розробити програми підготовки вчителів до роботи в кризових умовах.

Пілотне дослідження в у [8] оцінює ефективність психосоціальних втручань для дітей під час війни в Україні, зосереджуючись на зниженні стресу та покращенні міжособистісного функціонування. Автори визначають необхідність масштабних досліджень для підтвердження ефективності таких втручань.

3. Адаптація до змін: розвиток стійкості та гнучкості.

Дослідження у [9] виявило п’ять ключових процесів, що сприяють стійкості української молоді: позитивне мислення, почуття контролю, усвідомлення та регуляція емоцій, близькі особисті стосунки та підтримка спільноти. Необхідні програми, що навчають молодь навичкам стійкості та адаптації.

У [10] підкреслена ефективність психологічних втручань у підвищенні стійкості молоді, що пережила військові дії. Потрібні дослідження щодо довгострокової ефективності таких втручань.

4. Особливі групи: діти з інтелектуальними порушеннями.

Дослідження у [11] розглядає психологічну підтримку дітей з інтелектуальними порушеннями в умовах війни, виявляючи високий рівень стресу та потребу в спеціалізованій допомозі. Необхідно розробити адаптовані програми підтримки для цієї вразливої групи.

Незважаючи на наявні результати досліджень, але сьогодні в умовах триваючої війни існує потреба в: розробці та впровадженні довгострокових програм психологічної підтримки для дітей та молоді; підготовці педагогів до роботи в умовах кризи та з дітьми, які пережили травму; створенні адаптованих програм для особливих груп, таких як діти з інтелектуальними порушеннями; проведенні масштабних досліджень ефективності різних втручань та програм підтримки.

Постановка проблеми

Повномасштабна війна, розв’язана російською федерацією проти України, спричинила безпрецедентні виклики для системи освіти, психічного здоров’я та соціального середовища, у якому зростають діти й молодь. Порушення звичного укладу життя, досвід втрати, евакуації, руйнування, постійна загроза небезпеки – усі ці фактори призводять до глибоких травматичних переживань, які особливо гостро позначаються на психоемоційному стані дітей та підлітків.

Попри те, що низка вітчизняних і міжнародних досліджень уже торкаються питань емоційної травми, шкільного середовища як чинника безпеки, а також формування стійкості в умовах війни, їх здебільшого характеризує фрагментарність або зосередженість на окремих аспектах. Не вироблено цілісного підходу до психолого-педагогічної підтримки дітей та молоді, що б одночасно охоплював емоційне відновлення, забезпечення психологічної безпеки в освітньому просторі та формування адаптивності до змін – як нової реальності, в якій доводиться жити й навчатися.

Крім того, залишаються недостатньо вивченими питання ефективності практик психологічної підтримки в умовах тривалого воєнного конфлікту, особливо для дітей із особливими освітніми потребами, переміщених осіб, тих, хто зазнав окупації або втрати. Водночас зростає запит на підготовку педагогів до роботи в умовах кризи, інтеграцію психолого-педагогічної підтримки в освітню політику громад і трансформацію освіти як простору відновлення, а не додаткової травматизації.

У цьому контексті постає нагальна потреба в комплексному дослідженні підходів, практик і моделей психолого-педагогічної підтримки дітей і молоді в умовах воєнного стану. Такий аналіз має на меті виявити ефективні інструменти емоційного відновлення, розробити механізми забезпечення психологічної безпеки в освітніх закладах та сприяти формуванню життєстійкості дітей і підлітків у сучасних умовах нестабільності.

Результати

Вимір психолого-педагогічної підтримки охоплює три ключові напрями, а саме: емоційного відновлення дітей і підлітків; забезпечення психологічної безпеки в освітньому середовищі; сприяння адаптації до змін як нової норми життя.

1. Емоційне відновлення: цілеспрямована робота з травмою.

Війна – це травма, яка зачіпає навіть тих, хто фізично не перебуває в зоні бойових дій. Діти втрачають рідних, змушені тікати з дому, стають свідками руйнувань, гинуть під час обстрілів або проживають досвід окупації. Ці події формують посттравматичні реакції, які без належної підтримки ризикують трансформуватись у довготривалі порушення психоемоційного розвитку.

Сьогодні впевнено можна стверджувати, шо емоційне відновлення має бути інституціоналізованим, інтегрованим у шкільну, дошкільну та позашкільну освіту.

До основних конкретних напрямів реалізації можна віднести:

психологічна перша допомога (ППД) – обов’язкова навичка для кожного педагога, вихователя, шкільного психолога;

тренінги для освітян із виявлення тривожних симптомів, деструктивної поведінки, втрати інтересу до життя;

різні види терапії – арттерапія, казкотерапія, ігротерапія – ефективні інструменти безпечного опрацювання травматичного досвіду;

групи взаємопідтримки серед дітей, зокрема тих, хто є внутрішньо переміщеними особами або пережив окупацію;

присутність стабільного, чуйного дорослого (вчителя, наставника, батька/матері) як чинник емоційної рівноваги дитини.

Психолого-педагогічна підтримка – це не тільки про допомогу фахівця. Це нова культура взаємодії з дитиною або підлітком, де кожен дорослий має бути емоційно грамотним, уважним і надійним.

2. Психологічна безпека в освіті: школа як опора, а не джерело стресу.

У воєнних умовах школа перестає бути лише навчальним закладом – вона перетворюється на острів соціальної стабільності. Це місце, де дитина має отримати відчуття спокою, захищеності та передбачуваності.

Однак на практиці ситуація складна, тому що: достатньо значна кількість шкіл не мають укриттів; не обладнані тривожними кнопками чи системами оповіщення; шкільні психологи перевантажені, або відсутні зовсім; педагоги часто не мають наставництва та підтримки у кризових ситуаціях.

Що потрібно робити? Дамо відповіді на це запитання:

по-перше – визначити національні мінімальні стандарти безпеки у закладах освіти – як фізичної, так і емоційної;

по-друге – розробити алгоритми дій у разі тривоги, обстрілу, панічної атаки – доступні дітям, вчителям, батькам;

по-третє – впровадити психоедукацію – регулярні заняття про емоції, саморегуляцію, навички подолання стресу;

по-п’яте – створити територіальні психологічні служби, які працюватимуть із громадами, школами, гуртками;

по-шосте – стимулювати профілактику емоційного вигорання серед учителів через групи підтримки, супервізії, відновлювальні практики.

Ключовим меседжом для усіх повинно стати те, що школа має бути простором довіри, а не джерелом тривоги. Саме тут дитина має відчути, що її бачать, чують і розуміють.

3. Адаптація до змін: формування гнучкості та життєстійкості.

Сучасне покоління українських дітей живе в умовах постійної турбулентності: евакуації, зміна форм навчання, втрата домівки, вимушена міграція, відсутність стабільного майбутнього. Саме тому критично важливо сформувати у них адаптивне мислення, психологічну гнучкість та навіть базові навички самодопомоги.

Завдання педагогіки у воєнний час – переорієнтувати освіту на:

смисли, а не лише знання, тобто зменшити кількість фактологічного матеріалу, натомість приділити увагу критичному мисленню, творчості, комунікації;

адаптивний підхід до навчання, тобто зміст, темп, формат повинні відповідати психоемоційному стану дитини, а не лише календарному плануванню;

цифрову трансформацію, тобто організація безперервного навчання навіть у евакуації, в укриттях чи на тимчасово окупованих територіях;

підготовку дітей до життя в змінному середовищі, тобто навчити ставити запитання, планувати, помилятися, вибачати, пробачати.

Основна ідея цієї трансформація – це зміни. І зміни – це не “тимчасовий хаос”, а нова реальність, у якій дитина має право бути активним учасником, а не лише жертвою обставин.

У табл. 1 розкрито результати аналізу складових кожного виміру психолого-педагогічної підтримки дітей і молоді в умовах воєнного стану, а також розкрито найбільш значущі проблеми її реалізації в Україні, визначено особливості за кожною проблематикою, а також можливі практичні шляхи їх подолання (вирішення).

Актуальність такого дослідження зумовлена тривалим характером війни росії проти України, що спричинила системні соціальні, психологічні та освітні виклики для підростаючого покоління. У сучасних умовах психолого-педагогічна підтримка дітей і молоді є не лише гуманітарною потребою, а критичною умовою для забезпечення національної стійкості, збереження психічного здоров’я та майбутньої інтеграції молодих громадян у повоєнне суспільство.

Особливої актуальності набуває пошук ефективних моделей допомоги, здатних працювати в умовах нестабільності, обмежених ресурсів, часто за відсутності безпечного середовища. Це дослідження спрямоване на виявлення критичних зон, які потребують негайного реагування на рівні як державної політики, так і локальних освітніх та соціальних ініціатив.

Психолого-педагогічна підтримка в умовах війни – це багатовимірна система, що має поєднувати роботу з травмою, створення безпечного освітнього простору та розвиток навичок адаптації. Український контекст визначає необхідність швидких, але глибоко обґрунтованих рішень. Ключовим чинником успіху є інтеграція всіх трьох вимірів у стратегії освіти, охорони здоров’я, місцевого самоврядування та безпеки.

Таблиця 1 – Аналіз складових кожного виміру: проблеми – особливості – шляхи вирішення

Вимір підтримки	Складова	Особливості для українських дітей	Основні проблеми	Шляхи подолання
1. Емоційне відновлення	Психологічна перша допомога	Часто не отримували навіть базової підтримки	Відсутність системних програм, недостатня обізнаність вчителів	Впровадження ППД у школах і громадах, навчання педагогів
	Робота з травмою (ПТСР, тривога)	Травми втрати, бомбардувань, переселення	Відсутність фахівців у закладах освіти	Співпраця з психологами, мобільні команди допомоги
	Терапевтичні методики (арт, ігра, казка)	Позитивна динаміка в умовах безпеки	Недоступність методів у сільській місцевості	Онлайн-ресурси, підготовка фасилітаторів, закупівля матеріалів
	Соціальна взаємопідтримка	Ізоляція ВПО, складнощі інтеграції в нові колективи	Нерозуміння, ксенофобія, стигматизація	Формування інклюзивних груп, наставництво серед однолітків
2. Психологічна безпека	Безпечний фізичний простір	Часто не мають доступу до укриттів	Школа не відповідає стандартам цивільного захисту	Державне фінансування на безпечні простори, аудит безпеки в школах
	Психоедукація дітей та педагогів	Брак навичок саморегуляції	Відсутність програм з емоційного інтелекту в школах	Введення курсів з психоедукації, тренінги, інтеграція у програми
	Реагування в кризових ситуаціях	Потреба в алгоритмах дій при тривогах, обстрілах	Нерозуміння послідовності дій	Розробка зрозумілих алгоритмів, щотижневі повторення правил
	Робота шкільних психологів/служб	Штат обмежений, перевантажений	Низька зарплата, брак кваліфікації	Створення служб підтримки в ТГ, залучення фахівців з НУО
3. Адаптація до змін	Гнучкість освітніх програм	Часті зміни форм навчання (онлайн, офлайн, укриття)	Недостатньо адаптивних освітніх підходів	Адаптація програм, скорочення "знаннєвого" навантаження
	Розвиток життєстійкості (resilience)	Потребують моделей стабільності та прикладу	Недовіра до майбутнього, апатія	Позитивні приклади, індивідуальна підтримка, розвиток емоційного інтелекту
	Освоєння цифрових інструментів навчання	Часто єдина можливість навчання в евакуації	Брак техніки, нестабільний інтернет	Забезпечення девайсами, адаптовані онлайн-платформи
	Усвідомлення “нормальності змін”	Бажання повернутися до “старого життя”	Тривожність через невизначеність	Педагогіка змін: розмови про сучасність як реальність, а не “тимчасове лихо”

Результати дослідження та орієнтація на сучасний досвід, аналітичні дані, міжнародні практики та результати вітчизняних досліджень показують, що українському суспільству доцільно реалізувати наступні практичні рекомендації для підвищення психолого-емоційного відновлення дітей і молоді в умовах триваючого воєнного стану.

1. Інституційний розвиток системи психо-соціальної допомоги дітям, а саме:

створення системи міжсекторальної координації (освіта, охорона здоров’я, соцзахист, місцева влада) для реагування на психологічні потреби дітей у громадах;

впровадження інституту шкільних психологів і соціальних педагогів у кожному навчальному закладі, з реальним повноваженням та ресурсами;

регулярне фінансування програм психологічної допомоги, зокрема через механізми державно-громадського партнерства.

2. Підготовка фахівців і навчання дорослих, а саме:

обов'язкова підготовка педагогів та вихователів з основ психічного здоров'я дітей, посттравматичних реакцій, методів психологічної саморегуляції;

створення онлайн-платформ для батьків, учителів та волонтерів, які б містили: курси з емоційного супроводу дітей; поради щодо комунікації після травми; базові алгоритми надання психологічної першої допомоги;

розвиток спільнот практиків для обміну досвідом і формування професійної підтримки в умовах емоційного вигорання.

3. Інтеграція програм емоційного відновлення в освіту, а саме:

розробка й впровадження адаптованих програм соціально-емоційного навчання (SEL) у школах;

регулярне проведення занять з арттерапії, казкотерапії, ігротерапії як частини шкільного розкладу або позакласної діяльності;

забезпечення психологічного супроводу освітнього процесу — не лише індивідуального, а й групового, з урахуванням вікових і ситуаційних потреб.

4. Розвиток середовищ підтримки для дітей та молоді, а саме:

створення в громадах центрів психоемоційного відновлення для дітей і підлітків — як стаціонарних, так і мобільних;

розширення практики груп взаємопідтримки (підліткових, сімейних, для дітей ВПО чи тих, хто пережив втрату);

організація тематичних таборів, заходів, творчих ініціатив, спрямованих на розвиток життєстійкості, позитивного самосприйняття, комунікації.

5. Національна інформаційна кампанія, а саме:

запуск просвітницької кампанії з акцентом на важливість психічного здоров'я дітей у воєнний час;

поширення коротких відео, інфографік, порадників через медіа та соціальні мережі для батьків і педагогів;

дестигматизація звернення за психологічною допомогою — через публічні історії, підтримку лідерів думок, відкрите висвітлення цієї теми в школах і громадах.

6. Моніторинг і дослідження, а саме:

запровадження національної системи моніторингу психоемоційного стану дітей і молоді в умовах війни (у партнерстві з НУО, ООН, ЮНІСЕФ, академічними установами);

регулярне оновлення рекомендацій на основі нових досліджень, практик і контекстуальних змін;

збір і аналіз локальних даних щодо ефективності програм підтримки для адаптації інтервенцій під реальні потреби.

Практична реалізація більшості рекомендацій спрямована на створення цілісної, системної та гуманістичної моделі психолого-педагогічної підтримки, що стане не лише відповіддю на травму війни, а й запорукою формування стійкого покоління, здатного до розвитку, емпатії та національного відновлення.

Висновки

Сьогодні треба зрозуміти, що психолого-педагогічна підтримка дітей у воєнний час – це не лише гуманітарна місія. Це державницький вибір. Психолого-педагогічна підтримка дітей та молоді в умовах війни – стратегічне завдання національного масштабу.

Від того, як ми сьогодні подбаємо про психічне здоров'я та життєстійкість дітей та молоді, залежить те, якою буде Україна завтра:

сильною чи роздробленою;

відкритою чи травмованою;

активною чи апатичною.

Це наша спільна відповідальність – формувати покоління, здатне не лише вижити, а й творити майбутнє.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. UNICEF (2023). Psychosocial Support for Children in Armed Conflict. URL: https://www.unicef.org/reports/psychosocial-support-children-armed-conflict
2. Міністерство освіти і науки України (2024). Безпечне освітнє середовище в умовах війни. URL: https://mon.gov.ua/ua/news/bezpechne-osvitnye-seredovishche-v-umovah-vijni
3. Save the Children (2023). The Mental Health and Psychosocial Needs of Children in Ukraine. URL: https://www.savethechildren.net/news/ukraine-mental-health-crisis
4. Національна психологічна асоціація України (2023). Рекомендації з надання психологічної допомоги дітям і підліткам під час війни. URL: https://npa-ua.org/recommendations-children-war
5. Loades, M. E., et al. (2023). Change in child mental health during the Ukraine war: evidence from a large sample of parents. *European Child & Adolescent Psychiatry*. URL: https://link.springer.com/article/10.1007/s00787-023-02255-zSpringerLink
6. Reuters. (2025). Emotional trauma piles up for Ukraine's children three years after invasion. URL: https://www.reuters.com/world/europe/emotional-trauma-piles-up-ukraines-children-three-years-after-invasion-2025-02-20/
7. Budnyk, O., & Sajdak-Burska, A. (2023). Pedagogical Support for Ukrainian War-Affected Children: Future Teachers' Readiness to Work in Crisis. *Journal of Vasyl Stefanyk Precarpathian National University*. URL: https://journals.pnu.edu.ua/index.php/jpnu/article/view/7157journals.pnu.edu.ua+1ruj.uj.edu.pl+1
8. Cambridge University Press. (2023). Psychosocial Support Interventions for Children During Ongoing War in Ukraine: A Pilot Study. *Prehospital and Disaster Medicine*. Cambridge University Press & Assessment. URL: https://www.cambridge.org/core/journals/prehospital-and-disaster-medicine/article/psychosocial-support-interventions-for-children-during-ongoing-war-in-ukraine-a-pilot-study/0B904B64245FB1EF61E5285CE4D2B573
9. Frontiers in Psychology. (2024). Resilience processes among Ukrainian youth preparing to build resilience with peers during the Ukraine-Russia war. URL: https://www.frontiersin.org/articles/10.3389/fpsyg.2024.1331886/full
10. Sodolevska, V. (2024). The Impact of War on the Mental Health of Youth: The Role of Resilience and Psychological Interventions. Psychosomatic Medicine and General Practice. URL: https://e-medjournal.com/index.php/psp/article/view/532e-medjournal.com
11. Rudenok, A., et al. (2023). Psychological Support for Children with Intellectual Disorders in War Conditions. BRAIN. Broad Research in Artificial Intelligence and Neuroscience. URL: https://lumenpublishing.com/journals/index.php/brain/article/view/5588

References

1. UNICEF (2023). Psychosocial Support for Children in Armed Conflict. Available from : https://www.unicef.org/reports/psychosocial-support-children-armed-conflict
2. Ministry of Education and Science of Ukraine (2024). Safe Educational Environment in Wartime. URL: https://mon.gov.ua/ua/news/bezpechne-osvitnye-seredovishche-v-umovah-vijni
3. Save the Children (2023). The Mental Health and Psychosocial Needs of Children in Ukraine. Available from : https://www.savethechildren.net/news/ukraine-mental-health-crisis
4. National Psychological Association of Ukraine (2023). Recommendations for Providing Psychological Assistance to Children and Adolescents in Wartime. Available from : https://npa-ua.org/recommendations-children-war
5. Loades, M. E., et al. (2023). Change in child mental health during the Ukraine war: evidence from a large sample of parents. *European Child & Adolescent Psychiatry*. Available from : https://link.springer.com/article/10.1007/s00787-023-02255-zSpringerLink
6. Reuters. (2025). Emotional trauma piles up for Ukraine's children three years after invasion. Available from : https://www.reuters.com/world/europe/emotional-trauma-piles-up-ukraines-children-three-years-after-invasion-2025-02-20/
7. Budnyk, O., & Sajdak-Burska, A. (2023). Pedagogical Support for Ukrainian War-Affected Children: Future Teachers' Readiness to Work in Crisis. *Journal of Vasyl Stefanyk Precarpathian National University*. Available from : https://journals.pnu.edu.ua/index.php/jpnu/article/view/7157journals.pnu.edu.ua+1ruj.uj.edu.pl+1
8. Cambridge University Press. (2023). Psychosocial Support Interventions for Children During Ongoing War in Ukraine: A Pilot Study. *Prehospital and Disaster Medicine*. Cambridge University Press & Assessment. Available from : https://www.cambridge.org/core/journals/prehospital-and-disaster-medicine/article/psychosocial-support-interventions-for-children-during-ongoing-war-in-ukraine-a-pilot-study/0B904B64245FB1EF61E5285CE4D2B573
9. Frontiers in Psychology. (2024). Resilience processes among Ukrainian youth preparing to build resilience with peers during the Ukraine-Russia war. Available from : https://www.frontiersin.org/articles/10.3389/fpsyg.2024.1331886/full
10. Sodolevska, V. (2024). The Impact of War on the Mental Health of Youth: The Role of Resilience and Psychological Interventions. Psychosomatic Medicine and General Practice. Available from : https://e-medjournal.com/index.php/psp/article/view/532e-medjournal.com
11. Rudenok, A., et al. (2023). Psychological Support for Children with Intellectual Disorders in War Conditions. BRAIN. Broad Research in Artificial Intelligence and Neuroscience. Available from : https://lumenpublishing.com/journals/index.php/brain/article/view/5588

On the Issue of Military Education Transformation in the Context of Military Specialists Training with Higher Education at the Tactical Level

Щодо питання трансформації військової освіти в контексті підготовки військових фахівців з вищою освітою на тактичному рівні

Anatolii Loishyn
Doctor of Philosophy, e-mail: aloishyn@gmail.com, ORCID: 0000-0003-2769-9336
Military Institute of National Taras Shevchenko University of Kyiv, Kyiv, Ukraine

Анатолій Лойшин
Доктор філософії, e-mail: aloishyn@gmail.com, ORCID: 0000-0003-2769-9336
Військовий інститут Київського національного університету імені Тараса Шевченка, м. Київ, Україна

Received: March 24, 2025 | Revised: Aprile 28, 2025 | Accepted: Aprile 30, 2025

DOI: 10.33445/sds.2025.15.2.26

Purpose: is to identify key problematic issues that negatively impact: the development of professional military education, the implementation of education quality management, the motivation of applicants for higher education to learn, and the active engagement of educational process participants in activities within international programs and academic mobility.

Method: analysis and synthesis, decomposition approach.

Findings: The study identifies key issues and proposes specific solutions in the field of military education in Ukraine under the legal framework of martial law.

Theoretical implications: This research has an applied character and will be useful for scholars and administrators involved in military education in Ukraine, particularly its transformation and reform. The study emphasizes specific challenges and potential ways to address them.

Originality of the research: The research is based on original sources, including conceptual and strategic documents that define the development vectors of military education in both the short-term and long-term perspectives.

Research limitations: The study is limited to the use of publicly available information.

Paper type: Conceptual research.

Мета: виявлення ключових проблемних питань, які негативно впливають на розвиток професійної військової освіти, реалізацію управління якістю освіти, мотивацію здобувачів вищої освіти до навчання, а також активну участь учасників освітнього процесу в міжнародних програмах і заходах академічної мобільності.

Метод дослідження: аналіз і синтез, підхід декомпозиції.

Результати дослідження: У дослідженні визначено ключові проблеми та запропоновано конкретні шляхи їх вирішення у сфері військової освіти України в умовах правового режиму воєнного стану.

Теоретична цінність дослідження: Дослідження має прикладний характер і буде корисним для науковців та управлінців, які займаються військовою освітою в Україні, зокрема її трансформацією та реформуванням. У роботі акцентовано увагу на конкретних викликах і можливих шляхах їх подолання.

Оригінальність дослідження: Робота базується на оригінальних джерелах, включаючи концептуальні та стратегічні документи, які визначають вектори розвитку військової освіти як у коротко-, так і в довгостроковій перспективі.

Обмеження дослідження: Дослідження обмежене використанням загальнодоступної інформації.

Тип статті: Концептуальне дослідження.

Key words: professional military education, education quality management, foreign language learning, academic mobility.

Ключові слова: професійна військова освіта, управління якістю освіти, вивчення іноземної мови, академічна мобільність.

Introduction

As of today, Ukraine is in its fourth year of resisting the armed aggression of the russian federation. The Defense Forces continue to mount a resolute defense against an adversary that significantly surpasses Ukraine in terms of manpower and military-economic potential. In pursuit of victory, not only has the entire Ukrainian nation united, but partner countries have also provided invaluable material and technical assistance.

At the same time, the success of repelling armed aggression depends not only on the availability of modern weapons and military equipment, as well as a sufficient supply of missiles and ammunition, but also on the presence of well-trained and highly motivated personnel capable of carrying out complex missions in combat conditions.

Given this, we have analyzed certain priority aspects of military education in Ukraine and identified specific problematic issues that negatively impact the training of military specialists within the Defense Forces of Ukraine.

Theoretical background

The theoretical foundations of this study are based on monitoring educational process measures for the training of military specialists with higher education for the Defense Forces of Ukraine. The analysis covered specific regulatory and conceptual documents related to the reform and development of military education. In particular, the following were examined:

The military security strategy of Ukraine [1], which outlines the development of the military education system and the training of personnel for the Defense Forces of Ukraine. It also emphasizes the introduction of educational programs for officers, sergeants, and senior enlisted personnel based on combat experience, training methodologies, and NATO principles and standards.

