# ВОЄННА СТРАТЕГІЯ MILITARY STRATEGY and Technology та технології

№ 1(4)/2026

UKRAÍNE

Громадська організація
"Центр воєнної стратегії і технологій"

# ВОЄННА СТРАТЕГІЯ І ТЕХНОЛОГІЇ

НАУКОВО-ПРАКТИЧНИЙ ЖУРНАЛ

№ 1(4)/2026

ISSN (online): 3083-6476

Науково-практичний журнал "Military strategy and technology" № 1(4)/2026

УДК 355.4(082)

DOI: 10.63978/3083-6476.2026.1.4

ISSN (online): 3083-6476

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

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

Видається з травня 2025 року, чотири рази на рік

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

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

**Науковий профіль видання:**

К1 Державна безпека
К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
К4 Управління інформаційною безпекою
К5 Військове управління (за видами збройних сил)
К6 Забезпечення військ (сил)
К7 Озброєння та військова техніка
К10 Цивільна безпека
F5 Кібербезпека та захист інформації

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

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

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

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

*Усі статті, що публікуються в журналі, проходять обов'язкове рецензування, яке здійснюється за анонімною формою як для авторів, так і для рецензентів (подвійне сліпе рецензування). За достовірність викладених фактів, цитат та інших відомостей відповідальність несе автор*

## КООРДИНАЦІЙНА РАДА

*Голова Координаційної ради:* ***Залужний Валерій Федорович,*** доктор філософії

*Заступник голови Координаційної ради:* ***Шаптала Сергій Олександрович***

**Члени Координаційної ради:**

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

***Забродський Михайло Віталійович***

***Кириленко Олександр Миколайович***

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

***Кучеренко Віктор Віталійович***

***Мойсюк Євген Георгійович***

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

## РЕДАКЦІЙНА КОЛЕГІЯ

*Головний редактор:*

***Мохор Володимир Володимирович,*** доктор технічних наук, професор, Інститут проблем моделювання в енергетиці імені Г.Є. Пухова НАН України (Київ, Україна)

**Члени редакційної колегії:**

***Кульпа Христоф,*** доктор технічних наук, професор, Варшавський політехнічний університет (Варшава, Польща)

***Лисецький Юрій Михайлович,*** доктор технічних наук, доцент, Воєнна академія імені Євгенія Березняка (Київ, Україна)

***Марутян Рена Рубенівна,*** доктор наук з державного управління, доцент, Київський національний університет імені Тараса Шевченка (Київ, Україна)

***Непомнящий Олександр Михайлович,*** доктор наук з державного управління, професор, Національний авіаційний університет (Київ, Україна)

***Ноорма Март,*** доктор філософії, професор космічних та оборонних технологій, Тартуський університет (Тарту, Естонія)

***Піллей Дівакаран Падма Кумар,*** доктор філософії, Пенджабський університет (Патьяла, Індія)

***Помаза-Пономаренко Аліна Леонідівна,*** доктор наук з державного управління, старший дослідник, Національний університет цивільного захисту України ДСНС (Київ, Україна)

***Прав Юрій Григорович,*** доктор наук з державного управління, професор, Національний авіаційний університет (Київ, Україна)

***Рубан Ігор Вікторович,*** доктор технічних наук, професор, Харківський національний університет радіоелектроніки (Харків, Україна)

***Хижняк Ірина Анатоліївна,*** кандидат технічних наук, Харківський національний університет Повітряних Сил ім. І. Кожедуба (Харків, Україна)

***Худов Геннадій Володимирович,*** доктор технічних наук, професор, Харківський національний університет Повітряних Сил імені І. Кожедуба (Харків, Україна)

***Шишацький Андрій Володимирович,*** доктор технічних наук, старший науковий співробітник, Генеральний штаб Збройних Сил України (Київ, Україна)

***Ярош Сергій Петрович,*** доктор військових наук, професор, Харківський національний університет Повітряних Сил імені І. Кожедуба (Харків, Україна)

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

# MILITARY STRATEGY AND TECHNOLOGY

SCIENTIFIC AND PRACTICAL JOURNAL

№ 1(4)/2026

ISSN (online): 3083-6476

Scientific and practical journal "Military strategy and technology" № 1(4)/2026

UDC 355.4(082)

DOI: 10.63978/3083-6476.2026.1.4

ISSN (online): 3083-6476

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

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

Founded in May 2025, 4 times a year

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

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

**Scientific profile of the publication:**

K1 State Security
K3 National Security (by individual areas of support and types of activity)
K4 Information Security Management
K5 Military Management (by types of armed forces)
K6 Supply of troops (forces)
K7 Armaments and military equipment
K10 Civil Security
F5 Cybersecurity and information protection

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

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

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

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

*All articles published in the journal undergo mandatory peer review, which is carried out anonymously for both authors and reviewers (double-blind peer review). The author is responsible for the reliability of the facts, quotes and other information presented*