The strategic defense bulletin of Ukraine [2], which defines the mission and vision of the Defense Forces by 2030. According to this document, the Defense Forces will be unified under a single command and consist of well-trained and motivated personnel supported by effective and transparent systems of personnel management, military education and science, healthcare, and social protection.

The higher education development strategy [3], which states that the internationalization of higher education in Ukraine is one of the country's strategic goals. It also calls for the transformation of education in the security and defense sector in line with NATO doctrinal approaches and principles.

The policy on human capital recruitment, development, and retention in the defense forces [4], which includes provisions for continuous professional development of personnel throughout their military careers. It introduces a multi-level system of professional military education aligned with NATO approaches and the best domestic and international practices. The policy also aims to establish a military education quality assurance system, improve foreign language training for Defense Forces personnel in accordance with STANAG 6001 standards, enhance professional development programs for academic and teaching staff, including through the NATO "Defense Education Enhancement Program" (DEEP), and refine the organizational and staffing structure of military educational institutions.

The concept for transforming the military education system [5], which highlights shortcomings in the organizational and staffing structures of military educational institutions and training centers, as well as their misalignment with the evolving needs of the Armed Forces and other Defense Forces components. It also notes deficiencies in the foreign language training system for military personnel, which fails to ensure sufficient language proficiency for effective participation in international activities. Alongside identifying these challenges, the concept prioritizes the development of professional military education and education quality management.

The strategy for military education system management [6], which outlines several key measures, including the establishment of structural units for education quality control within military command bodies and educational institutions. It also proposes the creation of a quality assurance system for higher and specialized pre-higher education based on national quality standards and professional military education requirements in line with NATO Standard Bi-SCD 075-007 "Education and Individual Training" [7].

Problem Statement

The analysis of the aforementioned conceptual and strategic documents, along with the practical training of military specialists, has revealed both existing problems and promising pathways for

addressing them in the further transformation (improvement) of Ukraine's military education system.

At the same time, the study takes into account the practical implementation experience of specific areas, including:

the development of professional military education;

the acquisition of language competencies by higher education students and personnel of the Ministry of Defense and the Armed Forces of Ukraine;

the enhancement of pedagogical skills and professional competencies of academic staff, including their participation in international programs;

the implementation of education quality management in the learning process based on best practices from partner countries;

ensuring sufficient motivation for higher education students to pursue their studies during the period of martial law in Ukraine.

For each of these elements (areas), key problematic issues have been identified that hinder the effective and efficient achievement of defined objectives.

Methodology

To achieve the study's objective, a decomposition approach was applied, with a focus on analyzing the core issues related to:

1) The development and functioning of professional military education;
2) The management of higher education quality;
3) The academic performance of higher education students in military higher education institutions (hereinafter – MHEIs) and military educational units of higher education institutions (hereinafter – MTU HEIs);
4) The acquisition of language competencies by personnel, as well as the involvement of academic staff and higher education students in international programs and academic mobility initiatives.

The purpose of the study is to identify the key problematic issues that negatively impact: the development of professional military education, the implementation of education quality management the maintenance of a sufficient level of motivation among higher education students, the active participation of educational process participants in activities within international programs and academic mobility.

Results

1. At present, the reform of military education is being carried out in accordance with the requirements of several conceptual and strategic documents, including the Concept for the Transformation of Military Education, the Military Security Strategy of Ukraine, the Strategic Defense Bulletin, and other regulatory documents.

The key elements of the development of the subject area, as well as potential ways to improve the educational process, have been examined in the theoretical foundations of this study.

However, practical experience in implementing professional military education courses in MHEIs and MTU HEIs has revealed critical issues that need to be addressed as a priority.

Given the three main areas of military education implementation (academic (higher) education, professional military education (hereinafter – PME), advanced training), PME currently remains organizationally unstructured within military educational institutions.

The primary issue is the absence of a centralized competence center responsible for the organization and administration of PME courses.

For example, based on the experience of conducting the PME L1a+L1b course, three key organizational tasks have been identified as requiring urgent resolution:

1) overall management and daily operations of trainees (including coordination of arrivals, accommodation, and support throughout the training process);

2) implementation of the basic PME tactical-level course (hereinafter – L1a);

3) implementation of the specialized PME tactical-level course (hereinafter – L1b).

In practice, this necessitates the formal appointment of a course administration team from the personnel of MHEIs, MTU HEIs, and other structural units; personnel responsible for conducting general military and specialized training.

Considering that both basic (general military) and specialized training are conducted by the respective instructor and teaching staff of designated departments, with an assigned teaching workload, overall administration (management) is entrusted to non-staff personnel who must combine the performance of their official duties with tasks related to the PME course.

In this regard, it is worth presenting a successful example of addressing this issue based on the experience of the National Defense University of Ukraine.

Thus, the Professional Military Education Institute "Leadership School" operates within the structure of the National Defense University of Ukraine. The mission of this Institute is defined as: "preparing leaders at the strategic and operational levels based on national combat experience and best practices of NATO member states…" [8].

It should be noted that the organization of the educational process has been developed in accordance with the core requirements of the Joint Directive "Education and Individual Training" (075-007).

At the same time, the organizational and staffing structure of the Institute has been designed with consideration of best PME practices, ensuring the structured implementation of the «Joint staff officers course» (L-3), «Senior leadership course at the strategic level» (L-4), and «Strategic management and state policy course» (L-5) through the establishment of course director and mentor positions.

According to the information provided on the official website of the National Defense University, the main tasks of course mentors include developing a new style of military leadership among students, participating in all training sessions with students, and more.

At the same time, the Chief Mentor of the Institute coordinates the activities of the mentors.

One of the key advantages of implementing the mentor system is the necessity to combine theory and practice. This is justified by the fact that scientific and pedagogical staff (hereinafter – SPS), due to the nature of their daily activities, often lose connection with the practical component of the subject they teach.

Meanwhile, individual deployments of SPS from among military personnel, assigned by senior leadership, are often too short and sporadic to provide a full understanding of the actual situation.

Furthermore, SPS from among civilian personnel are entirely deprived of the opportunity to study the practical component of their activities, particularly in specialties related to combat command, logistics, and support.

It is also important to note certain peculiarities in the mechanisms for filling teaching positions, such as the position of professor, which requires prior research dissertation defense, teaching experience, etc.

The requirement to have teaching experience and achievements specifically in the field of teaching activity automatically excludes the possibility of appointing an officer with practical combat experience to such a position.

Therefore, practically combining theory and practice by involving both an instructor with a high level of theoretical expertise and a mentor – an officer with extensive practical experience enables the effective conduct of all types of training sessions.

Currently, PME courses are conducted not only at the National Defense University of Ukraine.

Thus, PME courses at the operational and strategic levels are organized and conducted at the aforementioned university, while PME courses at the tactical level are conducted at MHEIs and MTU HEIs.

At the same time, as of today, PME courses can be conducted both separately and as part of the educational and professional programs of bachelor's degree (L1a and L1b courses) and master's degree (L1c course).

For example, at the Military Institute of Taras Shevchenko National University of Kyiv, PME courses – Basic tactical-level PME course (L1a), Specialized PME course (L1b), and Command PME course (L1c) – have been fully integrated into all educational and professional training programs for bachelor's and master's degree specializations.

However, it should be added that PME courses are primarily conducted to attain the appropriate level of military education (tactical, operational, strategic). This means that course participants develop the ability to solve service-related tasks at the corresponding level of military command, rather than acquiring specialized competencies in specific fields (with the exception of the specialized PME course (L1b)).

Currently, there are different perspectives within Ukraine's military education system regarding the content and structure of PME courses, particularly concerning the tactical-level command and staff course (L2) (hereinafter – L2 course). The core focus of this course is the study of the Military Decision-Making Process (MDMP) [9], and there are ongoing discussions about whether it should be conducted separately for each specialization or for groups of specializations.

This debate is primarily driven by the requirement for officers to obtain the necessary level of military education for career advancement and promotion to higher military ranks.

For combat command specialties, the gradual completion of PME tactical-level courses follows a structured and systematic approach. An officer progresses through service, gains experience and gradually advances in rank and responsibility. For example:

platoon commander (after completing training at an MHEI, during which the service member completed the L1a course, acquiring the necessary military-professional competencies required for all platoon commanders in personnel management; and the L1b course, during which military-specialized competencies specific to the future commander's specialization (artillery, tank, reconnaissance units, etc.) are acquired; rank: "senior lieutenant").

company commander (after completing the L1c command course; rank: "captain").

battalion staff chief (after completing the L2 course; rank: "major").

At the same time, officers specializing in non-combat command fields, such as military translation, face specific challenges.

The core issue lies in the fact that, upon graduation, an officer in this specialization may immediately be assigned to positions in linguistic or international relations roles within strategic-level military command structures, often with an initial rank and position level higher ("captain", "major") than the baseline category of a platoon commander – "senior lieutenant".

At the same time, the key issue is that specialists in this field, under the existing personnel management approach, may go through their entire career without serving at the tactical unit level.

However, when becoming eligible for promotion to the next military rank, personnel departments will require the prospective "major" to present a certificate of successful completion of the L2 course.

The resolution of this issue leads to debates regarding the organization of a separate command and staff course for a specific category of specialties, which contradicts the fundamental purpose of PME courses.

However, returning to the content of tactical-level PME courses integrated into the educational and professional programs of bachelor's degree students, it is important to emphasize that the typical educational program of the L1a course [10] and the competency requirements that must be developed upon its completion are the same for all specialties (specializations).

For example, one of the military-professional competencies acquired during the course is: "*the ability to prepare the unit's standard weapons for combat use; effectively utilize the combat and technical capabilities of weapons during combat operations and training sessions with subordinate personnel; personally master techniques and methods of accurate fire with standard weapons against emerging and moving targets, both during the day and at night; manage the fire of subordinate units (fire support assets) during combat missions*".

At the same time, the learning outcomes associated with this competency include: "applying knowledge of the material structure of small arms, rules of shooting, operation, and maintenance of small arms; methods for organizing and conducting training for unit personnel; preparing weapons for use in both peacetime and combat conditions; and applying knowledge and skills in managing unit fire in combat".

This raises a critical issue regarding not only the availability of qualified instructor and teaching staff capable of implementing this training but also the presence of the necessary material and technical resources, including weapons and military equipment.

If for the Hetman Petro Sahaidachnyi National Army Academy and the Military Academy (Odesa) such training is standard, then for MTU HEIs such as the Military Institute of Taras Shevchenko National University of Kyiv, this activity differs from the profile of military specialist training.

In our opinion, the mentioned program requires revision in terms of clarifying its content in the context of the dynamic development of military affairs, as well as the need to consider the feasibility of separately developing the basic L1a course for combat command specialties and the basic L1a course for specialties not related to combat command.

Summarizing the above, it can be stated that to enhance the effectiveness and efficiency of PME courses, it is necessary to first consider the following issues:

1) organizational structuring of PME courses within the current (prospective) structures of MHEIs and MTU HEIs;

2) analysis and revision of existing competencies acquired during the L1a course;

3) establishing a clear hierarchy of officer positions across all military occupational specialties at all levels of military command, defining the requirements for filling these positions considering the specific activities of military specialists, and justifying the necessity of completing specific PME courses.

2. The Law of Ukraine "On Higher Education" [11] states: "*the quality of higher education is the compliance of the conditions for educational activities and learning outcomes with the requirements of legislation and higher education standards, professional and/or international standards (if available), as well as the needs of stakeholders and society, ensured through internal and external quality assurance procedures*".

Additionally, according to the Recommendations of the National Agency for Higher Education Quality Assurance regarding the implementation of an internal quality assurance system: "the internal (intra-university) quality assurance system aims to establish a framework for continuous institutional attention to education quality, including the review and improvement of courses and educational programs" [12].

The implementation of quality assurance in higher education has also extended to military education in Ukraine. According to the provisions of the Concept for the transformation of military education, MHEIs and MTU HEIs are tasked with ensuring the quality of military education, implementing stakeholder responsibility for educational activities, enforcing legally established

requirements for quality assurance and guarantees in education, and introducing institutional audits of professional military education.

In accordance with the above, the quality management of military education is being actively implemented based on the approaches of NATO member states, particularly the Joint Directive "Education and Individual Training" (075-007). The Joint Directive provides for the establishment of a five-element (tiered) system: quality management, quality assurance, quality control, and inspection. These elements are classified as either proactive or reactive in nature.

According to the Joint Directive, the quality management system is understood as a comprehensive framework of quality standards, methodologies, and authorities—elements that enable a holistic approach to the educational process at all stages, from planning to reporting on completed training activities. The analysis of quality management measures in education has shown that it can be associated with an audit system in military education. Audits are conducted to provide recommendations to educational process participants regarding existing issues, identifying their causes, and suggesting paths for improvement.

At the same time, the primary beneficiary of quality management is the head of the MHEI (MTU HEI), who, based on the provided recommendations, makes the necessary management decisions to improve the educational process.

Additionally, one of the key participants in the quality management process is the learner. Maintaining constant communication with students allows for the identification of organizational challenges in the educational process.

Overall, this approach is not new but is widely known in the business sector as the *PDCA (Plan/Do/Check/Act)* cycle, also referred to as the Shewhart-Deming Cycle [13] – a four-step model used for continuous improvement. This approach is a fundamental part of Lean Management [14], a strategy aimed at efficient business management. The strategy was successfully applied by Toyota during the post-war recovery of Japan's automotive industry. The PDCA approach focuses on business process improvement through planning and implementing solutions, testing them, and analyzing the results.

Taking this into account, as well as the provisions of the Joint Directive, one of the key principles of modern educational quality management is the Continuous Improvement Process (CIP), which involves a set of measures such as reporting, self-assessment, implementation, and review.

To initiate this process, specialized units (departments, offices) for quality assurance in educational activities and higher education have been established (or are being established) within MHEIs and MTU HEIs.

The practical establishment of quality assurance departments (units) has shown that the personnel of these departments, which are essentially expert bodies, should primarily consist of individuals with relevant experience in organizing and conducting the educational process. However, in practice, these units are staffed with personnel who lack sufficient experience and professional achievements in educational work.

This issue arises primarily due to the current approach to staffing policies and the classification of personnel categories and requirements for these units.

At present, even a senior lecturer of a department (assigned the 43rd tariff grade) does not receive a promotion in position or salary when serving in quality assurance units.

As a result, the requirements for personnel conducting expert evaluations, monitoring the educational process, and providing recommendations to the institution's leadership are lower than those for departmental teaching staff, who directly implement educational activities.

Given the above, it is essential for staff quality management units with personnel who have relevant backgrounds in educational activities. To ensure high motivation for serving in such units, their personnel should have higher staffing categories and salaries compared to those directly involved in conducting educational processes.

However, if it is not possible to staff these units with military personnel who are experts in education, an alternative solution could be recruiting civilian employees of the Armed Forces of Ukraine from among experienced academic staff while ensuring appropriate salary levels.

For the effective functioning of this unit and to maintain high motivation among its personnel, the transition from implementing educational activities to expert evaluation work should be considered a promotion.

At the same time, to enable experts in education to effectively fulfill their duties and produce impartial and objective assessments, a priority task for the Ministry of Defense of Ukraine is to ensure competitive salaries for these professionals within the labor market.

Summarizing the above, it can be stated that the introduction of a quality management system in MHEIs and MTU HEIs will undoubtedly contribute to improving the educational process by providing objective and impartial proposals (recommendations) aimed at its enhancement.

3. Next, it is proposed to examine specific problematic issues in the training of military specialists at the bachelor's degree level.

Currently, a pressing issue is the development of necessary physical fitness among cadets of MHEIs and MTU HEIs, as well as the assessment of their physical preparedness.

The full-scale invasion of the Russian Federation and the resulting armed resistance have necessitated the justified dispersal of personnel, including training units. Security measures in response to constant enemy air threats do not allow for full-scale outdoor training.

At the same time, it can be stated that the physical education system in Ukraine does not fully ensure the development of youth's physical abilities during their schooling, nor does it provide a gradual increase in their physical capabilities.

In an ideal physical education system, a student would progressively develop physical abilities, ensuring that by the time they take entrance exams for military educational institutions, they are physically prepared to complete the required physical training program.

Additionally, restrictive measures introduced during the COVID-19 pandemic, which lasted for several years, have significantly impacted the overall physical health of young people.

As a result, today's reality is that many prospective applicants who wish to pursue a military career are not always physically prepared to pass the entrance fitness tests required for admission to MHEIs and MTU HEIs.

Given the shortage of trained officer personnel in the Defense Forces, there is a need for a systematic approach to the initial physical development of prospective applicants.

A possible solution to this issue could be the implementation of a state reform (government initiative) in the field of school education. This reform could include a set of measures aimed at sufficient physical development throughout schooling.

Additionally, it is necessary to introduce a specialized program integrated into the curricula of graduating classes for students planning to apply to military educational institutions.

The existing physical fitness standards, if developed gradually and systematically throughout secondary education, are achievable for the vast majority of students.

Analyzing the issue of students mastering the prescribed training programs, it is necessary to focus on the lack of motivation among cadets of MHEIs and MTU HEIs for successful learning.

As of today, since the introduction of martial law in Ukraine, a problematic issue has been identified in the training of military specialists with higher education.

Specifically, there is no legal mechanism for dismissing cadets due to academic failure or violations of contract terms, particularly regarding termination of education contracts during martial law. This is due to the absence of such a provision in Ukrainian legislation as a legal basis for contract termination.

According to Clause 36 of the Presidential Decree of Ukraine No. 1153/2008 "On the Regulations for Military Service of Citizens of Ukraine in the Armed Forces of Ukraine", and Clause

3, Part Five, Article 26 of the Law of Ukraine "On Military Duty and Military Service", a training contract is terminated, and a cadet is dismissed during martial law only in the following cases:

"For health reasons – based on a conclusion (resolution) of the Military Medical Commission regarding unfitness for military service, with removal from military records; In connection with the entry into force of a court conviction imposing imprisonment, restriction of liberty, or deprivation of military rank" [15].

Thus, cadets of MHEIs and MTU HEIs lack motivation for successful learning due to the absence of grounds for dismissal in cases of academic failure.

This leads to disregard for recommendations and instructions from the academic staff of educational institutions regarding increased efforts in studying.

Moreover, the lack of legal regulation in this area results in the graduation of officers who, during their studies, failed to acquire the necessary competencies in their specialties. This leads to low professional qualifications when performing duties in the military.

As a consequence, poor decision-making by an unqualified officer may result in unjustified losses of personnel and state resources due to ineffective command and management decisions.

4. Alongside the development of physical fitness and the lack of motivation among cadets of MHEIs and MTU HEIs, another pressing issue is the insufficient acquisition of language competencies among both military education students and personnel within the Ministry of Defense of Ukraine.

According to the Roadmap for Enhancing Language Training in the Armed Forces of Ukraine (2021–2025) [16], the strategic goal is to ensure a rapid increase in the number of personnel with foreign language proficiency, achieving a minimum proficiency level of SLP 2 "Functional" under NATO STANAG 6001 for officers, sergeants, and civilian employees of the Armed Forces of Ukraine. This is necessary for Ukraine's Membership Action Plan with NATO, the implementation of NATO policies and standards at all levels of military command, service in international organizations, participation in multinational military exercises, international cooperation activities, peacekeeping and security operations, and education abroad.

The document outlines a set of measures aimed at developing language competencies among Ministry of Defense and Armed Forces personnel, recognizing language proficiency as a key requirement for Ukraine's Euro-Atlantic integration in the defense sector, including military education.

The implementation of these measures was planned across different levels of military education: tactical, operational, and strategic.

At the tactical level, the goal was to gradually build capabilities to ensure that graduates of MHEIs and MTU HEIs attain a minimum proficiency level of SLP 2 by 2025, with at least 20% of final-year courses taught in a foreign language.

It is important to note that the provisions of the roadmap were developed before the full-scale invasion of the Russian Federation in 2024. The onset of full-scale aggression has negatively impacted the organization of the educational process, including foreign language learning.

The conditions of constant air threats, personnel dispersal, and the priority of acquiring military-professional and military-specialized competencies in direct fields of expertise have objectively limited the ability to prioritize foreign language education.

In addition to the above, the development of language competencies among all personnel within the Ministry of Defense and the Armed Forces of Ukraine must be comprehensive, forming a system that covers the entire spectrum of issues related to the development and continuous improvement of subject-specific competencies.

The main issue in this area is the lack of a centralized competence hub (coordination center) for language competency development within the Ministry of Defense and the Armed Forces of Ukraine.

Such a center could be established as a Language Agency of the Armed Forces of Ukraine, with the following key tasks:

1) *initiating and participating in the development of policies* (in collaboration with relevant structural units within the Ministry of Defense of Ukraine), identifying priority tasks in foreign language training and ensuring their primary implementation;

2) *coordinating and monitoring* personnel training in foreign language acquisition.

The improvement of this process would involve a comprehensive set of measures, including the development of regulatory frameworks, personnel management, and institutional capacity-building in MHEIs and MTU HEIs engaged in conducting language courses, including enhancing instructor and teaching staff, reviewing and updating curricula, and developing online courses.

It is important to note that, when analyzing ways to enhance the language competencies of personnel and students, and considering the current number of personnel and the actual capabilities of MHEIs and MTU HEIs, it is advisable to explore not only the possibility of sending personnel to partner countries for language training but also applying the outsourcing principle. This would involve engaging external (civilian) commercial organizations that are certified and specialize in foreign language training courses.

At the same time, the process of improving language competencies among personnel must be strictly managed at all stages of implementation: from the selection of candidates for foreign language training based on specific priorities to their continued support throughout their military careers.

At the conclusion of this analysis, it is worth mentioning a government initiative introduced by the Government of Ukraine to encourage English language learning and proficiency at the national level.

According to Clause 6, Article 4 of the Law of Ukraine «On the Use of the English Language in Ukraine» [17]: «individuals holding positions specified in Parts One and Two of Article 3 of this Law shall receive a 10% salary bonus for English language proficiency at a level not lower than B2 according to the Common European Framework of Reference for Languages (CEFR), as determined by the Cabinet of Ministers of Ukraine».

Thus, given the current government initiatives and financial incentives for English language proficiency, this measure will undoubtedly motivate Ukrainian citizens to learn the language.

Furthermore, the mandatory requirement for English proficiency when filling specific positions in the state and military administration sectors will become a key motivational factor for language acquisition.

Additionally, when analyzing motivation for education and foreign language learning, an issue has been identified: the lack of motivation among students and academic staff to actively participate in international programs, including the Development Enhancing Education Program (DEEP).

At present, SPS and cadets are actively engaged in various international programs for personal and institutional development.

However, participation in relevant online (offline) courses (events) is practically not encouraged by leadership. For example, if an academic staff member applies for a course in a partner country under the DEEP program to acquire relevant language or professional competencies, successfully completes the training, and implements the acquired skills and competencies in the educational process, this does not directly influence career advancement.

It is also necessary to emphasize the practical implementation of the provisions of the Law of Ukraine “On Higher Education” particularly regarding the right to academic mobility for higher education students, including cadets (trainees) of MHEIs and MTU HEIs of the Armed Forces of Ukraine.

According to the law, academic mobility is defined as: “the ability of participants in the educational process to study, teach, intern, or conduct scientific activities at another higher education institution (scientific institution) within Ukraine or abroad”.

Academic mobility is an essential component for the successful implementation of the European Credit Transfer and Accumulation System (ECTS) and for shaping an individual educational trajectory for higher education students.

At the same time, Article 62 of the law states that higher education students have the right to academic mobility, including international mobility.

However, the Regulations on the Implementation of the Right to Academic Mobility [18] specify that these provisions do not apply to students (doctoral candidates) of military institutions of professional pre-higher and higher education (institutions of professional pre-higher and higher education with specific learning conditions), as well as to employees of such institutions.

Thus, the existing restrictions on academic mobility for cadets (trainees) of MHEIs and MTU HEIs do not facilitate the promotion of international programs, particularly Erasmus+ (the European Union's international cooperation program in education, youth, and sports) [19].

Discussion

The scientific novelty of the research results and their practical significance were confirmed during discussions with the personnel of the Training Department and the Quality Assurance Department of the Military Institute of Taras Shevchenko National University of Kyiv.

Conclusion

The objective of this study has been successfully achieved. Key problematic issues have been identified that adversely affect the development of PME, the implementation of education quality management mechanisms, the motivation of higher education applicants to engage in learning, and the active involvement of educational process participants in international programs and academic mobility initiatives.

Based on the analysis of the issues outlined, the following conclusions are drawn:

1. **The absence of a centralized competence center (or "hub") for PME within the organizational structures of military higher education institutions (MHEIs) and military training units of higher education institutions (MTU HEIs)** negatively impacts the quality, consistency, and efficiency of PME course implementation. The institutional structuring and resourcing of PME programs should be prioritized in each MHEI and MTU HEI. The National Defense University of Ukraine exemplifies best practices in this area, offering structured courses such as the *Joint Staff Officers Course (L-3)*, *Senior Leadership Course at the Strategic Level (L-4)*, and *Strategic Management and State Policy Course (L-5)*. The incorporation of mentoring practices within these programs ensures the effective integration of theoretical and practical components. For officers whose specializations lie outside operational command, logistics, or force support, participation in the *L-2 Command and Staff PME Course* remains a challenge. Addressing this issue necessitates the development of a coherent and vertically integrated PME framework across all military occupational specialties and command echelons.
2. **The current system of education quality management within the Ministry of Defense of Ukraine** requires a comprehensive reassessment of staffing policies and the qualification requirements for personnel responsible for quality assurance. The effective institutionalization of this function depends on the establishment of a qualified and competent workforce.
3. **The existing model of physical education in general secondary schools** does not adequately prepare prospective applicants for the physical demands associated with entry into MHEIs and MTU HEIs. To bridge this gap, it is imperative to develop and implement a national-level program for the progressive enhancement of youth physical fitness, beginning at the pre-university level.

4. **The absence of a dedicated competence center within the Ministry of Defense for language training and language skills development** impedes the systemic advancement of foreign language proficiency among military personnel. To overcome this structural deficiency, it is proposed to establish a *Language Training Agency* under the Ministry of Defense to coordinate institutional development and standardize foreign language instruction.
5. **Amendments to Presidential Decree No. 1153/2008 "On the Regulations for Military Service of Citizens of Ukraine in the Armed Forces of Ukraine"** are required to introduce a legal basis for contract termination due to academic underperformance. This measure would serve as a regulatory tool for upholding academic standards in military education.
6. **The existing regulations governing academic mobility for higher education students enrolled in MHEIs and MTU HEIs** require revision. A more flexible and inclusive legal framework is needed to ensure that military students have equitable access to international academic opportunities, consistent with broader national policies on higher education mobility.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

1. The Strategy of Military Security of Ukraine, enforced by the Decree of the President of Ukraine № 121/2021 dated March 25, 2021, "On the Decision of the National Security and Defense Council of Ukraine dated March 25, 2021" "On the Strategy of Military Security of Ukraine". Retrieved from : https://zakon.rada.gov.ua/laws/show/121/2021#Text.
2. Strategic Defense Bulletin of Ukraine, enforced by the Decree of the President of Ukraine № 473/2021 dated September 17, 2021, "On the Decision of the National Security and Defense Council of Ukraine dated August 20, 2021" "On the Strategic Defense Bulletin of Ukraine". Retrieved from : https://zakon.rada.gov.ua/laws/show/n0063525-21#Text.
3. Strategy for the Development of Higher Education, approved by the Order of the Cabinet of Ministers of Ukraine № 286 dated February 23, 2022, "On the Approval of the Strategy for the Development of Higher Education in Ukraine for 2022-2032." Retrieved from : https://mon.gov.ua/osvita-2/vishcha-osvita-ta-osvita-doroslikh/strategiya-rozvitku-vishchoi-osviti-v-ukraini-na-2022-2032-roki?form=MG0AV3
4. Policy on the Engagement, Development, and Retention of Human Capital in the Defense Forces, approved by the Minister of Defense of Ukraine on May 9, 2024. Retrieved from : https://mod.gov.ua/diyalnist/normativno-pravova-baza/politika-zaluchennya-rozvitku-ta-utrimannya-lyudskogo-kapitalu-v-silah-oboroni?form=MG0AV3.
5. Concept of Transformation of the Military Education System, Resolution of the Cabinet of Ministers of Ukraine № 1410 dated December 15, 1997 (as amended by the Resolution of the Cabinet of Ministers of Ukraine № 1490 dated December 30, 2022) "On the Transformation of the Military Education System". Retrieved from : https://zakon.rada.gov.ua/laws/show/1410-97-%D0%BF#Text.
6. Strategy for the Management of the Military Education System, approved by the Minister of Defense of Ukraine on December 12, 2023. Retrieved from : https://mod.gov.ua/normativni-dokumenti/strategiya-menedzhmentu-sistemi-vijskovoi-osviti?form=MG0AV3.

7. Education and Individual Training (E&IT) 075-007 (September 10, 2015): Joint Directive of NATO Strategic Commands: Reference Materials. / [Collective of Authors]. – Kyiv: National Defense University named after Ivan Chernyakhovsky, 2021. – 178 p.
8. Institute of Professional Military Education "Leader Training", National Defense University of Ukraine. Retrieved from : https://nuou.org.ua/u/stru/insti/nnc-mmd/?form=MG0AV3.
9. Military Decision-Making Process: Organizing and Conducting Planning, by Gary Kuczynski, CALL Analyst, November 17, 2023. Retrieved from : https://www.army.mil/article/271773/military_decision_making_process_organizing_and_conducting_planning?form=MG0AV3.
10. Educational Program of the Professional Military Education Course "Basic Tactical Level Course L-1A".
11. On Higher Education: Law of Ukraine dated March 5, 2025, № 1556-VII. Retrieved from : https://zakon.rada.gov.ua/laws/show/1556-18#Text.
12. Recommendations of the National Agency for Higher Education Quality Assurance regarding the implementation of the internal quality assurance system, approved by the decision of the National Agency for Higher Education Quality Assurance, protocol dated June 26, 2019, № 6.
13. PDCA Cycle. Retrieved from : https://www.productplan.com/glossary/pdca-cycle/.
14. Bezkorovaina, I. (2023). The Toyota Way. Ukrainian companies are increasing productivity thanks to the Japanese system of continuous improvement Lean. How it works in practice – cases of Arpal, Progress Group, Harley & Cho. Retrieved from : https://forbes.ua/business/lean-management-v-dii-yak-yaponska-sistema-postiynogo-vdoskonalennya-dopomagae-ukrainskim-virobnitstvam-stavati-efektivnimi-keysi-arpal-progressive-lviv-harleyampcho-08092023-15870.
15. Regulations on the Military Service of Citizens of Ukraine in the Armed Forces of Ukraine: Decree of the President of Ukraine № 1153/2008 dated December 8, 2008. Retrieved from : https://zakon.rada.gov.ua/laws/show/1153/2008.
16. Roadmap for the Improvement of Language Training in the Armed Forces of Ukraine (2021-2025), approved by the Minister of Defense of Ukraine on March 1, 2021. Retrieved from : https://mod.gov.ua/diyalnist/normativno-pravova-baza/dorozhnia-karta-vdoskonalennia-movnoi-pidgotovki-u-zbroinikh-silakh-ukraini-na-2021-2025-roki.
17. On the Use of the English Language in Ukraine: Law of Ukraine dated June 4, 2024, № 3760-IX. Retrieved from : https://zakon.rada.gov.ua/laws/show/3760-20#n78.
18. Procedure for the Implementation of the Right to Academic Mobility: Resolution of the Cabinet of Ministers of Ukraine dated August 12, 2015, № 579. Retrieved from : https://zakon.rada.gov.ua/laws/show/579-2015-%D0%BF#Text
19. About the Erasmus+ Program. Retrieved from : https://erasmusplus.org.ua/programa-yes-erazmus/pro-programu/

Список використаних джерел

1. Стратегія воєнної безпеки України, введена в дію Указом Президента України № 121/2021 від 25 березня 2021 року "Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України". URL: https://zakon.rada.gov.ua/laws/show/121/2021#Text
2. Стратегічний оборонний бюлетень України, введений в дію Указом Президента України № 473/2021 від 17 вересня 2021 року "Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України". URL: https://zakon.rada.gov.ua/laws/show/n0063525-21#Text
3. Стратегія розвитку вищої освіти в Україні на 2022–2032 роки, затверджена розпорядженням Кабінету Міністрів України № 286 від 23 лютого 2022 року. URL:

https://mon.gov.ua/osvita-2/vishcha-osvita-ta-osvita-doroslikh/strategiya-rozvitku-vishchoi-osviti-v-ukraini-na-2022-2032-roki?form=MG0AV3

4. Політика залучення, розвитку та утримання людського капіталу в Силах оборони, затверджена Міністром оборони України 9 травня 2024 року. URL: https://mod.gov.ua/diyalnist/normativno-pravova-baza/politika-zaluchennya-rozvitku-ta-utrimannya-lyudskogo-kapitalu-v-silah-oboroni?form=MG0AV3
5. Концепція трансформації системи військової освіти, постанова Кабінету Міністрів України № 1410 від 15 грудня 1997 року (у редакції постанови № 1490 від 30 грудня 2022 року). URL: https://zakon.rada.gov.ua/laws/show/1410-97-%D0%BF#Text
6. Стратегія менеджменту системи військової освіти, затверджена Міністром оборони України 12 грудня 2023 року. URL: https://mod.gov.ua/normativni-dokumenti/strategiya-menedzhmentu-sistemi-vijskovoi-osviti?form=MG0AV3
7. Освіта та індивідуальна підготовка (E&IT) 075-007 (10 вересня 2015 р.): Спільна директива стратегічних команд НАТО: Довідкові матеріали / [колектив авторів]. – Київ: Національний університет оборони України імені Івана Черняховського, 2021. – 178 с.
8. Інститут професійної військової освіти “Підготовка лідерів”, Національний університет оборони України. URL: https://nuou.org.ua/u/stru/insti/nnc-mmd/?form=MG0AV3
9. Процес прийняття військових рішень: організація та проведення планування, Ґері Кучинські, аналітик CALL, 17 листопада 2023 року. URL: https://www.army.mil/article/271773/military_decision_making_process_organizing_and_conducting_planning?form=MG0AV3
10. Освітня програма курсу професійної військової освіти “Курс базового тактичного рівня L-1A”.
11. Про вищу освіту: Закон України від 5 березня 2025 року № 1556-VII. URL: https://zakon.rada.gov.ua/laws/show/1556-18#Text
12. Рекомендації Національного агентства із забезпечення якості вищої освіти щодо впровадження внутрішньої системи забезпечення якості освіти, затверджені рішенням Агентства, протокол від 26 червня 2019 року № 6.
13. Цикл PDCA. URL: https://www.productplan.com/glossary/pdca-cycle/
14. Безкоровайна, І. (2023). *Toyota Way. Як японська система постійного вдосконалення Lean допомагає українським компаніям підвищувати ефективність. Практичні кейси Arpal, Progress Group, Harley & Cho*. URL: https://forbes.ua/business/lean-management-v-dii-yak-yaponska-sistema-postiynogo-vdoskonalennya-dopomagae-ukrainskim-virobnitstvam-stavati-efektivnimi-keysi-arpal-progressive-lviv-harleyampcho-08092023-15870
15. Положення про проходження громадянами України військової служби у Збройних Силах України: Указ Президента України № 1153/2008 від 8 грудня 2008 року. URL: https://zakon.rada.gov.ua/laws/show/1153/2008
16. Дорожня карта вдосконалення мовної підготовки у Збройних Силах України на 2021–2025 роки, затверджена Міністром оборони України 1 березня 2021 року. URL: https://mod.gov.ua/diyalnist/normativno-pravova-baza/dorozhnia-karta-vdoskonalennia-movnoi-pidgotovki-u-zbroinikh-silakh-ukraini-na-2021-2025-roki
17. Про застосування англійської мови в Україні: Закон України від 4 червня 2024 року № 3760-IX. URL: https://zakon.rada.gov.ua/laws/show/3760-20#n78
18. Порядок реалізації права на академічну мобільність: Постанова Кабінету Міністрів України від 12 серпня 2015 року № 579. URL: https://zakon.rada.gov.ua/laws/show/579-2015-%D0%BF#Text
19. Про програму ЄС Erasmus+. URL: https://erasmusplus.org.ua/programa-yes-erazmus/pro-programu/

Глобальний Південь як мегасуб'єкт нового світового порядку

The Global South as a Mega Subject of the New World Order

Сергій Мокляк [A]
Corresponding author: д. політ. наук, професор, e-mail: smokliak@ukr.net, ORCID: 0000-0002-5255-8941
Наталя Конопка [B]
к. істор.наук, доцент, доцент кафедри, e-mail: smokliak@ukr.net, ORCID: 0000-0002-1245-3459

Sergii Mokliak [A]
Corresponding author: Dr of Political Science, Professor, e-mail: smokliak@ukr.net, ORCID: 0000-0002-5255-8941
Nataliia Konopka [B]
PhD in History, Associate Professor, Associate Professor of the Department, e-mail: smokliak@ukr.net, ORCID: 0000-0002-1245-3459

[A] Воєнна академія імені Євгенія Березняка, Київ, Україна
[B] Національний університет "Острозька академія", м. Острог, Україна

[A] Yevgeniy Bereznyak Military Academy, Kyiv, Ukraine
[B] National University "Ostroh Academy", Ostroh, Ukraine

Received: April 20, 2025 | Revised: April 28, 2025 | Accepted: April 30, 2025

UDC 321.01(477)

DOI: 10.33445/sds.2025.15.2.27

Мета роботи: визначення основних геополітичних ознак нового світового порядку, зокрема, появу нового суб'єкту – Глобального Півдня.
Метод дослідження: методи порівняння, класифікації, real time.
Результати дослідження: Проаналізовано зміни геополітичної та геоекономічної обстановки після повномасштабного вторгнення російської федерації в Україну. Визначено тенденції формування нового середовища безпеки та процеси, які впливають на його трансформацію. Доведено, що так званий Глобальний Південь останніми роками став актуальним чинником сучасних геополітичних процесів.
Теоретична цінність дослідження: Сучасне геополітичне становище змушує Україну напрацьовувати зовнішньополітичні рішення відповідні її власним національним інтересам, геополітичному і геостратегічному положенню в регіональній і глобальній міжнародній системі.
Тип статті: теоретичний.

Purpose: identifying the main geopolitical features of the new world order, in particular, the emergence of a new entity – the Global South.
Method: comparison methods, classification, real time.
Findings: It examines the changes in the geopolitical and geoeconomic landscape following the full-scale invasion of Ukraine by the Russian Federation. The article outlines the trends in the formation of a new security environment and the processes influencing its transformation. It demonstrates that the so-called Global South has, in recent years, become a relevant factor in contemporary geopolitical processes.
Theoretical implications: The current geopolitical situation compels Ukraine to develop foreign policy decisions aligned with its national interests, and with its geopolitical and geostrategic position within both the regional and global international systems.
Paper type: theoretical.

Ключові слова: геополітика, безпека, нова архітектура безпеки, новий світовий порядок, повномасштабне вторгнення, міжнародні відносини, зовнішньополітичні рішення, геополітичне становище.

Key words: geopolitics, security, new security architecture, new world order, full-scale invasion, international relations, foreign policy decisions, geopolitical situation.

Вступ

Упродовж останніх десятиліть проблема трансформації світового порядку перебуває у центрі уваги міжнародних дослідників, політичних оглядачів та стратегічних аналітиків. Динаміка глобальних змін, що супроводжується появою нових полюсів сили, віддзеркалює процеси формування поліцентричної системи міжнародних відносин. Особливої актуальності це питання набуло в умовах повномасштабного вторгнення російської федерації в Україну, що не лише підірвало основи повоєнної безпекової архітектури, але й спричинило суттєвий перегляд підходів до оцінки ролі та впливу різних акторів на глобальному рівні.

У цьому контексті на особливу увагу заслуговує феномен так званого "Глобального Півдня" — умовного об'єднання країн, які дедалі активніше заявляють про власні геополітичні амбіції та прагнуть стати вагомим чинником у формуванні нового світового порядку. При цьому Глобальний Південь демонструє неоднорідність у своїх позиціях щодо ключових міжнародних подій, зокрема, російсько-української війни, що, в свою чергу, порушує питання про сутність, межі, інтереси й потенціал цього утворення як геополітичного суб'єкта.

Теоретичні основи дослідження

Проблема формування нового світового порядку вже тривалий час знаходиться у центрі уваги вчених. Серед класиків вивчення даної проблеми слід згадати Р.Арона, Г.Моргентау, К.Уолтца, Х.Булла, Л.Міллера, Р.Купера та ін.

В Україні активно використовують методологічний аспект геополітики в своїх наукових дослідженнях М. Дністрянський, О. Білорус, М. Дорошко, Г. Перепелиця, Л. Чекаленко, В. Бочарніков, С. Свєшніков та інші.

Активне осмислення регіонально-безпекової проблематики з врахуванням емпірики російсько-української війни відбувається в іноземних аналітичних центрах – у США: в Інституті вивчення війни (ISW), Інституті досліджень зовнішньої політики (FPRI), Центрі стратегічних та міжнародних досліджень (CSIS), Дослідницькому центрі RAND Corporation, Університеті національної оборони, у Великій Британії – в Центрі аналізу європейської політики при Королівському коледжі Лондона, Королівському об'єднаному інституті оборонних досліджень (RUSI), Міжнародному інституті стратегічних досліджень (IISS) та ін.

Водночас, останнім часом увага міжнародних експертів прикута до нового полюсу світової ваги та геополітичного тяжіння – Глобального Півдня.

Постановка проблеми

Повномасштабне вторгнення рф в Україну докорінно змінило сприйняття безпекової ситуації у світі як на глобальному, так і на регіональному й субрегіональному рівнях. Картина сучасного світу явно контрастує з тим, що був у другій половині XX ст., коли холодне протистояння між геостратегічним Сходом та Заходом базувалося швидше на міжнародній статиці, аніж динаміці.

Як слушно зауважив Надзвичайний і Повноважний Посол України Сергій Корсунський: "Стан геополітики на сучасному історичному етапі можна описати не надто простою, але зрозумілою для втаємничених формулою: кількість країн, які бажають закласти свою цеглу у фундамент нового світового порядку, більша або дорівнює кількості потенційних посередників у можливих переговорах із Росією щодо припинення війни й набагато менша за кількість вітчизняних експертів із Південно-Східної Азії, які ніколи там не були, але все добре розуміють. На виправдання останніх слід визнати, що розібратися в суперечливих діях деяких найважливіших країн регіону справді важко" [1].

Таким чином, важливість Східної та Південно-Східної Азії для світової політики й економіки є аксіомою сучасної геополітики. Глобалізація й Інтернет практично унеможливили ізоляціонізм, усунули віддаленість від зон конфліктів, і нині те, що відбувається в Європі, безпосередньо відгукується в Азії. Росія десятиліттями просувала свої інтереси в Індії та Китаї, постачала до Індо-Тихоокеанського регіону зброю, відкривала в багатьох країнах освітні центри й формувала експертне середовище. Міфи про "велику російську культуру", "боротьбу СРСР, а потім і Росії проти імперіалізму-колоніалізму", агресивне нав'язування вигідних і вигаданих історичних наративів і пряма політична корупція – далеко не повний перелік інструментів, які Москва використовувала для формування системи впливу на громадську думку та політичні кола.

Сучасне геополітичне становище змушує Україну напрацьовувати зовнішньополітичні рішення відповідні її власним національним інтересам, геополітичному і геостратегічному положенню в регіональній і глобальній міжнародній системі.

Метою статті є визначення основних геополітичних ознак нового світового порядку, зокрема, появу нового суб'єкту – Глобального Півдня.

Результати

2 березня 2022 року була прийнята перша резолюція одинадцятої надзвичайної спеціальної сесії Генеральної Асамблеї Організації Об'єднаних Націй (Резолюція Генеральної Асамблеї ООН ES-11/1) [2]. У документі висловлено жаль з приводу російського вторгнення в Україну та вимогу повного виведення російських військ і скасування рішення про визнання самопроголошених Донецької та Луганської народних республік.

Резолюцію було ухвалено: 141 голос – "за", 5 – "проти", 35 – "утрималися", 12 – "відсутні".

В свою чергу, більшість "неєвропейських" країн, які проголосували за засудження агресії Росії в березні 2022 року, не ввели санкції проти цієї держави.

Загалом, у серії голосувань в ООН з початку війни близько 40 країн, що представляють майже 50 відсотків населення світу, регулярно утримувалися або голосували проти пропозицій із засудженням російського вторгнення.

На думку експертів впливового видання *Foreign Affairs* – суперечки викликані не розбіжностями щодо війни в Україні, а натомість є симптомом ширшого синдрому: гніву з приводу подвійних стандартів Заходу та розчарування з приводу зусиль щодо реформування міжнародної системи. Зокрема деякі з них зазначають, що заснований на правилах міжнародний порядок не служить інтересам Африки. Навпаки, він зберіг статус-кво, за якого великі світові держави – західні чи східні – зберегли свої позиції домінування. Через Раду Безпеки ООН, зокрема, Китай, Франція, Росія, Великобританія та США здійснили величезний вплив на африканські країни та понизили африканські уряди лише до сторонніх спостерігачів у їхніх власних справах [3;4].

Авторитетний індійський дипломат Шівшанкар Менон підкреслив цю думку на початку 2024 року, написавши: "Відчужені та ображені, багато країн, що розвиваються, бачать війну в Україні та суперництво Заходу з Китаєм як відволікання від нагальних питань, таких як борги, зміна клімату та наслідки пандемії" [4].

Тобто, можемо констатувати, що Realpolitik зіграла свою роль у визначенні позицій окремих країн щодо повномасштабного вторгнення рф в Україну. Індія традиційно була залежною від Росії щодо військово-технічного співробітництва. ПВК "Вагнер" співпрацює з урядами Західної та Центральної Африки, щоб підтримати їх режими та виживання. А Китай, який є одним із головних джерел підтримки росії, є найбільшим торговельним партнером понад 120 країн світу.

Таким чином, так званий Глобальний Південь останніми роками став актуальним чинником сучасних геополітичних процесів. Хоча, ніхто на світовій арені нині не уявляє "Глобального Півдня" загалом. Дуже хоче його організувати й очолити об'єднання БРІКС, другий кандидат – ШОС.

Аналіз показує, що кожен, хто згадує про "Глобальний Південь", розуміє під ним щось своє. Одні мають на увазі групу держав із колоніальним минулим; інші – широкий спектр країн, що розвиваються, або в крайньому разі – членів Руху неприєднання або "групи 77". Ніхто й ніколи не складав переліку країн "Глобального Півдня", й кожне зі згаданих визначень не є ні вичерпним, ні однозначним.

Поділ на умовні Південь і Північ виник в умовах холодної війни, коли світ розділився на два табори. Східний, керований СРСР, та західний – на чолі зі США та країнами Західної Європи. В умовах цього протистояння виникла третя сила: країни, які не приєдналися ані до першого, ані до другого табору.

Термін "Глобальний південь" вперше до широкого загалу ввів у 1969 році американський політичний експерт Карл Оглсбі. В одній зі своїх статей він висловив думку, що війна у В'єтнамі завершує еру домінування цивілізаційної Півночі над Півднем. Під "Північчю"

він мав на увазі світові імперії, метрополії, тоді як терміном “Глобальний Південь” узагальнив колоніальний світ. У 60-х щодо колишніх колоній європейських (переважно) країн частіше вживали термін “Третій світ”. Малося на увазі, що перший світ – це найрозвинутіші демократичні країни з ринковою економікою, другий світ – соціалістичні країни, а третій світ – відповідно усі інші. Тобто країни, які за своїми якостями неможливо віднести до жодного з перелічених світів.

У такій класифікації явно відчувався дискримінаційний підтекст та симпатія до країн “Першого світу”. Здебільшого такими країнами були колишні колонії, які, отримавши незалежність, не завжди швидко орієнтувалися в перипетіях міжнародних відносин та не приєдналися до жодного з таборів. Оскільки за цим формулюванням читалося словосполучення “третій сорт”, то його вважали не зовсім коректним. Відтак з 1991 року (коли припинив своє існування “другий світ”) частіше став вживатися саме термін “Глобальний Південь”.

У 1980-му очолювана колишнім канцлером ФРН Віллі Брандтом комісія, опублікувала доповідь. Комісія констатувала величезну прірву в економічному розвитку різних країн світу. Цей поділ демонструвала так звана “лінія Брандта”. Ця лінія охоплює планету на рівні 30° північної широти, проходить між Північною та Центральною Америкою, північною частиною Африки, Близьким Сходом і більшою частиною Східної Азії. Далі лінія опускається на південь так, щоби показати належність Японії, Австралії та Нової Зеландії до Глобальної Півночі [5].

Географічно термін Глобальний південь застосовується до 32 країн, розташованих нижче екватора (у Південній півкулі), що відрізняє їх від 54 країн, які цілком розташовані на північ від нього. Однак цей термін нерідко помилково використовують як коротку назву для глобальної більшості, хоча більшість світового населення живе вище екватора (і там же розташована основна частина світової суші). Наприклад, ми часто чуємо, що Індія, найбільш густонаселена країна світу, і Китай, який посідає друге місце за чисельністю населення, змагаються за місце лідера Глобального Півдня. З цією метою обидві країни нещодавно провели дипломатичні конференції. Однак обидві розташовані в Північній півкулі.