# ЗМІСТ

*Received 04.03.2026 | Accepted 16.03.2026 | Published 30.03.2026*



УДК 355.45:623 DOI: 10.63978/3083-6476.2026.1.4.01

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

# ОБОРОННІ ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ ДЕРЖАВНОГО УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ ТА ТРАНСФОРМАЦІЇ МІЖНАРОДНОГО БЕЗПЕКОВОГО СЕРЕДОВИЩА

***Анотація.*** *У статті розглянуто розвиток оборонних технологій в Україні на тлі повномасштабної війни з росією з 2022 року та їхній вплив на міжнародне безпекове середовище. Особливу увагу приділено трансформації українського оборонно-промислового комплексу: технологічним інноваціям (масове виробництво дронів, системи радіоелектронної боротьби, елементи штучного інтелекту, кіберзахист), інституційним змінам (від децентралізованої моделі до спроб централізації, державно-приватне партнерство, створення Міжвідомчої комісії при РНБО) та геополітичним наслідкам.*

*На основі даних SIPRI (військові витрати України 64,7 млрд дол. США у 2024 р.), CFR, Atlantic Council та інших джерел проаналізовано зростання виробництва БПЛА (2,5–4 млн одиниць у 2025 р., план 7 млн у 2026 р.), інвестиції в defence-tech (понад 105 млн дол. у 2025 р.), перші експортні ліцензії та потенціал експорту на кілька мільярдів доларів щорічно за умови гармонізації з європейськими стандартами. Окремо висвітлено ризики: залежність від імпорту комплектуючих, дефіцит кваліфікованих фахівців, кіберзагрози (понад 2000 інцидентів у 2023 р. за даними CERT-UA та ENISA), бюрократичні бар'єри в НАТО та ЄС.*

*Запропоновано модель "Інтеграційна піраміда" з трьома рівнями: технологічна автономність (локалізація виробництва), регуляторна гармонізація (відповідність стандартам ЄС/НАТО), міжнародний вплив (експорт, спільні програми, внесок у колективну безпеку). Модель синтезує емпіричні дані та теоретичні концепції (RMA, "нові війни" Kaldor, роботи Horowitz та Scharre), але визнає власні обмеження: ефективна в асиметричних конфліктах середньої інтенсивності, менш універсальна в глобальних сценаріях.*

*Висновки підкреслюють роль України як реального випробувального полігону для Європи, де дешеві combat-proven рішення (наприклад, FPV-дрони) контрастують з провалами дорогих венчурних проєктів (Stark Defence). Рекомендації стосуються гармонізації стандартів, спільного виробництва (ППО, дрони, боєприпаси збільшеної дальності), збереження фронтового зворотного зв'язку, децентралізації критичної інфраструктури та регулярного SWOT-моніторингу ОПК.*

***Ключові слова:*** *оборонні технології, ОПК України, гібридна війна, дрони, радіоелектронна боротьба, кібербезпека, європейська безпека, НАТО, DIANA, інновації, експорт озброєнь.*

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

# DEFENSE TECHNOLOGIES AS A TOOL OF STATE MANAGEMENT OF NATIONAL SECURITY AND TRANSFORMATION OF THE INTERNATIONAL SECURITY ENVIRONMENT

***Abstract.*** *The article examines the development of defense technologies in Ukraine amid the full-scale war with Russia since 2022 and their impact on the international security environment. Particular attention is given to the transformation of Ukraine's defense-industrial complex: technological innovations (mass drone production, electronic warfare systems, AI elements, cybersecurity), institutional changes (from decentralized model to attempts at centralization, public-private partnerships, establishment of the Interagency Commission under the National Security and Defense Council), and geopolitical implications.*

*Drawing on data from SIPRI (Ukraine's military expenditure $64.7 billion in 2024), CFR, Atlantic Council and other sources, the study analyzes the growth of UAV production (2.5–4 million units in 2025, target 7 million in 2026), investments in defense-tech (over $105 million in 2025), first export licenses issued and export potential of several billion dollars annually subject to harmonization with EU standards. Specific risks are highlighted: dependence on imported components, shortage of qualified personnel, cyber threats (over 2000 incidents in 2023 according to CERT-UA and ENISA), bureaucratic barriers within NATO and the EU.*

*An "Integration Pyramid" model is proposed with three levels: technological autonomy (localization of production), regulatory harmonization (compliance with EU/NATO standards), international influence (export, joint programs, contribution to collective security). The model synthesizes empirical data and theoretical concepts (RMA, Kaldor's "new wars", works by Horowitz and Scharre), yet acknowledges its limitations: effective in asymmetric conflicts of medium intensity, less universal in global scenarios.*

*Conclusions emphasize Ukraine's role as a real testing ground for Europe, where low-cost combat-proven solutions (e.g., FPV drones) contrast with failures of expensive venture projects (Stark Defence). Recommendations focus on standards harmonization, joint production (air defense, drones, long-range munitions), preservation of frontline feedback loops, decentralization of critical infrastructure, and regular SWOT monitoring of the DIC.*

***Keywords:*** *defense technologies, Ukraine's DIC, hybrid warfare, drones, electronic warfare, cybersecurity, European security, NATO, DIANA, innovations, arms export.*