Крім цього, якщо брати до уваги географічну складову, то можна взяти за основу визначення Світового Банку, яке об’єднує в собі країни середнього доходу, розташовані в Африці, Азії, Океанії, Латинській Америці та Карибському басейні. Не всі країни, які знаходяться на півдні, належать до Глобального Півдня – так, до нього не входять Австралія та Нова Зеландія, натомість межі півдня є досить умовними і деякі експерти вважають, що до нього належить, наприклад, Туреччина.

А отже, цей термін є більшою мірою політичним гаслом, ніж точним описом світу. І в цьому сенсі він, судячи з усього, набув популярності, виконуючи функцію евфемізму для заміни менш прийнятних термінів.

У сучасній геополітиці термін “Глобальний Південь” особливо активно експлуатують ревізіоністські держави, які прагнуть нового переділу світу. Приміром, представляти інтереси неіснуючого об’єднання країн хоче Китай і Росія. Щоправда, розуміючи своє політичне банкрутство, рф придумала ще один варіант назви – **“глобальна більшість”,** який, як і всі попередні варіанти, не має ні визначення, ні класифікації. Якщо судити з результатів голосування за резолюції ГА ООН, то Росія якраз у меншості, а якщо пробувати поміркувати над спробами зарахувати до “глобальної більшості” найбільш густонаселені країни світу – Китай та Індію, які з різних причин входять і до БРІКС, і до ШОС і водночас претендують на власне лідерство в представленні інтересів “Глобального Півдня”, то треба спершу запитати в них, чи згодні вони з претензіями РФ зрівнятися з ними.

Країни “Глобального Півдня” дуже різноманітні. До них належать держави з майже ідеальними показниками демократії й відверті диктатури. Частина країн, що належать до

"Глобального Півдня", засудила вторгнення Росії в Україну, але є й чимало держав, які зайняли «нейтральну» позицію, точніше, **позицію "не висловлювати жодної позиції".**

Борцем за права "Глобального Півдня" та членом БРІКС є **Південна Африка.** За даними "The Africa Wealth Report 2024" компанії "Henley&Partners" в цій країні за підсумками 2023 року налічувалося 37 400 доларових мільйонерів, 102 мультимільйонери й п'ять мільярдерів [6]. Ця країна посідає перше місце в "індексі нерівності" швейцарського банку UBS із показником 82 зі 100 можливих, зростання – 17,7% проти 2008 року. Тільки в Йоганнесбурзі – 12 300 мільйонерів і два мільярдери.

Бразилія – на другому місці в "індексі нерівності", **Індія** – на четвертому. **США**, яким БРІКС кидає виклик, – на почесному третьому місці. Країни Глобального Півдня, як-от **Єгипет, Нігерія, Кенія, Марокко, Маврикій, Алжир, Гана, Ефіопія й Намібія,** належать до лідерів континенту за кількістю доларових мільйонерів, і прогнози кажуть про зростання їх кількості на 80% упродовж наступних десяти років.

За даними звіту OXFAM, традиційно представленого в Давосі, 1% багатих людей Африки володіє майже половиною багатства континенту. Майно сімох найбагатших людей становить 52 млрд дол., що перевищує доходи 700 мільйонів африканців. Єдиний мільярдер Зімбабве збільшив своє майно на 40% з 2020 року, а найбагатша людина Африки – нігерієць, у нього монополія на цемент, і він платить податок в 1% із прибутку вже 15 років.

Цікаво, що за даними OXFAM, **країни Африки щороку недоотримують по 200 млрд дол. через різні схеми ухиляння від податків найбільших корпорацій – національних і міжнародних**. Тим часом саме корпоративні податки для африканських держав **є основним джерелом фінансування соціальних програм і формування бюджетів**. Узагалі всі ці проблеми – не африканські й не "південні", а загальносвітові. П'ятеро найбагатших людей планети подвоїли свої статки за останні три роки, тоді як доходи 5 мільярдів людей за цей час зменшилися [7].

13,5% населення Індії живе на 15 дол. на місяць, ВВП на душу населення трохи перевищує 2 тис. дол. Водночас у липні 2024 року ЗМІ повідомили про триденні святкування з нагоди весілля сина найбагатшої людини в Індії й Азії **Ананта Амбані.** За різними оцінками, витрати на грандіозний захід становитимуть до 350 млн дол. На весілля запросили не тільки прем'єр-міністра найбільшої демократії Азії Нарендру Моді, членів уряду й парламенту, а й Марка Цукерберга, Білла Гейтса, Гілларі Клінтон, Тоні Блера, Бориса Джонсона, сестер Кардаш'ян, Бекхемів, доньку Трампа Іванку й багатьох інших [8].

В свою чергу, науковці Берлінського університету імені Гумбольдтів порахували, що 2004 року поняття "Глобальний Південь" зустрічалося в публікаціях близько 20 разів. Тоді як 2014-го таких публікацій було вже сотні.

Боротьба за Глобальний Південь була завжди і активізувалася в 50–60-ті роки через розпад колоніальної системи, коли в Африці, Азії і на Близькому Сході постали нові держави.

Але останні роки ця увага справді зростає. У країнах Глобального півдня живе більшість населення планети. А демографія показує, що через 25 років кожен п'ятий на Землі буде африканець. Географічні та кліматичні факторами, забезпечення міграційної безпеки, усі ці питання не дозволяють Глобальній Півночі не враховувати те, що відбувається тут.

Крім того, зауважує Ігор Семиволос, зростання уваги до Півдня збігається з певною кризою Заходу, який тривалий час активно контролював цю територію, а тепер відмовляється від цієї ролі. І в цих місцях виникає порожнеча, яку намагаються заповнити інші держави, зокрема Китай чи Індія [9].

Відомий індійський аналітик Сі Раджа Мохан зазначив: "Три саміти – один у Давосі, Швейцарія, а інші два (*NAM* і *G77*) у Кампалі, Уганда – вказують на те, що глобальна політика зміниться у 2024 році. Багаті та могутні люди світу в Давосі та знедолені в Кампалі мають спільну думку. Проблема – вирішення структурних змін у міжнародній системі. Старі гасла –

про глобалізм у Давосі та колективізм Глобального Півдня в Кампалі – більше не заслуговують на довіру та не є стійкими". Саміти, на його думку, також підкреслюють контраст між планами на майбутнє провідних держав Азії – Індії та Китаю, які змагаються, з-поміж іншого, і за вплив на Глобальному Півдні. Щорічна зустріч у Давосі є визнанням того, що відновлений конфлікт великих держав та економічний націоналізм загальмували "візок глобалізації", тоді як саміти в Кампалі виявили, що відновлена протягом останнього року політична ейфорія щодо Глобального Півдня недостатня для вирішення викликів і можливостей мінливого світового порядку [10].

Тобто, публічно доступні дані свідчать про **деяку невідповідність ідейного образу жертв колоніального минулого й практичних інтересів бізнес-еліти "жителів півдня".**

Але ж, виходячи з тих подій, які переживає Україна та й увесь світ у зв'язку з повномасштабною військовою агресією РФ, слід казати про наочну політичну кризу у сучасних міжнародних відносинах та важливість залучення держав Глобального Півдня до обговорення міжнародного порядку денного.

І, щоб досягти успіху на цьому шляху, ми маємо підходити індивідуально до кожної з цих країн, бо немає загального Глобального Півдня. Є партнери, які вже з нами, або яких вже треба переводити на наш бік.

Більшість країн Глобального Півдня намагаються представити свою **позицію щодо російсько-української війни як нейтральну**. Серед основних причин такої позиції можна виділити:

загальні антиамериканські настрої в окремих країнах, які при цьому необов'язково автоматично стають проросійськими у своїй позиції;

асоціація рф з так званою антиімперіалістичною потугою, ідеологічною спадкоємицею СРСР, а відповідно більшість Західних країн, які підтримали Україну, як представників імперіалістичних держав, що асоціюються з диктатом і колоніальним минулим;

несприйняття української боротьби як антиколоніальної. Тут відбувається нашарування як стереотипного мислення, що "білі не можуть бути колонією", так і асоціація України з Європою, яка завжди сприймається як колонізатор;

одночасна залежність від західної економічної допомоги та обіцянок економічної допомоги, або існуючих контрактів з РФ;

історична приналежність до руху неприєднання.

У частини країн є нерозуміння, **яким чином може відбуватися формування умов для закінчення конфлікту, якщо до переговорів не залучена інша сторона – Росія**. Тобто для країн залишається незрозумілим формат і мета ініціативи. Ті, хто представляє себе як нейтральних, мають застереження, оскільки вважають, що поточні зустрічі мають на меті формування позиції однієї "сторони" (України та Заходу) проти іншої (Росії). А відповідно їх участь у зустрічах присвячених українській "Формулі миру" буде розцінена, як займання української сторони в конфлікті.

Інше важливе нерозуміння в середовищі країн так званого Глобального Півдня – **чому вони взагалі повинні цікавиться українськими питаннями** та долучатися до вирішення конфлікту, який знаходиться так далеко від них. Цьому, зокрема, сприяє і значна дипломатична та пропагандистська робота РФ щодо просування фейкової інформації щодо причин війни, ситуації з українськими біженцями, причин відсутності експорту зерна тощо. Але часто у внутрішніх дискусіях лунають і аргументи, що Україна ніколи не цікавилась їхніми проблемами, відповідно немає підґрунтя для солідарності.

Через низький рівень грамотності населення країн Глобального Півдня можна сміливо стверджувати, що про Україну там в кращому разі знають як про колишню радянську республіку. І новітню історію чули у викладеному російською пропагандою варіанті. Проте у цих державах більшу роль грають настрої еліт, а еліти, як відомо, мислять більш прагматично,

ніж ціннісно. Російська пропаганда намагається показати Глобальний Південь у світлі якщо не союзника, то співчуваючих держав.

Висновки

Беручи до у ваги демографічну структуру більшості країн "Глобального Півдня", значну частку молодого населення, варто робити окремий трек публічної дипломатії, який сприяв би зростанню їх підтримки України, роз'яснення причин війни, поточної ситуації та пошук тем, які відгукнулись би серед молоді. Оскільки найближчим часом очікуються вибори у багатьох важливих країнах, це може мати вплив на те, яких політиків вони підтримують у своїх країнах.

Україні варто активно використовувати можливості та майданчики різноманітних міжнародних організацій, окрім ООН, де беруть участь країни Глобального Півдня. На додаток до АСЕАН та Африканського Союзу, де Україна в останній час демонструє підвищений рівень інтересу, важливо налагодження сталої комунікації з іншими організаціями, зокрема ЕКОВАС, АРЕС, ОАД, Лігою арабських держав тощо. Більше того, для багатьох країн цього регіону, парламентська дипломатія буде мати значний вплив, тому Україні необхідно посилити використання можливостей Міжпарламентського Союзу, де українські парламентарі вже активізували свою діяльність.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Корсунський С. Як Україні завоювати уми Азії. URL: https://zn.ua/ukr/WORLD/jak-ukrajini-zavojuvati-umi-aziji.html (дата звернення 15.04.2025).
2. Aggression against Ukraine: resolution / adopted by the General Assembly. URL: https://digitallibrary.un.org/record/3965290?ln=ru&v=pdf (дата звернення 16.04.2025).
3. ERO COMFORT. The Trouble With «the Global South». URL: https://www.foreignaffairs.com/world/trouble-global-south (дата звернення 25.04.2025).
4. Miliband David. The World Beyond Ukraine. URL: https://www.foreignaffairs.com/ukraine/world-beyond-ukraine-russia-west (дата звернення 25.04.2025).
5. Городиський А. Що таке Глобальний Південь, чого він хоче і чому про нього стільки говорять? URL: https://www.rfi.fr (дата звернення 15.04.2025).
6. The Africa Wealth Report 2024. URL: https://www.henleyglobal.com/publications/africa-wealth-report-2024 (дата звернення 16.04.2025).
7. The Middle East and North Africa Gap. URL: https://oxfamilibrary.openrepository.com/bitstream/handle/10546/621549/bp-mena-gap-prosperity-for-the-rich-austerity-for-the-rest-051023-en.pdf; jsessionid=30C645BA2DF485B6305EEF8F5EEDE050?sequence=13 (дата звернення 17.04.2025).
8. Зірки, політики і магнати приїхали з усього світу на розкішне весілля в Індії. URL: https://www.bbc.com/ukrainian/articles/crgevp9d1v9o (дата звернення 17.04.2025).
9. The Use of the Concept «Global South» in Social Science & Humanities. URL: https://www.academia.edu/7917466 (дата звернення 17.04.2025).
10. Борділовська О. Глобальний Південь у контексті нових викликів. URL: https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/hlobalnyy-pivden-u-konteksti-

novykh-vyklykiv (дата звернення 25.04.2025).

References

1. Korsunsky S. How Ukraine can win the minds of Asia. Availalble from : https://zn.ua/ukr/WORLD/jak-ukrajini-zavojuvati-umi-aziji.html (date of application 15.04.2025).
2. Aggression against Ukraine: resolution / adopted by the General Assembly. Availalble from : https://digitallibrary.un.org/record/3965290?ln=ru&v=pdf (date of application 16.04.2025).
3. ERO COMFORT. The Trouble With «the Global South». Availalble from : https://www.foreignaffairs.com/world/trouble-global-south (date of application 25.04.2025).
4. Miliband David. The World Beyond Ukraine. Availalble from : https://www.foreignaffairs.com/ukraine/world-beyond-ukraine-russia-west (date of application 25.04.2025).
5. Horodysky A. What is the Global South, what does it want and why is there so much talk about it? Availalble from : https://www.rfi.fr (date of application 15.04.2025).
6. The Africa Wealth Report 2024. URL: https://www.henleyglobal.com/publications/africa-wealth-report-2024 (date of application 16.04.2025).
7. The Middle East and North Africa Gap. Availalble from : https://oxfamilibrary.openrepository.com/bitstream/handle/10546/621549/bp-mena-gap-prosperity-for-the-rich-austerity-for-the-rest-051023-en.pdf; jsessionid=30C645BA2DF485B6305EEF8F5EEDE050?sequence=13 (date of application 17.04.2025).
8. Stars, politicians and tycoons came from all over the world for a luxurious wedding in India. Availalble from : https://www.bbc.com/ukrainian/articles/crgevp9d1v9o (date of application 17.04.2025).
9. The Use of the Concept «Global South» in Social Science & Humanities. Availalble from : https://www.academia.edu/7917466 (date of application 17.04.2025).
10. Bordilovska O. The Global South in the Context of New Challenges. Availalble from : https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/hlobalnyy-pivden-u-konteksti-novykh-vyklykiv (date of application 25.04.2025).

Резільєнтність ринку молочних продуктів України в контексті досягнення цілей сталого розвитку

Resilience of the Ukrainian Dairy Product Market in the Context of Achieving Sustainable Development Goals

Олександр Лайко
д. економ. наук, професор, e-mail: alexlayko@gmail.com, ORCID: 0000-0001-7082-0862

Oleksandr Laiko
Dr of Economics Science, Professor, e-mail: alexlayko@gmail.com, ORCID: 0000-0001-7082-0862

Державна установа "Інститут ринку і економіко-екологічних досліджень Національної академії наук України", Одеса, Україна

State Organization "Institute of Market and Economic and Ecological Research of the National Academy of Sciences of Ukraine", Odesa, Ukraine

Received: April 21, 2025 | Revised: April 28, 2025 | Accepted: April 30, 2025

UDC 338.439.5:637.1(477):005.334:330.341.1

DOI: 10.33445/sds.2025.15.2.28

Мета роботи: Наукове обґрунтування теоретико-методологічних засад формування резільєнтності ринку молочних продуктів України в умовах екстремальних шоків та розробка стратегічних рекомендацій щодо підвищення адаптивної здатності для досягнення цілей сталого розвитку в контексті воєнного стану та постконфліктного відновлення.

Метод дослідження: Комплексний підхід, що поєднує системний аналіз, статистичне моделювання, експертне оцінювання та порівняльний аналіз на основі теорії складних адаптивних систем, концепції панархії, теорії резільєнтності та методології оцінки сталого розвитку ООН.

Результати дослідження: Формування науково-методичного базису для державної стратегії резільєнтності молочної промисловості до 2030 року з інвестиційними потребами 1,4 млрд дол., створення інструментарію оцінки адаптивної здатності підприємств та механізмів адаптації європейських моделей резільєнтності до українських умов з рекомендаціями щодо диверсифікації експорту та подолання квотних обмежень ЄС.

Теоретична цінність дослідження: Розробка концепції "конфліктної резільєнтності" агропродовольчих систем в умовах воєнних дій, емпіричне обґрунтування феномену "адаптивної трансформації" з еволюцією в нову структурну конфігурацію, систематизація п'яти національних моделей резільєнтності молочних систем з оцінкою трансферабельності, формулювання принципів "адаптивної сталості" як динамічної балансировки цілей залежно від рівня загроз.

Тип статті: дослідницька.

Purpose: Scientific substantiation of theoretical and methodological foundations for forming resilience of Ukraine's dairy products market under extreme shocks and development of strategic recommendations for enhancing adaptive capacity to achieve sustainable development goals in wartime and post-conflict recovery.

Method: Comprehensive approach combining systems analysis, statistical modeling, expert assessment and comparative analysis based on complex adaptive systems theory, panarchy concept, resilience theory and UN sustainable development assessment methodology.

Findings: Formation of scientific-methodological basis for Ukraine's dairy industry resilience strategy until 2030 with $1.4 billion investment needs, creation of tools for assessing enterprises' adaptive capacity and mechanisms for adapting European resilience models to Ukrainian conditions with recommendations for export diversification and overcoming EU quota restrictions.

Theoretical implications: Development of "conflict resilience" concept for agri-food systems under warfare conditions, empirical substantiation of "adaptive transformation" phenomenon evolving into new structural configuration, systematization of five national dairy systems resilience models with transferability assessment, formulation of "adaptive sustainability" principles as dynamic goal balancing depending on threat levels.

Paper type: research.

Ключові слова: резільєнтність, ринок молочних продуктів, сталий розвиток, продовольча безпека, інновації, агропродовольчі системи, воєнний стан, адаптивна здатність, експорт молочної продукції, євроінтеграція.

Key words: resilience, dairy market, sustainable development, food security, innovation, agri-food systems, martial law, adaptive capacity, dairy exports, European integration.

Вступ

Трансформація глобальних агропродовольчих систем відповідно до принципів сталого розвитку визначає ключові вектори розвитку світової економіки у XXI столітті. Ринок молочних продуктів, який забезпечує понад 150 млн т продукції щорічно та формує 4% світового ВВП у сільськогосподарському секторі (FAO, 2024), посідає стратегічне місце у досягненні Цілей

сталого розвитку ООН. Концепція резільєнтності агропродовольчих систем, сформульована Tendall et al. (2015), визначає здатність продовольчої системи забезпечувати достатню кількість безпечної їжі перед обличчям непередбачуваних порушень при збереженні довгострокової стабільності. У молочній промисловості резільєнтність набуває особливого значення через мультифункціональність галузі.

Актуальність дослідження посилюється конвергенцією глобальних мегатрендів. Кліматичні зміни можуть призвести до скорочення продуктивності молочних корів на 10-25% до 2050 року (IPCC, 2024). Зростання світового населення до 9,7 млрд осіб (UN DESA, 2022) створює подвійний тиск на галузь.

Цілі сталого розвитку формують нормативну рамку трансформації. Особливе значення мають ЦСР 2 “Подолання голоду” (молочні продукти забезпечують 18% споживання білка, FAO, 2023), ЦСР 8 “Гідна праця” (понад 1 млрд зайнятих глобально, ILO, 2023), та ЦСР 12 “Відповідальне споживання” (потреба скорочення викидів на 30% до 2030 року, Paris Agreement, 2015).

Сучасні наукові дослідження демонструють еволюцію підходів до резільєнтності. Béné et al. (2019) розробляють багатовимірну модель, що інтегрує здатність до поглинання шоків, адаптації та трансформації. Marshall et al. (2016) аналізують роль трансформаційного потенціалу у підвищенні резільєнтності через системи точного землеробства та моніторингу. Інноваційні стратегії включають диверсифікацію білкових джерел. Kumar et al. (2022) досліджують потенціал мікроводоростей як джерела білка з використанням на 95 % менше водних ресурсів порівняно з традиційним виробництвом. Системи інтеграції ланцюгів постачання є ключовим механізмом підвищення резільєнтності. Bunchongpru & Maneerattanarungrot (2025) доводять, що інтеграція з постачальниками підвищує економічну ефективність на 23 %. Технологічні інновації спрямовані на мінімізацію екологічного впливу. Neethirajan (2024) аналізує метан-інгібуючі добавки, що скорочують викиди метану на 20-30%. Споживчі тренди формують нові вимоги: 67% споживачів готові доплачувати 15-20% за продукти з підтвердженими стандартами сталості (Jaeger et al., 2024).

В українському контексті дослідження набуває критичного значення через виклики воєнного стану. Агресія призвела до руйнування 23% потужностей молокопереробки, втрати 18% поголів'я та скорочення виробництва на 22% (Держстат України, 2024). Водночас промисловий сектор демонструє адаптивність, нарощуючи виробництво на 5,4 % у 2025 році (ABM, 2025).

Євроінтеграційні процеси створюють додаткові виклики адаптації до стандартів ЄС. Стратегія “Від ферми до виделки” (European Commission, 2020) передбачає скорочення використання антибіотиків на 50 % та досягнення 25 % частки органічного виробництва до 2030 року. Недостатньо вивченими залишаються питання адаптації міжнародних підходів до специфічних умов України, зокрема функціонування в умовах воєнного стану та майбутньої інтеграції до європейського продовольчого простору.

Мета дослідження полягає в науковому обґрунтуванні теоретико-методологічних засад формування резільєнтності ринку молочних продуктів України в умовах екстремальних шоків та розробленні стратегічних рекомендацій щодо підвищення його адаптивної здатності для досягнення цілей сталого розвитку.

Завдання дослідження:

1. Систематизувати теоретичні підходи до резільєнтності агропродовольчих систем та розробити концептуальну модель адаптації міжнародного досвіду.
2. Провести аналіз трансформаційних процесів у ринку молочних продуктів України в умовах воєнного стану та оцінити їх вплив на досягнення ЦСР.
3. Обґрунтувати стратегічні напрями підвищення резільєнтності в контексті євроінтеграції та сталого розвитку.

Об'єктом дослідження є резільєнтність ринку молочних продуктів України в умовах воєнного стану та глобальних викликів сталого розвитку.

Предметом дослідження є структурно-функціональні трансформації та стратегії формування резільєнтності ринку в контексті досягнення цілей сталого розвитку.

Методологічна база ґрунтується на теорії складних адаптивних систем (Holland, 1992), концепції панархії (Holling, 2001), теорії резільєнтності (Walker & Salt, 2006) та методології ООН (UN SDG Framework, 2015).

Практична значимість полягає у розробленні рекомендацій щодо відновлення галузі: розрахунок инвестиційних потреб у 1,4 млрд дол. до 2030 року; стратегія диверсифікації експорту; механізми консолідації галузі з урахуванням переваг великих підприємств (рентабельність 18,5% проти збитковості -7,3% у дрібних господарств).

Наукова новизна полягає у виявленні парадоксального ефекту війни: при загальному скороченні виробництва на 19% промислові підприємства збільшили виробництво на 13,2%, що змінило структуру галузі; систематизації міжнародного досвіду через аналіз п'яти національних моделей; розробленні методики кількісної оцінки трансферабельності практик; обґрунтуванні концентрації виробництва як основного фактора виживання в екстремальних умовах.

Теоретичні основи дослідження

Концепція резільєнтності, що виникла завдяки роботам К.С. Холлінга (Holling, 1973), еволюціонувала від простого розуміння здатності системи повертатися до первісного стану до складного уявлення про адаптивні властивості складних систем. Розвиток у працях Волкера та Солта (Walker & Salt, 2006) привів до розуміння резільєнтності як динамічного процесу, що включає опірність, відновлення та трансформацію. Tendall et al. (2015) формалізували визначення резільєнтності продовольчих систем як здатності забезпечувати достатню кількість прийнятної їжі перед обличчям непередбачуваних порушень. Теорія складних адаптивних систем (Holland, 1992) надає концептуальну основу для розуміння молочних ринків як мереж взаємопов'язаних агентів, де властивості емерджентності створюють нові якості.

Концепція сталого розвитку, формалізована у звіті Брундтланд (1987) та операціоналізована через ЦСР ООН (2015), забезпечує нормативну основу для оцінки ефективності з точки зору довгострокової життєздатності.

Mwirigi et al. (2025) досліджують реалізацію цілей сталого розвитку молочної промисловості засобами інноваційних технологій та впровадженням системи сталого управління для вирішення нових проблем сталого розвитку в цьому секторі. Paiva et al. (2024) демонструють, як інтеграція сталих практик може трансформувати сільські громади. Концепція соціально-екологічних систем Ostrom (2009) підкреслює нерозривний зв'язок між людською діяльністю та природними екосистемами. Mosibo et al. (2024) аналізують білки мікроводоростей Arthrospira platensis та Chlorella vulgaris, які містять 50-70% білків від сухої ваги. Abbas et al. (2013) досліджують потенціал холодної плазми як альтернативи пастеризації. Infascelli et al. (2023) представляють підхід "One Health" через "Noble Method®", який інтегрує принципи здоров'я людини, тварин та навколишнього середовища.

Теорія ланцюгів створення вартості Porter (1985) надає аналітичну рамку для розуміння взаємодії етапів виробництва молочних продуктів. Bunchongpru та Maneerattanarungrot (2025) показали позитивний вплив інтеграції з постачальниками на сталість молочних господарств. Artukoglu & Olgun (2008) встановили, що 70% виробників молока є акціонерами кооперативів.

Paeizi et al. (2023) представляють багатоетапну структуру проектування мереж ланцюгів постачання з урахуванням сталості та резільєнтності. Abbasian & Jamili (2025) розвивають гібридну модель машинного навчання для оцінки постачальників у контексті Supply Chain 4.0.

Jaeger et al. (2024) провели опитування 1206 новозеландців щодо очікувань від сталих

йогуртів, виявивши зв'язок між сенсорними та несенсорними очікуваннями споживачів. Balan & Trasca (2025) моделюють сценарії заміни тваринного білка рослинним, виявивши потенціал збереження від 84 020 до 1 067 443 гектарів землі. Patel et al. (2023) підкреслюють важливість систем відстеження для швидкопсувних продуктів через зростання фальсифікації. Martínez-Olvera & Mora-Vargas (2019) представляють структуру оцінки продуктивності в контексті Industry 4.0. Tița et al. (2024) розкривають потенціал циркулярної економіки через використання молочної сироватки, оскільки понад 40 % сироватки викидається глобально.

Економічна теорія ринкових невдач забезпечує аналітичну основу для розуміння ситуацій неоптимального розподілу ресурсів. У молочній промисловості важливі екстерналії, асиметрія інформації та монопольна влада. Поведінкова економіка додає психологічний вимір через концепції обмеженої раціональності та когнітивних упереджень.

Синтез теоретичних підходів створює комплексну концептуальну рамку для аналізу резільєнтності як багаторівневої системи, що функціонує в умовах невизначеності. Виявляються прогалини щодо комплексної оцінки резільєнтності в умовах екстремальних шоків, що актуалізує дослідження адаптивних механізмів у кризових умовах.

Результати

1. Національні моделі резільєнтності молочних систем у контексті сталого розвитку

Дослідження міжнародного досвіду формування резільєнтних молочних систем виявляє існування п'яти домінуючих національних моделей, кожна з яких відображає унікальне поєднання природно-кліматичних умов, інституційного середовища та стратегічних пріоритетів розвитку (табл. 1).

Таблиця 1. Порівняльна характеристика національних моделей резільєнтності молочних систем

Країна/Модель	Ключові характеристики	Механізми резільєнтності	Внесок у ЦСР	Показники ефективності
Данія (Скандинавська модель)	Високотехнологічне виробництво, потужні кооперативи	Цифровізація ферм, довгострокові контракти, екостандарти	ЦСР 2, 8, 12, 13	Продуктивність +15-20%, викиди ПГ -12%
Швеція (Скандинавська модель)	Інтеграція екологічних стандартів, стабільність доходів	Контрактна система, інвестиції в сталі технології	ЦСР 3, 12, 15	85% ферм у кооперативах
Нідерланди (Інтенсивна модель)	Максимальна продуктивність, циркулярна економіка	Точне землеробство, біогаз з відходів, автоматизація	ЦСР 7, 9, 12	9000+ кг молока/корову, 40% енергії з біогазу
Нова Зеландія (Експортна модель)	Пасовищне виробництво, глобальна орієнтація	Система хеджування, диверсифікація ринків	ЦСР 2, 8, 15	95% молока на експорт, стабільні ціни
Канада (Регульована модель)	Квотна система, гарантовані ціни	Управління пропозицією, екологічні квоти	ЦСР 1, 2, 13	Стабільні доходи, -18% викидів за 10 років
Німеччина (ЄС модель)	Добровільні угоди, премії за сталість	Еко-схеми САП, стандарти добробуту тварин	ЦСР 3, 12, 15	25% виплат на еко-схеми

Джерело: складено автором на основі Neethirajan (2024), European Commission (2023), Bunchongpru & Maneerattanarungrot (2025)

Скандинавська модель (Данія, Швеція) характеризується поєднанням високих технологій, кооперативної організації та екологічних стандартів. Данська молочна галузь лідирує у впровадженні цифрових технологій: автоматизовані системи доїння, IoT-моніторинг здоров'я тварин, прецизійна годівля (Neethirajan, 2024).

Кооператив Arla Foods об'єднує понад 9000 фермерів та інвестує 150 млн євро щорічно в сталі технології. Результат: підвищення продуктивності на 15-20% при скороченні викидів на 12% (European Commission, 2023).

Нідерландська інтенсивна модель демонструє максимальну продуктивність через циркулярну економіку та точне землеробство. Досягнуто рекордну продуктивність понад 9000 кг молока на корову завдяки передовій генетиці, оптимізованій годівлі та автоматизації (Bunchongpru & Maneerattanarungrot, 2025). Органічні відходи перетворюються на біогаз, забезпечуючи 40% енергопотреб ферм (Tița et al., 2024).

Новозеландська експортна модель базується на пасовищному утриманні та глобальній орієнтації – 95% молока спрямовується на експорт (Jaeger et al., 2024). Fonterra розробила систему управління ризиками через глобальне хеджування та диверсифікацію ринків у понад 140 країнах.

Канадська регульована модель поєднує ринкові механізми з державним регулюванням через квоти на виробництво молока. Канадська рада встановлює квоти на основі внутрішнього споживання, що забезпечує стабільні ціни та доходи при скороченні викидів на 18% за 10 років (Neethirajan, 2024).

Європейська модель (Німеччина) демонструє найбільш прогресивний підхід до інтеграції сталого розвитку через реформовану Спільну аграрну політику ЄС. Нова архітектура САП 2023-2027 революційно змінює систему підтримки фермерів, спрямовуючи 25% прямих виплат на еко-схеми, що включають органічне виробництво, підвищення стандартів добробуту тварин та збереження біорізноманіття (European Commission, 2023). Німецькі переробні підприємства активно укладають добровільні угоди з фермерами щодо підвищення стандартів виробництва в обмін на премії до закупівельних цін, створюючи ринкові стимули для сталого розвитку (Infascelli et al., 2023). Ця модель особливо важлива для України як кандидата в члени ЄС, оскільки демонструє практичні механізми імплементації європейських стандартів сталості в молочному виробництві.

Ключові закономірності:

– Високий рівень організації виробників через кооперативи забезпечує мобілізацію ресурсів для інвестицій.

– Інтеграція екологічних цілей з економічними через ринкові стимули та регуляторні вимоги.

– Технологічні інновації поєднують цифровізацію з циркулярними підходами.

– Ефективне управління ризиками через диверсифікацію та фінансові інструменти.

Європейська модель має критичне значення для України в контексті євроінтеграційних процесів, оскільки демонструє практичні шляхи адаптації до стандартів ЄС через поступове впровадження еко-схем та механізмів стимулювання сталого виробництва, що може стати основою для розробки національної стратегії розвитку молочної галузі.

2. Інтеграція принципів сталого розвитку в молочне виробництво

Міжнародний досвід демонструє еволюцію від традиційних підходів до інтегрованих моделей. Спільна аграрна політика ЄС на період 2023-2027 років стала каталізатором системної трансформації молочного виробництва (рис. 1).

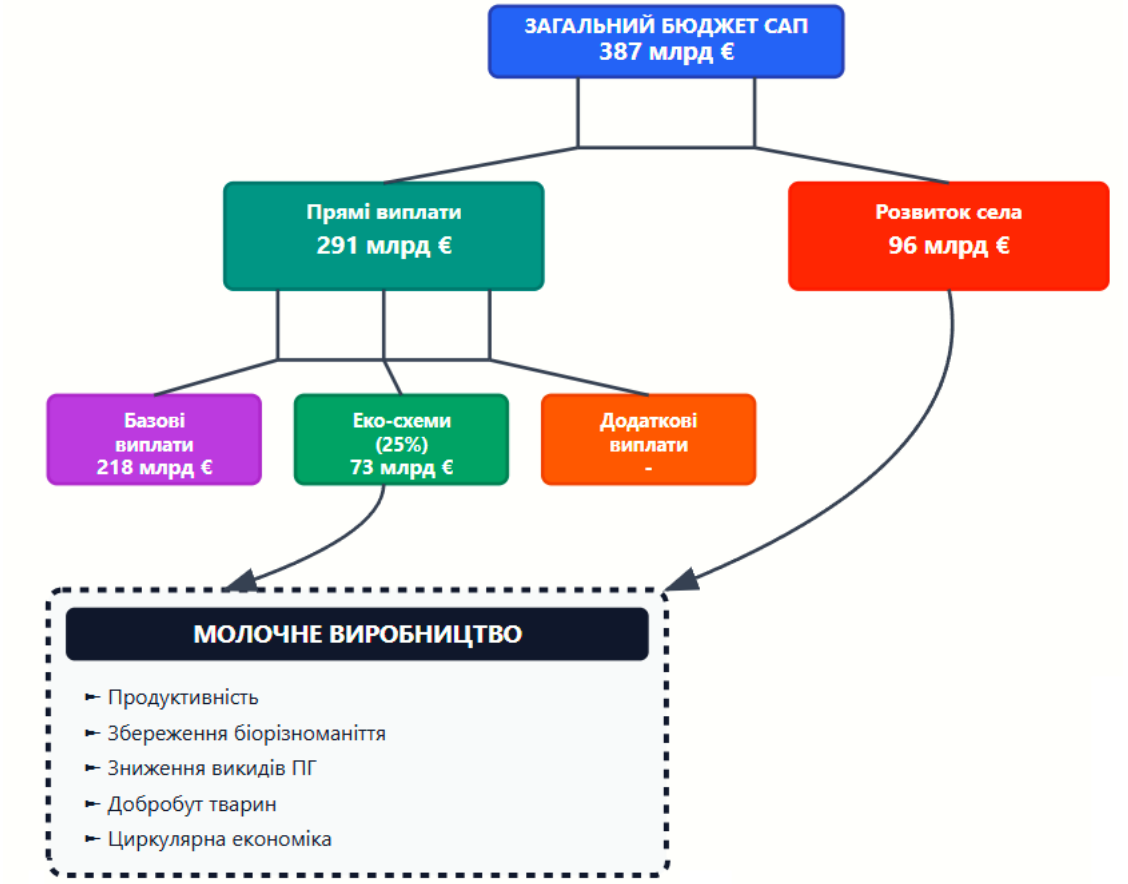


Рисунок 1. Структура фінансування САП ЄС 2023-2027: екологізація молочного виробництва
Джерело: складено автором на основі European Commission (2023)

Нова архітектура САП кардинально змінила підходи до підтримки аграрного сектору, переорієнтувавши фінансування з виробничих субсидій на стимулювання сталих практик (European Commission, 2023).

Революційність нового підходу полягає в обов'язковому спрямуванні 25% прямих виплат фермерам на еко-схеми, що включають органічне виробництво, підвищення стандартів добробуту тварин, збереження біорізноманіття та зменшення викидів парникових газів.

Німецький досвід демонструє ефективність поєднання регуляторних вимог з ринковими стимулами через добровільні угоди. Провідні кооперативи (DMK Group, Arla Foods Deutschland) запровадили програми преміальних виплат фермерам за дотримання підвищених стандартів сталості. Ферми, що впроваджують еко-схеми, отримують додаткові 3-5 євроцентів за літр молока, що становить 240-400 євро додаткового доходу на корову щорічно.

Французька модель акцентує на коротких ланцюгах постачання та регіональних брендах. Програма "Lait de nos régions" об'єднує понад 2800 ферм у 12 регіонах, гарантуючи походження молока в радіусі 80 км від переробного підприємства.

Європейські програми базуються на комплексному підході, що включає технологічні інновації, оптимізацію годівлі та моніторинг викидів.

Данська програма "Klimapartnerskab for Fødevarer" встановила ціль зниження викидів від молочного виробництва на 50% до 2030 року. Програма включає фінансову підтримку технологій точної годівлі, що зменшують викиди метану на 15-20% (Neethirajan, 2024).

Нідерландська програма "Koeien & Kansen" об'єднує 17 експериментальних ферм для тестування технологій зниження викидів. Результати показують можливість зниження викидів метану на 25-30 % при збереженні продуктивності.

Ірландська програма “Origin Green” охоплює понад 95% ірландського молочного експорту. Середнє зниження викидів учасників становить 12% за три роки при підвищенні економічної ефективності на 8%.

Стандарти добробуту тварин та соціальної відповідальності:

Німецька ініціатива “Tierwohl” встановлює підвищені стандарти: мінімум 6 м² простору на корову, доступ до пасовищ 120 днів на рік, заборона больових процедур без анестезії. Ферми отримують премії 4 євроцента за літр молока (Infascelli et al., 2023).

Швейцарська програма “BTS” включає вимоги до освітлення, вентиляції та можливостей для природної поведінки корів. Участь приносить додаткові 190 швейцарських франків на корову щорічно.

Данська система класифікації включає щорічний аудит за 30 критеріями з оцінкою від 1 до 4 смайликів. Рівень 3-4 смайлики обов’язковий для постачання до провідних роздрібних мереж.

Нідерландська модель демонструє найрозвиненішу циркулярну економіку. Кооператив FrieslandCampina об’єднує понад 800 ферм з мережею біогазових установок (Tița et al., 2024). Типова ферма на 200 корів генерує 180 000 м³ біогазу щорічно, забезпечуючи 60 % енергопотреб ферми.

Данська модель включає промислові симбіози. Arla Foods розвиває партнерства з пивоварнями, хлібопекарнями та виробниками біопластику, зменшуючи витрати на корми на 15-20%.

Французька програма “Méthanisation” стимулює колективні біогазові установки для 8-12 ферм. Держава надає субсидії до 40% капітальних витрат та гарантовані тарифи на 20 років.

Інноваційні підходи включають переробку молочної сироватки на функціональні інгредієнти. Італійська Glanbia Nutritionals створює додану вартість 15-20 євро за кілограм порівняно з 0,3 євро за сиру сироватку.

Результати впровадження циркулярних моделей на 150 європейських фермах показали (Bunchongpru & Maneerattanarungrot, 2025): зниження операційних витрат на 12-18%; зменшення викидів пг на 20-25%; створення додаткових джерел доходу 8-15% від загального доходу.

Ці результати підтверджують ефективність циркулярних підходів як інструменту досягнення ЦСР в молочному виробництві.

3. Механізми підвищення резільєнтності на різних рівнях системи

Резільєнтність молочних систем формується через взаємодію механізмів на трьох основних рівнях: фермерському (мікрорівень), галузевому (мезорівень) та національному (макрорівень). Ефективність загальної системи визначається синергетичною взаємодією між рівнями та узгодженістю їх функціонування в умовах зовнішніх викликів.

Фермерський рівень: диверсифікація та технологічні інновації.

Механізми резільєнтності концентруються навколо стратегій диверсифікації, технологічних інновацій та кооперативних зв’язків.

Диверсифікація реалізується через продуктову, географічну та функціональну диверсифікацію. Данські ферми з дуальною моделлю виробництва (органічна + традиційна продукція) показують на 25% вищу стабільність доходів, оскільки органічна продукція забезпечує премії 30-40% до цін (Neethirajan, 2024).

Французькі ферми програми “Circuits Courts” демонструють 18% нижчу волатільність доходів завдяки географічній диверсифікації збуту через прямі продажі та регіональні мережі.

Технологічні інновації спрямовані на підвищення ефективності та зменшення екологічного впливу. Нідерландські системи точного тваринництва дозволяють підвищити продуктивність на 12-15% при зменшенні витрат кормів на 8-10% та скороченні використання ветеринарних препаратів на 20% (Abbas et al., 2013).

Кооперативна модель відіграє критичну роль у підвищенні резільєнтності. Фермери-члени кооперативу Arla Foods показують на 22% вищу стабільність цін завдяки довгостроковим контрактам та механізмам взаємного страхування (Can & Engindeniz, 2025).

Галузевий рівень: інтеграція ланцюгів вартості.

Механізми фокусуються на оптимізації ланцюгів створення вартості, розвитку логістичної інфраструктури та стимулюванні інновацій.

Вертикальна інтеграція демонструється нідерландським кооперативом FrieslandCampina, що об'єднує понад 17000 фермерів і контролює весь ланцюг від виробництва до реалізації у 100 країнах світу (Bunchongpru & Maneerattanarungrot, 2025).

Горизонтальна інтеграція реалізується через стратегічні альянси, такі як Arla Foods і фінська Valio для ефективної конкуренції на балтійському ринку.

Цифрові платформи управління ланцюгами постачання оптимізують логістику. Данська платформа "DairyChain" інтегрує дані від понад 3000 ферм з 25 переробними підприємствами, зменшуючи логістичні витрати на 12-15%.

Національний рівень: політична підтримка та інституційний розвиток.

Механізми включають політичну підтримку, інституційну інфраструктуру та регулювання міжнародної торгівлі.

Політична підтримка еволюціонувала до комплексних програм сталого розвитку. Данська стратегія "Green Tripartite Agreement" передбачає інвестування 24 млрд данських крон до 2030 року в трансформацію аграрного сектору.

Французька модель акцентує на територіальних брендах. Система AOC для сирів (понад 400 французьких сирів) генерує додану вартість 2,3 млрд євро щорічно та забезпечує стабільні доходи для 35000 молочних ферм.

Інституційний розвиток включає спеціалізовані агенції підтримки. Канадська рада з молочних продуктів регулює ринок через систему управління пропозицією, встановлюючи річні квоти виробництва.

Регулювання міжнародної торгівлі демонструється новозеландською стратегією диверсифікації. Fonterra експортує до понад 140 країн, при цьому жоден ринок не становить більше 15% загального експорту.

Синергетична взаємодія механізмів на різних рівнях створює системний ефект. Скандинавська модель демонструє найрозвиненішу інтеграцію, де фермерські кооперативи підтримуються галузевими програмами інновацій та національною політикою сталого розвитку, забезпечуючи найвищу в світі резільєнтність молочних систем.

4. Стан та динаміка розвитку ринку молочних продуктів України в умовах воєнного стану

Молочна промисловість України зазнала кардинальних трансформацій у період повномасштабного вторгнення, демонструючи стійкість промислового сектору та глибокі структурні зміни. До війни Україна входила до двадцятки найбільших світових виробників молока, при цьому функціонувало близько 350 підприємств з переробки молока (Herun, 2022).

Найбільш значущою тенденцією є кардинальна зміна структури виробництва молока з концентрацією в промисловому секторі. Дані за 2018-2024 роки демонструють парадоксальну ситуацію: при загальному скороченні виробництва на 15,5% (з 10,064 до 8,5 млн т) сільськогосподарські підприємства збільшили обсяги на 8,9%, тоді як господарства населення скоротили виробництво до 75,3% від рівня 2018 року (Ужва, 2024; АВМ, 2025).

Така диференціація свідчить про фундаментальну трансформацію галузі в бік концентрації виробництва у великих підприємствах, які мають кращі можливості для адаптації до воєнних умов. Частка підприємств у загальному виробництві зросла з 27,4% у 2018 році до 35,3% у 2024 році, що засвідчує прискорення процесів консолідації галузі.

Унікальність української ситуації підтверджується міжнародним порівнянням:

промисловий сектор демонструє зростання виробництва на 5,3% у 2024 році, тоді як традиційні молочні лідери показують значно скромніші результати. Нова Зеландія, світовий лідер молочного експорту, досягла зростання лише на 0,8%, Австралія скоротила виробництво на 1,5% через кліматичні виклики, а ЄС загалом демонструє спад на 0,9% через екологічні обмеження та скорочення поголів'я (USDA, 2024).

Це обумовлено інвестиціями в модернізацію, консолідацією виробництва та підвищенням ефективності великих підприємств, які змогли адаптуватися до екстремальних умов функціонування. Водночас структурні зміни у виробництві тісно пов'язані з динамікою поголів'я худоби, що розкриває глибинні причини диференціації між категоріями господарств.

Поголів'я великої рогатої худоби в Україні зазнало катастрофічного скорочення за період 2018-2024 років на 29,1% (з 3,333 до 2,362 млн голів), при цьому поголів'я корів скоротилося на 35,7% - з 1,956 до 1,257 млн голів (Держстат України, 2024). Особливо критичною є ситуація в господарствах населення, де поголів'я ВРХ зменшилося на 38,6%, тоді як на підприємствах скорочення становило лише 6,3%.

Скорочення поголів'я в господарствах населення обумовлено комплексом факторів: прямими військовими втратами через бомбардування сільських територій, вимушеною релокацією з прифронтових районів, економічними труднощами населення та відсутністю ефективної державної підтримки малих виробників. Водночас великі підприємства демонструють відносну стабільність завдяки можливостям інвестування в захисні споруди, резервні джерела енергопостачання та системи біологічної безпеки.

Ці структурні зміни безпосередньо впливають на ціноутворення молочного ринку, оскільки скорочення пропозиції з боку дрібних виробників створює передумови для зміни цінової кон'юнктури.

Ціноутворення на українському молочному ринку характеризується поступовою стабілізацією після періоду високої волатільності. Співвідношення цін на молоко-сировину екстра ґатунку між Україною та ЄС еволюціонувало з 68,5% наприкінці 2022 року до 85,2% наприкінці 2024 року, що свідчить про підвищення конкурентоспроможності української продукції при збереженні цінових переваг (АВМ, 2025).

Така динаміка відображає ефект девальвації гривні, зростання внутрішніх витрат виробництва через подорожчання енергоносіїв та кормів, а також адаптацію до європейських стандартів якості. Збереження цінового диференціалу на рівні 14,8% забезпечує експортний потенціал українських виробників при збереженні достатньої рентабельності для покриття підвищених ризиків воєнного періоду.

Однак реалізація експортного потенціалу стикається з серйозними викликами через обмеження доступу до ключових зарубіжних ринків.

Експорт молочної продукції стикається з критичними викликами через перевищення встановлених ЄС квот. У 2024 році українські експортери перевищили квоту на сухе знежирене молоко майже у 3 рази (298,2 % використання квоти), на вершкове масло – на 24,7 %, на згущене молоко – на 12 % (АВМ, 2025). Загальний рівень використання квот становив 119,6 %, що створює загрозу введення 25 % додаткових мит на надквотні обсяги з червня 2025 року.

Відновлення торговельних обмежень ЄС становить найбільшу загрозу для галузі, оскільки європейський напрям забезпечує 67,2 % українського молочного експорту. Потенційні втрати від введення додаткових мит можуть сягнути понад 20 млн євро щорічно лише через підвищення митних платежів, не враховуючи втрату частки ринку через зниження конкурентоспроможності.

Експортні виклики посилюються нерівномірним географічним розподілом виробничих потужностей, що сформувався внаслідок воєнних дій.

Воєнні дії спричинили значну регіональну диференціацію у розвитку молочної промисловості з формуванням нових центрів зростання у відносно безпечних регіонах.

Лідерські позиції у виробництві молока підприємствами займають Полтавська (19,0 % загального виробництва), Хмельницька (17,9 %) та Вінницька (15,7 %) області (АВМ, 2025).

Особливо вражаючими є темпи зростання у західних областях: Хмельницька область демонструє приріст виробництва на 17,1%, що пов'язано з розширенням існуючих ферм та залученням інвестицій у безпечний регіон. Такі тенденції відображають процеси релокації виробничих потужностей з прифронтових територій та концентрацію інвестицій у регіонах з мінімальними ризиками військових дій.

Регіональні зміни у виробництві тісно корелюють з економічною ефективністю різних категорій виробників, що визначає довгострокові перспективи розвитку галузі.

Аналіз економічної ефективності розкриває кардинальні відмінності між категоріями виробників, що обумовлюють подальшу концентрацію галузі. Промислові підприємства досягають середнього надою 6850 кг на корову на рік проти 3200 кг у господарствах населення, що відображає більш ніж дворазову різницю в продуктивності (АВМ, 2025).

Собівартість виробництва молока на підприємствах становить 13,20 грн за кілограм проти 16,80 грн у господарствах населення, що забезпечує промисловому сектору конкурентну перевагу у 21 %. Рентабельність виробництва на підприємствах досягає 18,5 %, тоді як господарства населення працюють збитково з рентабельністю -7,3%. Така ситуація робить неминучою подальшу концентрацію виробництва в промисловому секторі.

Однак економічна ефективність галузі знаходиться під постійною загрозою епізоотичних ризиків, що можуть миттєво знищити досягнуті результати.

Український молочний сектор функціонує в умовах підвищених епізоотичних ризиків, пов'язаних з поширенням ящуру в сусідніх країнах ЄС. З початку 2024 року в Угорщині, Словаччині та Німеччині зафіксовано 12 уражених ферм з знищенням 26,7 тис. голів худоби (Global Dairy Trade, 2025). Така ситуація створює реальну загрозу поширення інфекції в Україну з потенційно катастрофічними наслідками для експорту та внутрішнього виробництва.

Загроза епізоотій посилюється воєнними діями, які ускладнюють контроль ветеринарної ситуації на окупованих та прифронтових територіях. Порушення системи ветеринарного нагляду та вакцинації створює сприятливі умови для поширення інфекційних захворювань тварин.

Усі виявлені виклики та загрози вимагають масштабних інвестицій для забезпечення сталого розвитку галузі (табл. 2).

Таблиця 2. Інвестиційні потреби та стратегічні пріоритети

Напрям	Потреба, млн дол.	Очікуваний ефект
Відновлення пошкоджених ферм	450	Повернення 150 тис. т молока
Модернізація переробки	380	Підвищення якості на 25%
Енергонезалежність	220	Стабільність виробництва
Біологічна безпека	150	Запобігання епізоотіям
Всього	**1400**	Зростання виробництва на 30%

Джерело: авторські розрахунки на основі даних АВМ (2025), Ужва (2024)

Для повного відновлення та модернізації молочної галузі необхідно близько 1,4 млрд дол. інвестицій упродовж 2025-2030 років. Пріоритетними напрямами є відновлення пошкоджених ферм, модернізація переробних потужностей, забезпечення енерго-незалежності та підвищення біологічної безпеки.

На основі аналізу інвестиційних потреб та наявних викликів можна сформулювати реалістичні сценарії розвитку галузі.

Реалізація базового сценарію розвитку з інвестуванням 1,4 млрд дол. дозволить

досягти рівня виробництва 9,5 млн т молока до 2030 року з ймовірністю 60%. Оптимістичний сценарій передбачає досягнення 11,2 млн т при збереженні доступу до ринків ЄС та залученні додаткових інвестицій. Песимістичний сценарій може обмежити виробництво рівнем 7,8 млн т у випадку ескалації конфлікту та втрати експортних ринків.

Проведений комплексний аналіз стану молочної промисловості України в умовах воєнного стану засвідчує формування принципово нової архітектури галузі, що характеризується як адаптивними процесами, так і системними викликами. Статистичні дані за період 2018-2024 років демонструють парадоксальну резільєнтність промислового сектору: при загальному скороченні виробництва на 15,5 % великі підприємства збільшили обсяги на 8,9 %, що корелює з висновками Bunchongpru та Maneerattanarungrot (2025) про переваги інтегрованих виробничих систем в умовах криз.

Концентрація як стратегія виживання. Зростання частки підприємств у загальному виробництві з 27,4 % до 35,3 % підтверджує тезу Zarei-Kordshouli et al. (2023) про те, що консолідація є ключовим механізмом підвищення резільєнтності ланцюгів постачання в умовах невизначеності. Дворазова різниця в продуктивності між промисловими підприємствами (6850 кг/корову) та господарствами населення (3200 кг/корову) відображає структурну ефективність, описану в роботах Wang et al. (2025) щодо переваг цифровізованих молочних систем.

Епізоотичні ризики як критичний фактор. Поширення ящуру в сусідніх країнах ЄС (26,7 тис. знищених голів у 2024 році) актуалізує висновки Neethirajan (2024) про необхідність комплексних систем біологічної безпеки. Порушення ветеринарного контролю на окупованих територіях створює додаткові ризики, що підтверджує важливість інвестицій у профілактику епізоотій на рівні 150 млн дол., обґрунтовану у дослідженнях Infascelli et al. (2023).

Експортна залежність та торговельні обмеження. Перевищення квот ЄС на 119,6% (особливо критичні 298,2% по сухому молоку) підтверджує актуальність диверсифікації ринків збуту, обґрунтовану Can & Engindeniz (2024) на прикладі турецьких кооперативів. Потенційні втрати 20+ млн євро від введення додаткових мит корелюють з розрахунками Jaeger et al. (2024) щодо чутливості молочних ринків до торговельних бар'єрів.

Стратегічні рекомендації на основі емпіричних даних:

1. Диверсифікація експортних ринків – зменшення залежності від ЄС з поточних 67,2% до 50% відповідно до рекомендацій Balan & Trasca (2025) щодо географічного розподілу ризиків. Це потребує розвитку логістичної інфраструктури для далекомагістральних перевезень та адаптації продукції до стандартів азійських та африканських ринків.

2. Біологічна безпека як пріоритет національної безпеки – інвестиції 150 млн дол. у системи профілактики, обґрунтовані Abbas et al. (2024) через аналіз ефективності превентивних заходів. Створення буферних зон на кордоні з ЄС та впровадження цифрових систем моніторингу здоров'я тварин за прикладом нідерландської моделі.

3. Енергонезалежність як основа стабільності - інвестиції 220 млн дол. в автономні джерела енергії відповідають концепції циркулярної економіки Tița et al. (2024). Розвиток біогазових установок за нідерландським зразком може забезпечити 40% енергопотреб ферм при одночасній утилізації відходів.

4. Підтримка дрібних виробників для соціальної стабільності – збереження 64,7 % частки господарств населення потребує спеціальних програм, обґрунтованих Choephel et al. (2024) щодо соціальної функції молочного виробництва. Створення кооперативних структур за данською моделлю може підвищити ефективність малих господарств.

5. Інноваційна модернізація за європейськими стандартами – загальні інвестиції 1,4 млрд дол. відповідають масштабам програм САП ЄС, проаналізованих European Commission (2023). Впровадження еко-схем може забезпечити доступ до європейських програм підтримки та підвищити конкурентоспроможність на 25%.

Прогнозні сценарії та ймовірності реалізації. Базовий сценарій досягнення 9,5 млн т виробництва до 2030 року з ймовірністю 60% базується на аналізі адаптивної здатності промислового сектору, що демонструє зростання 5,3 % навіть в умовах війни. Оптимістичний сценарій (11,2 млн т) можливий за умови збереження доступу до ринків ЄС та реалізації повного інвестиційного пакету, що корелює з висновками про потенціал інноваційних технологій. Реалізація запропонованих рекомендацій потребує координації державної політики з приватними інвестиціями та міжнародною технічною допомогою. Успішність стратегії залежить від швидкості адаптації до нових торговельних реалій та ефективності заходів з біологічної безпеки, що підтверджується міжнародним досвідом у кризових умовах.

5. Трансферабельність міжнародних практик до українських умов

Для оцінки потенціалу адаптації міжнародних практик резільєнтності молочних систем до українських умов проведено комплексний SWOT-аналіз з кількісною оцінкою факторів та їх впливу на успішність трансферу технологій і підходів (табл. 3).

Таблиця 3. SWOT-матриця адаптації міжнародних практик резільєнтності до українських умов

СИЛЬНІ СТОРОНИ (S)	**Вага**	**Оцінка**	**Зважена оцінка**
S1. Значні природні ресурси (41,5 млн га с.-г. угідь)	0,15	4,8	0,72
S2. Розвинена система аграрної освіти (45 ВНЗ)	0,12	4,2	0,50
S3. Традиційно сильні позиції в зерновиробництві	0,13	4,5	0,59
S4. Географічне розташування для експорту	0,10	4,0	0,40
S5. Наявність великих інтегрованих підприємств	0,08	3,8	0,30
Всього сильних сторін	**0,58**	-	**2,51**
СЛАБКІ СТОРОНИ (W)	**Вага**	**Оцінка**	**Зважена оцінка**
W1. Обмежені фінансові ресурси (потреба 1,4 млрд дол.)	0,18	2,1	0,38
W2. Фрагментованість структури (63% у господарствах населення)	0,15	2,3	0,35
W3. Слабкий кооперативний рух (15% охоплення)	0,12	2,5	0,30
W4. Інституційна нестабільність	0,10	2,2	0,22
W5. Застаріла матеріально-технічна база	0,08	2,4	0,19
Всього слабких сторін	**0,63**	-	**1,44**
МОЖЛИВОСТІ (O)	**Вага**	**Оцінка**	**Зважена оцінка**
O1. Євроінтеграційні процеси та адаптація до стандартів ЄС	0,20	4,5	0,90
O2. Міжнародна фінансова допомога (50 млрд євро від ЄС)	0,18	4,2	0,76
O3. Зростаючий попит на якісні продукти (+20-30% доплата)	0,15	3,8	0,57
O4. Розвиток цифрових технологій та здешевлення IoT	0,12	4,0	0,48
O5. Потенціал органічного виробництва	0,10	3,5	0,35
Всього можливостей	**0,75**	-	**3,06**
ЗАГРОЗИ (T)	**Вага**	**Оцінка**	**Зважена оцінка**
T1. Тривалість воєнного конфлікту	0,25	1,8	0,45
T2. Скасування автономних торговельних заходів ЄС	0,20	2,2	0,44
T3. Кліматичні зміни та екстремальні погодні явища	0,15	2,5	0,38
T4. Зростаюча конкуренція на європейських ринках	0,12	2,8	0,34
T5. Геополітичні ризики та нестабільність регіону	0,10	2,0	0,20
Всього загроз	**0,82**	-	**1,81**

Примітка: Оцінка проводилася за 5-бальною шкалою, де 1 – мінімальний вплив, 5 – максимальний вплив. Вага факторів визначена експертним методом на основі аналізу літератури та консультацій з галузевими експертами.

Розрахунок інтегральних показників:

Показник сильних сторін (S): 2,51 Показник слабких сторін (W): 1,44 Показник можливостей (O): 3,06 Показник загроз (T): 1,81

Інтегральні коефіцієнти:

Коефіцієнт внутрішніх факторів (IFE) = S - W = 2,51 - 1,44 = 1,07

Коефіцієнт зовнішніх факторів (EFE) = O - T = 3,06 - 1,81 = 1,25

Загальний коефіцієнт привабливості = (S + O) - (W + T) = (2,51 + 3,06) - (1,44 + 1,81) = 2,32

Обґрунтування оцінок та розрахунків:

Сильні сторони. Найвищу оцінку (4,8) отримали природні ресурси України через наявність 41,5 млн га сільськогосподарських угідь, що становить 69% території країни та забезпечує потенціал для виробництва достатньої кількості кормів для 4-5 млн голів молочного поголів'я. Традиційно сильні позиції в зерновиробництві (4,5 бали) обумовлені входженням України до топ-5 світових експортерів зернових, що створює синергетичні ефекти для молочного тваринництва через забезпечення якісною кормовою базою.

Розвинена система аграрної освіти (4,2 бали) включає 45 вищих навчальних закладів аграрного профілю та 12 науково-дослідних інститутів, що готують щорічно понад 15000 спеціалістів для аграрного сектору. Географічне розташування (4,0 бали) забезпечує доступ до ринків ЄС (450 млн споживачів) та країн Близького Сходу й Азії через портову інфраструктуру.

Слабкі сторони. Найкритичнішим фактором є обмеженість фінансових ресурсів (2,1 бали), оскільки потреба в інвестиціях для модернізації галузі (1,4 млрд дол.) у 3,5 рази перевищує річний обсяг капітальних інвестицій в аграрний сектор. Фрагментованість структури (2,3 бали) проявляється в тому, що 63% молока виробляється в господарствах населення з середнім поголів'ям 2-3 корови, що ускладнює впровадження сучасних технологій.

Слабкий розвиток кооперативного руху (2,5 бали) контрастує з європейськими показниками: в Україні лише 15% фермерів об'єднані в кооперативи проти 85% у Данії. Інституційна нестабільність (2,2 бали) проявляється в частих змінах регуляторного середовища – за останні 5 років змінювалися 12 ключових нормативних актів у сфері молочного виробництва.

Можливості. Євроінтеграція (4,5 бали) створює правові передумови для адаптації європейських стандартів та доступу до ринку ЄС з 27 країнами. Міжнародна фінансова допомога (4,2 бали) включає 50 млрд євро від ЄС на відновлення, з них орієнтовно 8-10% може бути спрямовано на аграрний сектор. Зростаючий попит на якісні продукти (3,8 бали) підтверджується дослідженнями, що показують готовність 67% українських споживачів доплачувати 20-30% за органічні та екологічні молочні продукти.

Загрози. Воєнний конфлікт (1,8 бали) залишається найкритичнішою загрозою, оскільки вже призвів до втрати 23% переробних потужностей та 18% поголів'я. Скасування АТЗ ЄС (2,2 бали) може призвести до втрати 67% експорту до Європи, оскільки українська продукція програватиме в ціні при відновленні мит. Кліматичні зміни (2,5 бали) проявляються в збільшенні частоти екстремальних явищ - у 2024 році зафіксовано 45 днів з температурою понад 30°C, що негативно впливає на продуктивність корів.

Стратегічні висновки на основі SWOT-аналізу:

Позитивні значення коефіцієнтів внутрішніх (1,07) та зовнішніх (1,25) факторів, а також загального коефіцієнта привабливості (2,32) свідчать про сприятливі умови для адаптації міжнародних практик резільєнтності до українських умов. Водночас успішність трансферу залежить від ефективного використання сильних сторін для реалізації можливостей та мінімізації впливу загроз.

Пріоритетними стратегіями є: максимізація використання природного потенціалу через залучення міжнародного фінансування для модернізації; розвиток кооперативного руху

для подолання фрагментованості; адаптація європейських стандартів як інструмент доступу до преміальних ринків; створення резерву стійкості до кліматичних та геополітичних шоків через диверсифікацію та технологічні інновації.

Дискусія

Проведене дослідження демонструє, що резільєнтність ринку молочних продуктів України характеризується складною динамікою адаптивних процесів, що поєднують руйнівні та трансформаційні ефекти. Ключові висновки розширюють теоретичне розуміння резільєнтності агропродовольчих систем, підтверджують важливість масштабу та інтеграції для забезпечення адаптивної здатності, вводять концепцію "конфліктної резільєнтності" та мають практичне значення для формування політики сталого розвитку у контексті зростаючої глобальної нестабільності.

Емпірично підтверджена гіпотеза про нелінійний характер адаптації молочних систем до екстремальних шоків суттєво доповнює класичні теоретичні моделі резільєнтності. На відміну від традиційних концепцій поступового відновлення після порушень (Holling, 1973; Walker & Salt, 2006), український досвід демонструє феномен "адаптивної трансформації", коли система не повертається до первісного стану, а еволюціонує в принципово нову конфігурацію з вищими характеристиками ефективності. Промисловий сектор молочного виробництва збільшив обсяги на 8,9% порівняно з довоєнним рівнем, одночасно радикально змінивши структуру галузі – частка підприємств зросла з 27,4% у 2018 році до 35,3% у 2024 році. Це відповідає концепції "panarchy" Холлінга (Holling, 2001), згідно з якою кризи можуть стати каталізаторами переходу на вищий рівень організації.

Результати підтверджують теорію економії від масштабу, демонструючи кратно вищі адаптивні здатності великих інтегрованих підприємств порівняно з дрібними виробниками. Промислові підприємства демонструють продуктивність корів на рівні 6850 кг/рік проти 3200 кг у господарствах населення, позитивну рентабельність 18,5% проти збитковості -7,3%, що кореспондує з висновками Bunchongpru та Maneerattanarungrot (2025) про переваги інтеграції ланцюгів постачання. Водночас отримані результати вступають у суперечність з поширеними в літературі тезами про переваги диверсифікованих дрібнотоварних систем для забезпечення резільєнтності (Darnhofer, 2014). Український досвід свідчить, що в умовах екстремальних шоків критичними стають не диверсифікація та гнучкість, а концентрація ресурсів, доступ до капіталу та можливості забезпечення біологічної безпеки.

Воєнні конфлікти створюють унікальне поєднання прямих фізичних руйнувань, логістичних обмежень, інституційної нестабільності та довгострокової невизначеності. Успішна адаптація в таких умовах потребує здатності забезпечувати критичні функції автономно, що підтверджується необхідністю інвестицій у енергонезалежність в обсязі 220 млн дол.

Порівняння з міжнародними дослідженнями виявляє як спільні закономірності, так і унікальні особливості українського досвіду. Зіставлення з дослідженням Neethirajan (2024) щодо канадських інноваційних стратегій демонструє, що обидва дослідження підтверджують ключову роль технологічних інновацій у підвищенні резільєнтності, проте канадський досвід фокусується на превентивних заходах адаптації до кліматичних змін, тоді як український – на реактивних стратегіях виживання. Порівняння з висновками Bunchongpru та Maneerattanarungrot (2025) показує: їх дослідження демонструє підвищення економічної ефективності на 23%, тоді як український досвід показує різницю в продуктивності між інтегрованими підприємствами та окремими господарствами на рівні 214%, що свідчить про критичну важливість інтеграції в умовах кризи. Результати корелюють з висновками Zarei-Kordshouli et al. (2023) щодо важливості резільєнтності ланцюгів постачання, проте демонструють значно вищі рівні невизначеності: волатільність цін коливалася від 68,5% до 94,6% відносно європейського рівня, тоді як їх модель враховувала лише ±25%.

Дослідження виявляє важливі імплікації для теорії сталого розвитку, зокрема щодо співвідношення між резільєнтністю та сталістю. Традиційна парадигма сталого розвитку передбачає збалансованість економічних, соціальних та екологічних цілей, водночас український досвід демонструє, що в умовах екстремальних викликів може виникати конфлікт між короткостроковою резільєнтністю та довгостроковою сталістю. Концентрація виробництва в великих підприємствах, що виявилася найефективнішою стратегією виживання, суперечить принципам соціальної сталості через негативний вплив на зайнятість у сільських територіях. Можливим рішенням є концепція "адаптивної сталості", що передбачає динамічну балансировку dimensions сталого розвитку залежно від рівня загроз.

Результати мають значні практичні наслідки для формування державної політики та бізнес-стратегій. На рівні державної політики критично важливим є перехід від традиційних підходів підтримки дрібнотоварного виробництва до стимулювання консолідації галузі, оскільки дані переконливо демонструють ефективність лише великих інтегрованих підприємств. Для бізнесу ключовими є диверсифікація ризиків через географічний розподіл активів та переорієнтація експортних стратегій, оскільки небезпечна залежність від ЄС (67,2% експорту) створює системні ризики через квотні обмеження та потенційні втрати понад 20 млн євро щорічно.

Проведене дослідження має кілька важливих обмежень, що визначають напрями подальших наукових пошуків. Базування на агрегованих статистичних даних не дозволяє глибоко проаналізувати мікроекономічні механізми адаптації окремих підприємств, а відносно короткі часові рамки (2018-2024) обмежують оцінку довгострокових ефектів резільєнтності. Фокус на економічних аспектах з недостатньою увагою до соціальних та екологічних dimensions створює потребу комплексних міждисциплінарних досліджень. Майбутні дослідження мають сфокусуватися на мікроекономічному аналізі адаптаційних стратегій через лонгітюдні дослідження окремих підприємств, соціально-екологічних аспектах резільєнтності та порівняльних дослідженнях з іншими конфліктними зонами.

На основі результатів дослідження сформульовано рекомендації щодо розроблення Національної стратегії резільєнтності агропродовольчих систем з механізмами фінансування консолідації галузі, програмами розвитку альтернативної енергетики та системами раннього попередження епізоотичних ризиків. На міжнародному рівні необхідним є перегляд підходів до гуманітарної допомоги з фокусуванням на підтримці інтегрованих структур та розроблення міжнародних стандартів оцінки резільєнтності в умовах конфліктів.

Висновки

Розроблено сценарії розвитку галузі до 2030 року з базовим варіантом досягнення 8,5 млн т виробництва молока при 65 % частці підприємств з ймовірністю реалізації 60%, оптимістичним сценарієм 10,2 млн т при 75 % частці підприємств з ймовірністю 25% та песимістичним варіантом 6,8 млн т при 55 % частці підприємств з ймовірністю 15%, що дозволяє планувати розвиток галузі з урахуванням різних рівнів ризиків та можливостей фінансування.

Практична значимість отриманих результатів полягає у формуванні науково-методичного базису для розроблення державної стратегії розвитку молочної промисловості України в умовах воєнного стану та постконфліктного відновлення, створенні інструментарію кількісної оцінки адаптивної здатності підприємств для корпоративного стратегічного планування та розробленні механізмів адаптації європейських моделей резільєнтності до українських умов з урахуванням специфіки євроінтеграційних процесів та обмежень квотної системи ЄС. Визначено ключові напрями майбутніх досліджень, що включають мікроекономічний аналіз адаптаційних стратегій окремих підприємств через лонгітюдні дослідження, соціально-екологічні аспекти концентрації виробництва та їх вплив на сільські громади, розробку прогностичних моделей резільєнтності з використанням методів

машинного навчання та порівняльні дослідження з країнами, що зазнали воєнних конфліктів, для виявлення універсальних закономірностей адаптації агропродовольчих систем до екстремальних викликів. Результати дослідження підтверджують можливість досягнення високих показників резільєнтності агропродовольчих систем навіть в умовах екстремальних викликів за умови ефективної адаптації міжнародного досвіду, концентрації ресурсів у великих інтегрованих структурах та послідовної державної підтримки трансформаційних процесів, що дозволить забезпечити не лише відновлення українського ринку молочних продуктів до довоєнного рівня, але й досягнення якісно нового рівня ефективності та конкурентоспроможності на світових ринках у контексті реалізації цілей сталого розвитку та європейської інтеграції.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Abbas, S., Hayat, K., Karangwa, E. *et al.* (2013). An Overview of Ultrasound-Assisted Food-Grade Nanoemulsions. *Food Eng Rev* 5, 139–157. https://doi.org/10.1007/s12393-013-9066-3
2. Abbasian, M., Jamili, A. A (2025). Hybrid Machine Learning Approach to Evaluate and Select Agile-Resilient-Sustainable Suppliers Considering Supply Chain 4.0: A Real Case Study. *Process Integr Optim Sustain* **9**, 717–735. https://doi.org/10.1007/s41660-025-00483-1
3. Artukoglu, M.M., & Olgun, A. (2008). Cooperation tendencies and alternative milk marketing channels of dairy producers in Turkey: A case of Menemen. *Agricultural Economics*, *54*(1), 32-37. https://doi.org/10.17221/252-AGRICECON
4. Balan, I. M., & Trasca, T. I. (2025). Reducing Agricultural Land Use Through Plant-Based Diets: A Case Study of Romania. *Nutrients*, *17*(1), 175. https://doi.org/10.3390/nu17010175
5. Béné, C., Oosterveer, P., Lamotte, L., Brouwer, I. D., de Haan, S., Prager, S. D., Talsma, E. F., & Khoury, C. K. (2019). When food systems meet sustainability – Current narratives and implications for actions. *World Development*, 113, 116-130. https://doi.org/10.1016/j.worlddev.2018.08.011
6. Brundtland Commission (1987). Our Common Future: Report of the World Commission on Environment and Development. Oxford: Oxford University Press. URL: https://surl.lu/olqwwu
7. Bunchongpru, C., & Maneerattanarungrot, C. (2025). Influence of Supply Chain Integration on the Sustainable Performance of Dairy Farms in Pak Chong District, Nakhon Ratchasima. *Suranaree Journal of Social Science*, 19(1). https://doi.org/10.55766/sjss277236
8. Can BA & Engindeniz S (2025) The effects on milk marketing of cooperative partnership of dairy farmers: a case study from Türkiye. *Front. Sustain. Food Syst*. 8:1451687. https://doi.org/10.3389/fsufs.2024.1451687
9. Darnhofer, I. (2014). Resilience and why it matters for farm management. *European Review of Agricultural Economics*, 41(3), 461–484. https://doi.org/10.1093/erae/jbu012
10. European Commission. (2020). Farm to Fork strategy: For a fair, healthy and environmentally-friendly food system. *Food, Farming, Fisheries*. URL: https://surl.li/hzkfaz
11. European Commission. (2023). EU agricultural outlook 2023-35: A resilient sector adapts to climate change, sustainability concerns, and shifting consumer demand. Publications Office of the European Union. URL: https://surl.li/elldxn

12. FAO. (2023). The State of Food Security and Nutrition in the World 2023. Rome: Food and Agriculture Organization of the United Nations. URL: https://surl.li/pulhhz
13. FAO. (2024). Building resilient food systems – HLPE-FSN consultation on the scope of the report. URL: https://surl.li/tjllcj
14. Global Dairy Trade. (2025). Trading Events Results. URL: https://www.globaldairytrade.info/
15. Herun, I. V. (2022). *Sanitary and hygienic assessment of quality and safety of cow milk obtained using the latest technologies* [Doctoral dissertation, Sumy National Agrarian University]. https://surl.li/vrsqlh
16. Holland, J. H. (1992). Complex adaptive systems. *Daedalus*, 121(1), 17-30. URL: https://philpapers.org/rec/HOLCAS-4
17. Holling, C. S. (1973). Resilience and stability of ecological systems Annual Review of Ecology, Evolution, and Systematics, 4(1), 1-23. https://doi.org/10.1146/annurev.es.04.110173.000245
18. Holling, C. S. (2001). Understanding the complexity of economic, ecological, and social systems. *Ecosystems*, 4(5), 390-405. https://doi.org/10.1007/s10021-001-0101-5
19. ILO. (2023). World Employment and Social Outlook 2023: The value of essential work. Geneva: International Labour Organization. URL: https://surl.lt/ncvise
20. Infascelli, F., Musco, N., Lotito, D., Pacifico, E., Matuozzo, S., Zicarelli, F., Iommelli, P., Tudisco, R., & Lombardi, P. (2023). The "Noble Method®": A One Health Approach for a Sustainable Improvement in Dairy Farming. *Sustainability*, *15*(21), 15201. https://doi.org/10.3390/su152115201
21. IPCC. (2024). Climate Change 2023: Synthesis Report. Geneva: Intergovernmental Panel on Climate Change. https://doi.org/10.59327/IPCC/AR6-9789291691647
22. Jaeger, S. R., Chheang, S. L., Llobell, F., & Cardello, A. V. (2024). Consumers' Expectations of Liking, Emotional, Conceptual and Sustainability Characteristics of Dairy, Plant-Based and Sustainable Yoghurts. *Journal of Sensory Studies*, 39(6). https://doi.org/10.1111/joss.12955
23. Kumar, R., Hegde, A. S., Sharma, K., Parmar, P., & Srivatsan, V. (2022). Microalgae as a sustainable source of edible proteins and bioactive peptides – Current trends and future prospects. *Food Research International*, 111338. https://doi.org/10.1016/j.foodres.2022.111338
24. Marshall, N. A., Crimp, S., Curnock, M., Greenhill, M., Kuehne, G., Leviston, Z., & Ouzman, J. (2016). Some primary producers are more likely to transform their agricultural practices in response to climate change than others. *Agriculture, Ecosystems & Environment*, 222, 38-47. https://doi.org/10.1016/j.agee.2016.02.004
25. Martínez-Olvera, C., & Mora-Vargas, J. (2019). A Comprehensive Framework for the Analysis of Industry 4.0 Value Domains. *Sustainability*, *11*(10), 2960. https://doi.org/10.3390/su11102960
26. Mosibo, O. K., Ferrentino, G., & Udenigwe, C. C. (2024). Microalgae Proteins as Sustainable Ingredients in Novel Foods: Recent Developments and Challenges. *Foods*, *13*(5), 733. https://doi.org/10.3390/foods13050733
27. Mwirigi, D., Fekete-Farkas, M., & Borbély, C. (2025). From Cow to Climate—Tracing the Path of Dairy Sustainability: Unveiling the Impact on Sustainable Development Goals Through Bibliometric and Literature Analyses. *Animals*, *15*(7), 931. https://doi.org/10.3390/ani15070931
28. Neethirajan, S. (2024). Innovative Strategies for Sustainable Dairy Farming in Canada amidst Climate Change. *Sustainability*, *16*(1), 265. https://doi.org/10.3390/su16010265
29. Ostrom E. (2009). A general framework for analyzing sustainability of social-ecological systems. *Science (New York, N.Y.)*, *325*(5939), 419–422. https://doi.org/10.1126/science.1172133

30. Paiva, C. M. N., Quintino, D. D., Morais, T. B. C. d., Cozadi, E. G., Costa, J. S. d., Leme, P. H. M. V., & Scolforo, J. R. S. (2024). Pathways to Rural Sustainability: Opportunities and Challenges in the Creation of an Agrotechnological District in Ingaí City, Brazil. *Agriculture*, *14*(12), 2185. https://doi.org/10.3390/agriculture14122185
31. Paris Agreement. (2015). United Nations Framework Convention on Climate Change. Paris: United Nations. URL: https://surli.cc/lddyrg
32. Patel, A. S., Brahmbhatt, M. N., Bariya, A. R., Nayak, J. B., & Singh, V. K. (2023). Blockchain technology in food safety and traceability concern to livestock products. *Heliyon*, 9(6), e16526. https://doi.org/10.1016/j.heliyon.2023.e16526
33. Paeizi, A., Makui, A., & Pishvaee, M. S. (2023). A multi-stage stochastic programming approach for an inventory-routing problem considering life cycle. *RAIRO Operations Research*, 57, 2537-2559. https://doi.org/10.1051/ro/2023122
34. Porter, M. E. (1985). *Competitive advantage: Creating and sustaining superior performance*. New York: Free Press.
35. Tendall, D. M., Joerin, J., Kopainsky, B., Edwards, P., Shreck, A., Le, Q. B., Kruetli, P., Grant, M., & Six, J. (2015). Food system resilience: Defining the concept. *Global Food Security*, 6, 17-23. https://doi.org/10.1016/j.gfs.2015.08.001
36. Tița, M. A., Moga, V.-M., Constantinescu, M. A., Bătușaru, C. M., & Tița, O. (2024). Harnessing the Potential of Whey in the Creation of Innovative Food Products: Contributions to the Circular Economy. *Recycling*, *9*(5), 79. https://doi.org/10.3390/recycling9050079
37. UN DESA. (2022). World Population Prospects 2022: Summary of Results. New York: United Nations Department of Economic and Social Affairs. URL: https://surl.li/lckybz
38. UN SDG Framework. (2015). Transforming our world: The 2030 Agenda for Sustainable Development. New York: United Nations. URL: https://sdgs.un.org/2030agenda
39. United Nations General Assembly. (2015, September 25). *Transforming our world: the 2030 Agenda for Sustainable Development* (Resolution A/RES/70/1). United Nations. URL: https://surl.li/rdblax
40. USDA Foreign Agricultural Service. (2024). Dairy: World Markets and Trade. Washington: USDA. https://apps.fas.usda.gov/psdonline/circulars/dairy.pdf
41. Walker, B., Salt, D., & Reid, W. V. (2006). *Resilience thinking: Sustaining ecosystems and people in a changing world*. Island Press. URL: https://surli.cc/yleftz
42. Wang, S., Yang, Y., Yin, H., Zhao, J., Wang, T., Yang, X., Ren, J., & Yin, C. (2025). Towards Digital Transformation of Agriculture for Sustainable Development in China: Experience and Lessons Learned. *Sustainability*, *17*(8), 3756. https://doi.org/10.3390/su17083756
43. Zarei-Kordshouli, F., Paydar, M.M. & Nayeri, S. (2023). Designing a dairy supply chain network considering sustainability and resilience: a multistage decision-making framework. *Clean Techn Environ Policy* 25, 2903–2927. https://doi.org/10.1007/s10098-023-02538-8
44. Асоціація виробників молока України (АВМ). (2025). Промисловий сектор збільшив обсяги надою в січні-квітні 2025 року. URL: https://www.avm-ua.org/
45. Державна служба статистики України. (2024). Статистичний щорічник України. Київ: Держстат України. https://surl.li/wwtqws
46. Ужва, А. М. (2024). Аналітичний моніторинг стану виробництва молока в Україні. *Український журнал прикладної економіки та техніки*, 9(2), 236-239. https://doi.org/10.36887/2415-8453-2024-2-40

References

1. Abbas, S., Hayat, K., Karangwa, E. *et al.* (2013). An Overview of Ultrasound-Assisted Food-Grade Nanoemulsions. *Food Eng Rev* 5, 139–157. https://doi.org/10.1007/s12393-013-9066-3

2. Abbasian, M., Jamili, A. A (2025). Hybrid Machine Learning Approach to Evaluate and Select Agile-Resilient-Sustainable Suppliers Considering Supply Chain 4.0: A Real Case Study. *Process Integr Optim Sustain* 9, 717–735. https://doi.org/10.1007/s41660-025-00483-1
3. Artukoglu, M.M., & Olgun, A. (2008). Cooperation tendencies and alternative milk marketing channels of dairy producers in Turkey: A case of Menemen. *Agricultural Economics*, *54*(1), 32-37. https://doi.org/10.17221/252-AGRICECON
4. Balan, I. M., & Trasca, T. I. (2025). Reducing Agricultural Land Use Through Plant-Based Diets: A Case Study of Romania. *Nutrients*, *17*(1), 175. https://doi.org/10.3390/nu17010175
5. Béné, C., Oosterveer, P., Lamotte, L., Brouwer, I. D., de Haan, S., Prager, S. D., Talsma, E. F., & Khoury, C. K. (2019). When food systems meet sustainability – Current narratives and implications for actions. *World Development*, 113, 116-130. https://doi.org/10.1016/j.worlddev.2018.08.011
6. Brundtland Commission (1987). Our Common Future: Report of the World Commission on Environment and Development. Oxford: Oxford University Press. Available from : https://surl.lu/olqwwu
7. Bunchongpru, C., & Maneerattanarungrot, C. (2025). Influence of Supply Chain Integration on the Sustainable Performance of Dairy Farms in Pak Chong District, Nakhon Ratchasima. *Suranaree Journal of Social Science*, 19(1). https://doi.org/10.55766/sjss277236
8. Can BA & Engindeniz S (2025) The effects on milk marketing of cooperative partnership of dairy farmers: a case study from Türkiye. *Front. Sustain. Food Syst*. 8:1451687. https://doi.org/10.3389/fsufs.2024.1451687
9. Darnhofer, I. (2014). Resilience and why it matters for farm management. *European Review of Agricultural Economics*, 41(3), 461–484. https://doi.org/10.1093/erae/jbu012
10. European Commission. (2020). Farm to Fork strategy: For a fair, healthy and environmentally-friendly food system. *Food, Farming, Fisheries*. Available from : https://surl.li/hzkfaz
11. European Commission. (2023). EU agricultural outlook 2023-35: A resilient sector adapts to climate change, sustainability concerns, and shifting consumer demand. Publications Office of the European Union. Available from : https://surl.li/elldxn
12. FAO. (2023). The State of Food Security and Nutrition in the World 2023. Rome: Food and Agriculture Organization of the United Nations. URL: https://surl.li/pulhhz
13. FAO. (2024). Building resilient food systems – HLPE-FSN consultation on the scope of the report. Available from : https://surl.li/tjllcj
14. Global Dairy Trade. (2025). Trading Events Results. URL: https://www.globaldairytrade.info/
15. Herun, I. V. (2022). *Sanitary and hygienic assessment of quality and safety of cow milk obtained using the latest technologies* [Doctoral dissertation, Sumy National Agrarian University]. Available from : https://surl.li/vrsqlh
16. Holland, J. H. (1992). Complex adaptive systems. *Daedalus*, 121(1), 17-30. Available from : https://philpapers.org/rec/HOLCAS-4
17. Holling, C. S. (1973). Resilience and stability of ecological systems Annual Review of Ecology, Evolution, and Systematics, 4(1), 1-23. https://doi.org/10.1146/annurev.es.04.110173.000245
18. Holling, C. S. (2001). Understanding the complexity of economic, ecological, and social systems. *Ecosystems*, 4(5), 390-405. https://doi.org/10.1007/s10021-001-0101-5
19. ILO. (2023). World Employment and Social Outlook 2023: The value of essential work. Geneva: International Labour Organization. Available from : https://surl.lt/ncvise
20. Infascelli, F., Musco, N., Lotito, D., Pacifico, E., Matuozzo, S., Zicarelli, F., Iommelli, P., Tudisco, R., & Lombardi, P. (2023). The "Noble Method®": A One Health Approach for a Sustainable Improvement in Dairy Farming. *Sustainability*, *15*(21), 15201. https://doi.org/10.3390/su152115201

21. IPCC. (2024). Climate Change 2023: Synthesis Report. Geneva: Intergovernmental Panel on Climate Change. https://doi.org/10.59327/IPCC/AR6-9789291691647
22. Jaeger, S. R., Chheang, S. L., Llobell, F., & Cardello, A. V. (2024). Consumers' Expectations of Liking, Emotional, Conceptual and Sustainability Characteristics of Dairy, Plant-Based and Sustainable Yoghurts. *Journal of Sensory Studies*, 39(6). https://doi.org/10.1111/joss.12955
23. Kumar, R., Hegde, A. S., Sharma, K., Parmar, P., & Srivatsan, V. (2022). Microalgae as a sustainable source of edible proteins and bioactive peptides – Current trends and future prospects. *Food Research International*, 111338. https://doi.org/10.1016/j.foodres.2022.111338
24. Marshall, N. A., Crimp, S., Curnock, M., Greenhill, M., Kuehne, G., Leviston, Z., & Ouzman, J. (2016). Some primary producers are more likely to transform their agricultural practices in response to climate change than others. *Agriculture, Ecosystems & Environment*, 222, 38-47. https://doi.org/10.1016/j.agee.2016.02.004
25. Martínez-Olvera, C., & Mora-Vargas, J. (2019). A Comprehensive Framework for the Analysis of Industry 4.0 Value Domains. *Sustainability*, *11*(10), 2960. https://doi.org/10.3390/su11102960
26. Mosibo, O. K., Ferrentino, G., & Udenigwe, C. C. (2024). Microalgae Proteins as Sustainable Ingredients in Novel Foods: Recent Developments and Challenges. *Foods*, *13*(5), 733. https://doi.org/10.3390/foods13050733
27. Mwirigi, D., Fekete-Farkas, M., & Borbély, C. (2025). From Cow to Climate—Tracing the Path of Dairy Sustainability: Unveiling the Impact on Sustainable Development Goals Through Bibliometric and Literature Analyses. *Animals*, *15*(7), 931. https://doi.org/10.3390/ani15070931
28. Neethirajan, S. (2024). Innovative Strategies for Sustainable Dairy Farming in Canada amidst Climate Change. *Sustainability*, *16*(1), 265. https://doi.org/10.3390/su16010265
29. Ostrom E. (2009). A general framework for analyzing sustainability of social-ecological systems. *Science (New York, N.Y.)*, *325*(5939), 419–422. https://doi.org/10.1126/science.1172133
30. Paiva, C. M. N., Quintino, D. D., Morais, T. B. C. d., Cozadi, E. G., Costa, J. S. d., Leme, P. H. M. V., & Scolforo, J. R. S. (2024). Pathways to Rural Sustainability: Opportunities and Challenges in the Creation of an Agrotechnological District in Ingaí City, Brazil. *Agriculture*, *14*(12), 2185. https://doi.org/10.3390/agriculture14122185
31. Paris Agreement. (2015). United Nations Framework Convention on Climate Change. Paris: United Nations. Available from : https://surli.cc/lddyrg
32. Patel, A. S., Brahmbhatt, M. N., Bariya, A. R., Nayak, J. B., & Singh, V. K. (2023). Blockchain technology in food safety and traceability concern to livestock products. *Heliyon*, 9(6), e16526. https://doi.org/10.1016/j.heliyon.2023.e16526
33. Paeizi, A., Makui, A., & Pishvaee, M. S. (2023). A multi-stage stochastic programming approach for an inventory-routing problem considering life cycle. *RAIRO Operations Research*, 57, 2537-2559. https://doi.org/10.1051/ro/2023122
34. Porter, M. E. (1985). *Competitive advantage: Creating and sustaining superior performance*. New York: Free Press.
35. Tendall, D. M., Joerin, J., Kopainsky, B., Edwards, P., Shreck, A., Le, Q. B., Kruetli, P., Grant, M., & Six, J. (2015). Food system resilience: Defining the concept. *Global Food Security*, 6, 17-23. https://doi.org/10.1016/j.gfs.2015.08.001
36. Tița, M. A., Moga, V.-M., Constantinescu, M. A., Bătușaru, C. M., & Tița, O. (2024). Harnessing the Potential of Whey in the Creation of Innovative Food Products: Contributions to the Circular Economy. *Recycling*, *9*(5), 79. https://doi.org/10.3390/recycling9050079

37. UN DESA. (2022). World Population Prospects 2022: Summary of Results. New York: United Nations Department of Economic and Social Affairs. Available from : https://surl.li/lckybz
38. UN SDG Framework. (2015). Transforming our world: The 2030 Agenda for Sustainable Development. New York: United Nations. Available from : https://sdgs.un.org/2030agenda
39. United Nations General Assembly. (2015, September 25). *Transforming our world: the 2030 Agenda for Sustainable Development* (Resolution A/RES/70/1). United Nations. URL: https://surl.li/rdblax
40. USDA Foreign Agricultural Service. (2024). Dairy: World Markets and Trade. Washington: USDA. https://apps.fas.usda.gov/psdonline/circulars/dairy.pdf
41. Walker, B., Salt, D., & Reid, W. V. (2006). *Resilience thinking: Sustaining ecosystems and people in a changing world*. Island Press. Available from : https://surli.cc/yleftz
42. Wang, S., Yang, Y., Yin, H., Zhao, J., Wang, T., Yang, X., Ren, J., & Yin, C. (2025). Towards Digital Transformation of Agriculture for Sustainable Development in China: Experience and Lessons Learned. *Sustainability*, *17*(8), 3756. https://doi.org/10.3390/su17083756
43. Zarei-Kordshouli, F., Paydar, M.M. & Nayeri, S. (2023). Designing a dairy supply chain network considering sustainability and resilience: a multistage decision-making framework. *Clean Techn Environ Policy* 25, 2903–2927. https://doi.org/10.1007/s10098-023-02538-8
44. Association of Milk Producers of Ukraine (AVM). (2025). The industrial sector increased milk yield in January-April 2025. Available from : https://www.avm-ua.org/
45. State Statistics Service of Ukraine. (2024). Statistical Yearbook of Ukraine. Kyiv: State Statistics Service of Ukraine. Available from : https://surl.li/wwtqws
46. Uzhva A. Analytical monitoring of milk production in Ukraine. Ukrainian Journal of Applied Economics and Technology. 2024. Volume 9. № 2, pp. 236–239 https://doi.org/10.36887/2415-8453-2024-2-40

Теоретична платформа інтеграції оборонно-промислового комплексу в загальнонаціональну економічну систему

Theoretical Platform for Integrating the Defense-Industrial Complex into the National Economic System

Володимир Коваль
кандидат військових наук, старший науковий співробітник, e-mail: vladimerkoval69@gmail.com, ORCID: 0000-0002-6209-6779

Міністерство оборони України, м. Київ, Україна

Volodymyr Koval
Candidate of Military Sciences, Senior Researcher, e-mail: vladimerkoval69@gmail.com, ORCID: 0000-0002-6209-6779

Ministry of Defense of Ukraine, Kyiv, Ukraine

Received: April 21, 2025 | Revised: April 28, 2025 | Accepted: April 30, 2025

DOI: https://doi.org/10.33445/sds.2025.15.2.29

Мета роботи. Обґрунтування теоретичної платформи інтеграції оборонно-промислового комплексу в загальнонаціональну економічну систему на основі впровадження інтелектуальних технологій управління, зокрема цифрових двійників та динамічних когнітивних сценаріїв.

Методи дослідження. У роботі застосовано методи параметричної теорії систем, логіко-лінгвістичне моделювання, фреймовий підхід для представлення знань, а також системно-ситуаційний аналіз для класифікації рівнів управління складними об'єктами національної економіки.

Результати дослідження. Сформовано концепцію «цифрового двійника» підприємства ОПК як інструменту випереджального реагування на стратегічні виклики; розроблено трирівневу структуру ситуаційного управління (стратегічний, оперативний, виконавчий); запропоновано використання фреймових моделей для структурування ресурсних потоків. Визначено роль динамічного когнітивного сценарію як інструменту зворотного логічного виводу для моделювання альтернативних шляхів досягнення цілей в умовах ресурсних обмежень.

Теоретична цінність дослідження. Робота поглиблює параметричну теорію систем через розмежування атрибутивних та реляційних концептів у контексті ОПК. Розкрито наукову новизну застосування логіко-лінгвістичних моделей (продукційних, фреймових, семантичних) для відтворення складності взаємодії суб'єкта та об'єкта управління в оборонному секторі.

Практична цінність дослідження. Запропоновані моделі та інструментарій (ДКС, ДСС, МАУ) дозволяють автоматизувати процеси розпізнавання проблемних ситуацій на підприємствах ОПК, оптимізувати мережеві графіки виробництва та забезпечити синхронізацію галузевих ресурсних комплексів у реальному часі, що критично важливо для зміцнення національної стійкості.

Цінність дослідження. Уперше запропоновано інтегрований підхід до управління ОПК через механізм адаптивного управління, який поєднує методи математичної лінгвістики та нечіткої логіки для створення "містка" між теоретичними параметрами економічної системи та практичною діяльністю органів державного управління.

Обмеження дослідження. Обмеження пов'язані зі складністю алгоритмізації зворотного логічного виводу в умовах високої динамічності законодавства та необхідністю високої якості вхідних даних (Big Data) для коректного функціонування цифрових двійників галузей.

Тип статті: Теоретико-методологічний / Дослідницький.

Purpose. To substantiate the theoretical platform for integrating the defense-industrial complex (DIC) into the national economic system through the implementation of intelligent management technologies, specifically digital twins and dynamic cognitive scenarios.

Method. The study employs methods of parametric systems theory, logical-linguistic modeling, a frame-based approach for knowledge representation, and systemic-situational analysis to classify management levels of complex national economy objects.

Findings. The concept of a "digital twin" of a DIC enterprise is formulated as a tool for proactive response to strategic challenges; a three-level structure of situational management (strategic, operational, executive) is developed; the use of frame models for structuring resource flows is proposed. The role of the Dynamic Cognitive Scenario as a backward logical inference tool for modeling alternative paths to goal achievement under resource constraints is identified.

Theoretical implications. The work deepens the parametric systems theory by distinguishing between attributive and relational concepts within the DIC context. The scientific novelty of applying logical-linguistic models (production, frame, semantic) to replicate the complexity of subject-object interaction in the defense sector is revealed.

Practical implications. The proposed models and tools (DCS, DSN, AMM) enable the automation of problem situation recognition at DIC enterprises, optimization of production schedules, and synchronization of industry resource complexes in real-time, which is critical for strengthening national resilience.

Originality. For the first time, an integrated approach to DIC management is proposed through an adaptive management mechanism that combines methods of mathematical linguistics and fuzzy logic to create a "bridge" between theoretical economic system parameters and the practical activities of state management bodies.

Research limitations. Limitations relate to the complexity of algorithmizing backward logical inference under highly dynamic legislation and the requirement for high-quality input data (Big Data) for the correct functioning of industrial digital twins.

Paper type. Theoretical-methodological / Research.

Ключові слова: оборонно-промисловий комплекс, національна економіка, цифровий двійник, логіко-лінгвістичне моделювання, динамічний когнітивний сценарій, адаптивне управління, фреймовий підхід.

Key words: Defense-Industrial Complex, National Economy, Digital Twin, Logical-Linguistic Modeling, Dynamic Cognitive Scenario, Adaptive Management, Frame-Based Approach.

Вступ

Сучасна геополітична нестабільність та воєнні виклики зумовлюють необхідність докорінного перегляду підходів до функціонування оборонно-промислового комплексу (ОПК). Оборонно-промисловий комплекс перестав бути ізольованим сектором і перетворився на ключовий драйвер національної економіки, що потребує глибокої інтеграції в загальногосподарську структуру. Традиційні методи управління, що базуються на статичних планах, виявляються неефективними в умовах високої невизначеності.

Цифрова трансформація та впровадження інтелектуальних систем створюють передумови для переходу до адаптивного управління. Центральним елементом цієї парадигми стає концепція "цифрового двійника" та логіко-лінгвістичного моделювання, які дозволяють не лише моніторити поточний стан галузі, а й здійснювати антиципацію (випереджальне реагування) на загрози. Актуальність дослідження посилюється потребою України у створенні стійкої, гнучкої та технологічно незалежної системи ресурсного забезпечення сектору безпеки.

Теоретичні основи дослідження

Теоретичний підґрунтя роботи базується на синтезі трьох наукових напрямів: загальна параметрична теорія систем, яка дозволяє розглядати ОПК як складний об'єкт із чітко визначеними атрибутивними (властивості) та реляційними (відносини) концептами; школа адаптивного управління, що впроваджує механізми зворотного зв'язку та самоорганізації економічних систем; логіко-лінгвістичне моделювання (ЛЛМ), засноване на працях Лотфі Заде та Д. Поспєлова, яке використовує семіотичні моделі та нечітку логіку для формалізації знань, що не піддаються класичному математичному опису.

Особлива увага приділяється концепції "Великої стратегії" (Grand Strategy), де економічне процвітання та оборонна спроможність розглядаються як єдиний гомеокінетичний механізм.

Постановка проблеми

Попри значну кількість розробок у сфері стратегічного планування, залишається низка невирішених проблем:

брак алгоритмізації: існуючі механізми адаптивного управління часто залишаються на рівні загальних концепцій без інструментів практичної реалізації в реальному часі;

інформаційний розрив: відсутність наскрізних технологій, які б поєднували рівень прийняття державних рішень із безпосереднім виконавчим рівнем (підприємствами ОПК);

ризикозахищеність: недостатня розробка методів моделювання "гнучких" сценаріїв, які б дозволяли миттєво перебудовувати логістичні та виробничі ланцюжки у разі блокування ресурсних каналів.

Таким чином, виникає необхідність розробки динамічного когнітивного сценарію (ДКС) як інструменту інтеграції ОПК у національну економіку.

Методологія дослідження

Для досягнення мети дослідження використано комплексний методологічний інструментарій: системно-параметричний аналіз: для дефініції системних параметрів об'єкта управління та виявлення стійких залежностей між ними; фреймовий підхід: для структурування знань про ресурси ОПК (метали, енергія, праця) у вигляді одиниць представлення знань зі специфічними слотами; логіко-лінгвістичне моделювання: створення дискретно-ситуаційних мереж (ДСС), що дозволяють описувати переходи системи з одного стану в інший.

Застосована методологія дозволяє розглядати суб'єкт і об'єкт управління у нерозривному взаємозв'язку, забезпечуючи високу якість прийняття рішень через семантичну інтеграцію функцій планування та контролю.

Результати

Сучасний етап розвитку національної економіки вимагає використання аналогії між бізнес-системою та ІТ-системою, що веде до концепції цифрового двійника підприємства ОПК. Структура такої системи відображає методологію управління, склад елементів та їхні взаємозв'язки. В умовах цифровізації цифровий двійник стає основою для наскрізних технологій управління, які являють собою програмні комплекси на базі інтелектуальних рішень. Вони дозволяють здійснювати антиципацію (випереджальне реагування) та розв'язання стратегічних проблемних ситуацій під час реалізації ключових метафункцій: планування, організації, координації та стратегічного контролю в структурі національної економіки [1].

Розвиваючи теорію системного аналізу, вітчизняні наукові школи розглядають вивчення системних параметрів як ключовий етап побудови моделей управління. Системні властивості (характерні для об'єкта) та системні відносини (що виникають у суб'єкта) формують підґрунтя для когнітивного аналізу, оцінки та прогнозування наслідків управлінських впливів.

У параметричній теорії виокремлюють два типи концептів, що описують стан національної економіки:

- Атрибутивний концепт — це визначена властивість (наприклад, технічна характеристика ресурсу або виробнича потужність), якій має відповідати певне відношення в системі. На етапі ідентифікації об'єкта це відношення часто є невизначеним.
- Реляційний концепт — відповідає визначеним відносинам у суб'єкті управління, яким задовольняє певна (спочатку неочевидна) властивість. Це фактично «цифровий двійник» у свідомості ОПР або в інтелектуальній інформаційній системі, що формалізує діяльність людини (включаючи як цілеспрямовані дії, так і випадкові чинники).

Загальна параметрична теорія передбачає дослідження системи у три етапи:

1. Опис об'єкта через поєднання реляційних концептів та атрибутивних структур (або навпаки).
2. Дефініція системних параметрів (специфічних властивостей та відносин) в об'єкті управління.
3. Виявлення стійких залежностей між параметрами для формалізації загальносистемних закономірностей (універсальності, подвійності, додатковості).

Такий підхід використовує логіко-лінгвістичне моделювання як основний інструментарій для опису формалізованих концептів, що дозволяє розглядати суб'єкт і об'єкт управління у нерозривному взаємозв'язку.

Для наочного представлення місця ситуаційного управління в структурі ОПК розроблено табл. 1.

Сучасна кібернетична концепція управління великими системами в межах ОПК базується на спеціально розроблених мовах ситуаційного управління. Це дозволяє створювати конструкти знань, де кожна зміна у зовнішньому середовищі або всередині підприємства автоматично веде до перерахунку траєкторії досягнення стратегічних цілей. Таким чином, ситуаційне моделювання стає "містком" між теоретичними параметрами системи та реальною практикою управління національною економікою в умовах невизначеності.

Таблиця 1 – Рівні ситуаційного управління складним об’єктом національної економіки (ОПК)

Рівень системи	Тип моделі та інструментарій	Функціональне призначення
Рівень прийняття стратегічних рішень (Суб'єкт)	Семіотична модель, Логіко-лінгвістичні правила	Розпізнавання проблемних ситуацій, формування сценаріїв розвитку, адаптація до стратегічних загроз.
Рівень оперативного управління (Інтерфейс)	Ситуаційна модель, Семантичні мережі	Класифікація поточного стану об’єкта, вибір типових рішень, координація ресурсних потоків.
Виконавчий рівень (Об'єкт)	Параметрична модель, Технічні АСУ	Безпосереднє виконання виробничих функцій, контроль параметрів металів, енергії та праці.
Зовнішнє середовище	Моделі прогнозування зовнішнього світу	Моніторинг ринків, безпекових викликів та технологічного прогресу.

Джерело: складено автором на основі [2]

Для формалізації знань у системах управління національною економікою та ОПК використовується фреймовий підхід, який дозволяє структурувати інформацію про події та явища (табл. 2).

Таблиця 2 – Структурна схема фрейму як одиниці представлення знань (за шаблоном фрейма)

Елемент фрейму	Зміст та характеристика (адаптовано для ресурсів ОПК)
Ім'я фрейму	Найменування об’єкта, процесу або явища (наприклад, “Виробнича потужність підприємства”)
Слот 1 (Ім'я / Значення)	Тип ресурсу / Метал, енергія, комплектуючі тощо.
Слот 2 (Ім'я / Значення)	Часовий параметр / Термін постачання, цикл виробництва.
Слот 3 (Ім'я / Значення)	Обмеження / Граничні обсяги бюджетного фінансування.
Слот N (Ім'я / Значення)	Результативність / Відповідність державним стандартам та показникам безпеки.

Джерело: розроблено автором на основі [3]

Сучасна школа адаптивного управління [4] значно розширила інструментарій підтримки рішень, впровадивши:

- концептуальні каркаси моделей складних економічних систем;
- семантичну інтеграцію метафункцій управління (планування, координація);
- логіко-лінгвістичні моделі у вигляді дискретно-ситуаційних мереж (наприклад, система “Керівник”);
- поняття когнітивних цільових нормативів, що застосовуються для забезпечення ризикозахищеності стратегічного планування.

Отже, інтеграція ОПК у національну економіку вимагає переходу до систем, які здатні автоматично розпізнавати класи проблемних ситуацій та пропонувати альтернативні мережеві графіки досягнення стратегічних цілей з урахуванням обмежень реального часу та ресурсів.

Управління знаннями в системі ресурсного забезпечення сектору безпеки та оборони доцільно здійснювати у фреймовому представленні. У теорії адаптивного управління під фреймами розуміють необхідні та достатні сукупності стандартних одиниць знань (СОЗ) для розпізнавання та розв’язання проблемних ситуацій на галузевому рівні. Слотами у цій

структурі виступають дескриптивні функції управління: цілепокладання, облік, аналіз, прогноз та регулюючий вплив.

Основне завдання функціонування складної системи ОПК полягає у збереженні гомеокінетичної рівноваги. Це означає, що всі галузеві ресурсні комплекси повинні бути синхронізовані за обсягами, потужністю та інтенсивністю споживання й випуску продукції у просторі та часі. Суб'єкт управління (державні інституції) має забезпечувати адекватну реакцію на виникнення стратегічних ризиків, що загрожують цілісності та безпеці національної економіки.

Для реалізації адаптивного управління в оборонному секторі використовується логіко-лінгвістичне моделювання та "механізм адаптивного управління" (МАУ), що спирається на зворотний логічний вивід. Проте брак алгоритмізації цього механізму в існуючих теоретичних розробках ускладнює його практичне застосування в ОПК.

Одним із ключових елементів наукової новизни даної роботи є методичне забезпечення розробки динамічного когнітивного сценарію (ДКС).

ДКС — це дослідницький конструкт, створений на основі інтелектуальних технологій, що здійснює зворотний логічний вивід для встановлення зв'язків між елементами знань у системі стратегічного планування.

ДКС дозволяє моделювати не лише поточні виробничі процеси, а й альтернативні шляхи досягнення стратегічних цілей у разі блокування певних ресурсних каналів або зміни воєнно-політичної обстановки.

Логіко-лінгвістичне моделювання синтезує методи математичної лінгвістики, теорії ігор та нечіткої логіки для представлення складних систем. Воно базується на чотирьох китах: тезаурусі, граматиці, семантиці та прагматиці [5].

Класифікація логіко-лінгвістичних моделей в економіці включає:

1. Продукційні моделі (правила "ЯКЩО... ТО...").
2. Фреймові моделі (структуровані одиниці знань).
3. Семантичні мережі (зв'язки між поняттями галузі).
4. Онтології та терміносистеми (єдина мова взаємодії суб'єктів ОПК).

Застосування ЛЛМ дозволяє відійти від спрощених "іграшкових" математичних моделей до відтворення справжньої складності технологічних, часових та людських компонентів оборонного сектору. Фундаментальні праці Лотфі Заде щодо нечітких множин у поєднанні з сучасними інтелектуальними методами обробки великих даних (Big Data) створюють підґрунтя для цифрових двійників цілих галузей промисловості, що є критично важливим для забезпечення національної стійкості України.

Підприємства ОПК та відповідні галузі ресурсного забезпечення оборони є складними економічними системами, що функціонують у середовищі динамічного законодавства та жорстких міжнародних санкцій. Це змушує національну економіку еволюціонувати, виявляючи властивості самоорганізації та адаптивності.

Для структурування логіко-лінгвістичного моделювання (ЛЛМ) та представлення процесу формування нових можливостей щодо динамічного моделювання сценаріїв функціонування галузі доцільно використовувати інтегрований підхід (табл. 3).

Зазначені аспекти ЛЛМ володіють науковою новизною, оскільки розкривають потенціал динамічного когнітивного сценарію як інструменту стратегічного планування. На відміну від статичних моделей, ДКС дозволяє здійснювати моделювання потреб та можливостей на вході та виході елементарних об'єктів у реальному часі.

ЛЛМ забезпечує принцип "непростої складності", де кожна ситуація моделюється з урахуванням контексту. В ОПК це виявляється в:

- Інтеграції в інформаційні системи: наприклад, прозорість через цифрові казначейські рахунки та системи оборонних закупівель.

Таблиця 3 – Компоненти логіко-лінгвістичного моделювання та динамічного представлення сценаріїв в ОПК (за Рисунком 8)

Абревіатура	Найменування компонента	Роль у системі ресурсного забезпечення
ДКС	Динамічний когнітивний сценарій	Новий інструмент планування: дослідницький конструкт для зворотного логічного виводу.
ДСС	Дискретно-ситуаційна мережа	Графічне представлення взаємодії проблемних ситуацій та шляхів їх подолання.
ДЦС / ДЦО	Дерево цілей суб'єкта / об'єкта	Ієрархічна структура стратегічних цілей галузі та конкретних виробничих завдань.
МС / МО	Модель суб’єкта / об’єкта	Формалізоване представлення органів управління та виробничої бази.
АСГ_С / АСГ_О	Альтернативні мережеві графіки	Варіативні плани дій для суб'єкта та об'єкта відповідно до мінливих умов.

Джерело: розроблено автором

- Підвищенні якості: зміна вимог стандартизації та сертифікації відповідно до стандартів НАТО.
- Трансформації логістики: перебудова ланцюгів постачання для відновлення ресурсного забезпечення в умовах санкцій.

Принципи системного підходу, закладені в національних стандартах (аналогах ГОСТ РВ), де роботи спочатку випробовуються окремо, а потім у складі системи, ідеально корелюють із логікою ЛЛМ. Це дозволяє зробити висновок, що використання семантичних моделей в інформаційно-аналітичному забезпеченні ОПК:

1. Підготує інфраструктуру (цифрові двійники) для вербалізації та обґрунтування управлінських рішень.
2. Забезпечить обробку Big Data для формалізації відносин із замовниками та контролюючими органами.
3. Створить умови для взаємодії із ситуаційними центрами для упередження стратегічних загроз.

Для побудови семантичної моделі предметної області для ресурсного забезпечення ОПК на основі ЛЛМ необхідно визначити її межі, структуру та зв’язки через семантичне моделювання. Автор спирається на концептуальний каркас соціально-економічної системи, адаптований під потреби безпекового сектору (табл. 4).

Таблиця 4 – Елементи семантичної моделі предметної області ОПК

Категорія об’єктів	Елементарні об’єкти (вузли моделі)	Зміст та причинно-наслідкові зв’язки
Зовнішні регулятори	ГР, К	Державне регулювання та контролюючі органи (вплив на правове поле).
Контрагенти	ПР, З	Постачальники ресурсів та Замовники (ресурсні та цільові потоки).
Ресурсна база	Ф, ОФ, М, Т, НМА	Фінанси, основні фонди, матеріали, праця, інтелектуальна власність.
Природне середовище	П	Екологічні обмеження та сировинний потенціал.
Інструменти планування	ДЦО, ДЦС, АСГ, ДСС	Механізми узгодження цілей та формування адаптивних графіків.

Джерело: доопрацьовано автором на основі [6]

Науковою новизною доопрацьованої семантичної моделі є виокремлення сукупності специфічних елементарних об’єктів з атрибутивними (властивості) та реляційними (відносини) параметрами. Це дозволило деталізувати аналіз мікросередовища підприємства ОПК, визначивши рівні корисності кожного ресурсу для подальшої цифровізації стратегічного планування. Такий підхід створює фундамент для інвестиційного проєктування та впровадження інтелектуальних систем управління, що будуть розглянуті у наступних розділах.

Для побудови моделі предметної області необхідно визначити та охарактеризувати всі досліджувані елементарні об’єкти, а також відносини між ними. Візуалізація такої моделі здійснюється у вигляді графа, де вершини — це елементарні об’єкти, а дуги описують взаємозв’язки та потоки між ними.

Об’єктом, для якого будується предметна область, є підприємство ОПК (або сукупність підприємств галузі), що здійснює науково-дослідні та дослідно-конструкторські роботи (НДДКР), виробництво засобів і комплексів автоматизованого зв’язку, а також повний цикл сервісних та ремонтних робіт для потреб національної безпеки. Участь у державному оборонному замовленні (ДОЗ), з одного боку, забезпечує стабільне завантаження потужностей на середньострокову перспективу (1–3 роки), а з іншого — накладає жорсткі обмеження, визначені чинним законодавством України.

Визначимо основні елементарні об’єкти, що формують семантичний каркас моделі:

1. Модель об’єкта — сукупність елементарних виробничих ланок (“нульовий” ярус управління), що беруть участь у створенні оборонної продукції, та спрямованих потоків ресурсів між ними.

2. Модель суб’єкта — сукупність центрів прийняття рішень, пов’язаних ієрархічними відносинами підпорядкування та координації.

3. Дерево цілей суб’єкта — стратегічні цілі державного управління, формалізовані у вигляді вершин графа, де дуги визначають рівні їх вкладеності та пріоритетності.

4. Дерево цілей об’єкта — цілі виробничого комплексу (підприємства), спрямовані на реалізацію тактичних завдань у межах стратегії розвитку.

5. Альтернативний мережевий графік — когнітивна динамічна модель процесу досягнення цілей. Вона використовує фреймове представлення знань (стандартні одиниці знань про ситуації) та цільове динамічне нормування для аналізу наслідків стратегічних рішень.

6. Дискретно-ситуаційна мережа — мережевий граф, де вершини характеризують проблемні ситуації в національній економіці, а дуги — причинно-наслідкові зв’язки між ними.

7. Державне регулювання — сукупність законодавчої бази (зокрема законів про оборонні закупівлі) та обсягів бюджетних асигнувань, що виділяються на фінансування оборонних витрат.

Важливим аспектом моделі є взаємодія з постачальниками та замовниками, що формує ресурсний контур управління національною економікою (табл. 5).

Контролюючі органи та нагляд

У системі стратегічного планування особливе місце займають органи, що здійснюють нагляд за дотриманням законодавства в ОПК:

- Антимонопольний комітет України (АМКУ) — контроль за недопущенням зловживань монопольним становищем.
- Органи прокуратури та ДБР — нагляд за законністю виконання оборонних контрактів.
- Міністерство з питань стратегічних галузей промисловості — регулювання ціноутворення та ліцензування діяльності.
- Служба безпеки України — контроль за режимом секретності та боротьба з корупцією.

Військові представництва (ВП МОУ) — безпосередній контроль якості та обґрунтованості цін на етапі виробництва та приймання озброєння та військової техніки.

Таблиця 5 – Класифікація постачальників ресурсів в інтересах ОПК

Тип постачальника	Специфіка ресурсів / послуг	Роль у забезпеченні стійкості
Матеріальних ресурсів	Енергоносії (вода, газ, електроенергія), метали, комплектуючі вироби.	Забезпечення безперервності виробничого циклу.
Фінансових ресурсів	Держава (бюджет), банки, інвестиційні фонди.	Фінансування НДДКР та модернізації фондів.
Трудових ресурсів	Профільні заклади вищої освіти (ЗВО).	Підготовка висококваліфікованих кадрів під специфічні потреби ОПК.
Інтелектуальних послуг	Проєктні та конструкторські бюро.	Розробка конструкторської документації та інноваційних рішень.
Виробничих послуг	Субпідрядники та спеціалізовані заводи.	Виконання окремих технологічних операцій (аутсорсинг).

Сукупність факторів державного регулювання, постачальників, замовників та контролюючих органів формує зовнішнє середовище галузі. При цьому знання про об’єкт дослідження, за умови необхідності, можуть бути деталізовані та розширені через уточнення внутрішніх ресурсних комплексів.

Таблиця 6 – Ключові групи замовників (З) продукції та послуг ОПК

Група замовників	Характер взаємодії	Об’єкт постачання
Суднобудівні та ремонтні заводи	Формують основну контрактну базу.	Засоби зв'язку, пусконалагоджувальні роботи.
Проєктно-конструкторські бюро	Визначають технічні вимоги до обладнання.	Проєктна документація, зразки для випробувань.
Підприємства радіоелектроніки	Кооперація в межах систем вищого рівня.	Модулі зв’язку, мікроелектроніка.
Міністерство оборони України	Державний замовник №1.	Озброєння та військова техніка, НДДКР.

Внутрішні ресурсні комплекси в системі ОПК

Для забезпечення стратегічної стійкості галузевої економіки виокремлюються наступні ресурсні комплекси, що визначають можливості підприємств:

1. Ресурсний комплекс “Фінанси” — форма концентрації грошових коштів (бюджетних асигнувань, власних доходів), що підлягають розподілу для забезпечення потреб оборонного циклу.
2. Ресурсний комплекс “Основні фонди” — сукупність засобів праці (виробничих ліній, випробувальних стендів), необхідних для багаторазового забезпечення потреб виробничого процесу.
3. Ресурсний комплекс “Матеріали” — форма концентрації палива, енергії, сировини, напівфабрикатів та електронної компонентної бази (ЕКБ), необхідних для випуску високотехнологічної продукції.
4. Ресурсний комплекс “Праця” — сукупність робочої сили з необхідними професійними характеристиками та допусками до роботи зі специфічною технікою.
5. Ресурсний комплекс “Нематеріальні активи” — форма концентрації технологій, патентів, ліцензій та секретів виробництва (know-how), що контролюються галуззю та забезпечують конкурентні переваги.

Сукупність цих комплексів визначає стратегічний потенціал національної економіки в оборонній сфері та надає системі властивість емерджентності — коли спільний ефект від взаємодії ресурсів перевищує суму їх окремих можливостей.

На основі проведеного аналізу логіко-лінгвістичного моделювання та теорії адаптивного управління, сформулюємо уточнений термінологічний апарат, адаптований до галузевого рівня:

- Стратегія — система правил досягнення цілей ресурсного забезпечення оборони.
- Стратегічне планування — процес прийняття рішень щодо ліквідації “вузьких місць” та диспропорцій у ресурсних комплексах ОПК з урахуванням життєвого циклу озброєння.
- Стратегічна організація — процес приведення розрізнених компонентів у цілісну систему, розбудова управляючої структури та інформаційно-аналітичного забезпечення.
- Стратегічна координація — узгодження цілей та інтересів суб’єктів управління (міністерств, відомств, заводів) у просторі та часі.
- Стратегічний контроль — відстеження результативності рішень на основі фреймового представлення знань (порівняння факту з еталоном).

Система управління ОПК — це комплекс забезпечувальних підсистем, що перебувають у динамічному взаємозв’язку для планомірного досягнення цілей шляхом антиципації (випереджального розпізнавання) проблемних ситуацій.

Авторське бачення ключових інноваційних категорій:

1. Система стратегічного планування — комплекс компонентів, взаємопов’язаних інформаційно-логічними процесами, де знання про ризики та шляхи їх вирішення агреговані у фреймах і візуалізовані через семантичні структури.
2. Альтернативний мережевий графік — когнітивна модель процесу прийняття рішень, що відображає багатоваріантність шляхів реалізації цілей через цільове динамічне нормування граничних параметрів.
3. Динамічний когнітивний сценарій — дослідницький конструкт на базі інтелектуальних технологій, що здійснює прямий та зворотний логічний вивід для підтримки управлінських рішень.
4. Ризикозахищеність — внутрішня властивість системи планування зберігати рівноважний стан і забезпечувати потреби оборони навіть у разі реалізації критичних загроз.

Порівняльна характеристика традиційного та логіко-лінгвістичного підходів до планування в ОПК представлена у табл. 7.

Таблиця 7 – Порівняльна характеристика традиційного та логіко-лінгвістичного підходів до планування в ОПК

Параметр порівняння	Традиційний підхід	Логіко-лінгвістичний підхід
Форма представлення даних	Числові показники, таблиці	Фрейми знань, семантичні мережі
Метод обробки	Статистичні екстраполяції	Логічний вивід (прямий та зворотний)
Реакція на проблему	Констатація відхилення (post factum)	Антиципація (передбачення ситуації)
Облік контексту	Абстрактні середні величини	Врахування мотивації ОПР та специфіки ситуації

Джерело: розроблено автором

Висновки

1. Обґрунтовано необхідність інтеграції оборонно-промислового комплексу в національну економічну систему на основі адаптивного управління з використанням інтелектуальних технологій в умовах високої невизначеності.

2. Доведено доцільність застосування параметричної теорії систем і логіко-

лінгвістичного моделювання для формалізації взаємодії суб'єкта та об'єкта управління в ОПК через розмежування атрибутивних і реляційних концептів.

3. Показано, що цифровий двійник і динамічний когнітивний сценарій є ключовими інструментами антиципації стратегічних загроз, синхронізації ресурсних потоків та моделювання альтернативних шляхів досягнення стратегічних цілей.

4. Узагальнено, що запропонований теоретико-методологічний підхід створює основу для побудови систем адаптивного управління ОПК, спрямованих на підвищення стійкості та ризикозахищеності національної економіки.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Brzoska M. Smart Defense and the Future of European Defense Industrial Policy. Rome: IAI, 2012. 124 p. URL: https://www.iai.it/sites/default/files/iai_7.pdf.
2. Stiglitz J. E. Globalization and Its Discontents. New York: W. W. Norton & Company, 2002. 304 p.
3. Gansler J. S. Democracy's Arsenal: Creating a Twenty-First-Century Defense Industry. Cambridge, MA: MIT Press, 2011. 432 p.
4. Strategic Compass for Security and Defence. Brussels: European External Action Service, 2022. 64 p. URL: https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf.
5. National Defense Industrial Strategy 2023. Washington, D.C.: U.S. Department of Defense, 2023. 60 p. URL: https://www.businessdefense.gov/NDIS.html.
6. Геєць В. М. Бар'єри на шляху розвитку промисловості на інноваційній основі та можливості їх подолання. *Економіка України*. 2018. № 1. С. 3–26.
7. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегію розвитку оборонно-промислового комплексу України": Указ Президента України від 20.08.2021 № 372/2021. URL: https://zakon.rada.gov.ua/laws/show/372/2021.

References

1. Brzoska, M. (2012). Smart Defense and the Future of European Defense Industrial Policy. IAI. https://www.iai.it/sites/default/files/iai_7.pdf
2. Stiglitz, J. E. (2002). Globalization and Its Discontents. W. W. Norton & Company.
3. Gansler, J. S. (2011). Democracy's Arsenal: Creating a Twenty-First-Century Defense Industry. MIT Press.
4. European External Action Service. (2022). Strategic Compass for Security and Defence. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf
5. U.S. Department of Defense. (2023). National Defense Industrial Strategy 2023. https://www.businessdefense.gov/NDIS.html
6. Heiets, V. M. (2018). Bariery na shliakhu rozvytku promyslovosti na innovatsiinii osnovi ta mozhlyvosti yikh podolannia [Barriers to industrial development on an innovative basis and ways to overcome them]. *Economy of Ukraine*, (1), 3–26.
7. President of Ukraine. (2021). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 20 serpnia 2021 roku «Pro Stratehiiu rozvytku oboronno-promyslovoho kompleksu Ukrainy» [On the decision of the National Security and Defense Council of Ukraine dated August 20, 2021 "On the Strategy for the Development of the Defense-Industrial Complex of Ukraine"]. https://zakon.rada.gov.ua/laws/show/372/2021