**JEL Classification:** O32, H56, L64, F52

## Вступ

Повномасштабна збройна агресія російської федерації проти України, що розпочалася у лютому 2022 року, не лише спричинила глибоку гуманітарну кризу та фундаментальні геополітичні зрушення, але й стала потужним каталізатором для трансформації глобальних оборонних систем, військової організації та технологічних підходів до ведення сучасної війни. Цей воєнний конфлікт, що триває вже понад чотири роки, продемонстрував, як високотехнологічні інновації, інтегровані в реальні бойові умови, можуть радикально змінити динаміку протистоянь, переорієнтувавши акцент з традиційних обсягів матеріальних ресурсів на швидкість адаптації та ефективність цифрових рішень. Зокрема, війна виявила, що сучасні конфлікти все більше залежать від гібридних елементів, де кіберзагрози, автономні системи та інформаційні мережі відіграють ключову роль, доповнюючи кінетичні операції [1].

Актуальність теми посилюється останніми подіями в Ірані, де ескалація конфлікту з США та Ізраїлем, включаючи удари по лідерству (вбивство Верховного лідера Аятолли Алі Хаменеї) та військових об'єктах, призвела до асиметричної відповіді Ірану з використанням гіперзвукових ракет Fattah-2, кібератак на інфраструктуру та ударів по країнах Перської затоки. Це спричинило зростання цін на нафту через атаки на танкери в Ормузькій протоці та інтернет-блекаут в Ірані. Це переконливо ілюструє, як оборонні технології (гіперзвук, кібер, дрони) можуть швидко ескалувати регіональні кризи, загрожуючи глобальній енергетичній безпеці та європейській стабільності через потенційні потоки біженців і ланцюгові реакції [23-25].

За даними Stockholm International Peace Research Institute (SIPRI), військові витрати України до 2024 року зросли і сягнули 64,7 млрд доларів США: це вже не просто зростання,

а один із найвищих показників військового навантаження на економіку (близько 34 % ВВП). Цей стрибок не лише підкреслив економічну напругу, але й стимулював перехід до гібридного характеру конфлікту, де технологічна якість – автономні дрони, системи радіоелектронної боротьби – дедалі більше доповнює традиційні фактори, включаючи логістику та артилерійську підтримку.

Наприклад, за оцінками Atlantic Council, значна частина втрат у початкових фазах війни були пов'язані з логістичними проблемами, але стабілізація постачань у 2024-2025 роках дозволила зосередитися на технологічних перевагах, таких як FPV-дрони з оптоволоконним керуванням, що підвищили ефективність на 30-40 % у зонах інтенсивних бойових дій [9; 10]. Водночас варто зауважити, що ці оцінки ефективності часто базуються на польових звітах і можуть бути суб'єктивними. Точна статистика втрат від дронів досі частково класифікована.

У міжнародному контексті трансформація українського оборонно-промислового комплексу (ОПК) розглядається як стратегічний фактор посилення безпекової архітектури Європи. Згідно з аналізом Council on Foreign Relations (CFR), саме українська оборонно-промислова база може стати одним із ключових елементів відновлення європейської обороноздатності, особливо з огляду на дефіцит виробничих потужностей у країнах ЄС [2].

Потенціал експорту українських оборонних технологій оцінюється орієнтовно в діапазоні кількох мільярдів доларів США щорічно за умови відповідності стандартам ЄС, це базується на прогнозі зростання ОПК та інтеграції з європейськими ланцюгами постачань (Reuters, лютий 2026). Інвестиції в deftech зросли стократно з 2023 року до понад 105 млн доларів у 2025 році [2]. Але чи стійке це зростання – питання відкрите: значна частина інвестицій залежить від зовнішніх партнерів, і в разі зміни політичної кон'юнктури (наприклад, зменшення допомоги) темпи можуть сповільнитися.

Проблематика дослідження полягає у необхідності розібратися у взаємозв'язку між технологічними інноваціями, інституційною перебудовою оборонної галузі та змінами в міжнародному безпековому середовищі. Російсько-українська війна виявила потребу в переосмисленні європейської безпеки, де традиційні моделі НАТО доповнюються новими ініціативами, такими як DIANA (Defence Innovation Accelerator for the North Atlantic) з бюджетом 1 млрд євро, спрямованими на прискорення інновацій [15]. Переговори про участь України в DIANA ведуться з грудня 2025 року – це може стати першим випадком залучення не-члена Альянсу як повноцінного партнера, але поки що статус не фіналізований.

Гіпотеза дослідження сформульована як модель з трьома незалежними змінними та одним залежним результатом: якщо рівень технологічної автономності (виражений як частка локалізованого виробництва в загальному обсязі ОПК, наприклад, 50 % за SIPRI) перевищує критичний поріг і поєднується з регуляторною інтеграцією (відповідність стандартам ЄС та НАТО, вимірювана кількістю спільних програм), тоді формується системний міжнародний вплив України на європейську безпеку.

Механізм впливу реалізується через три взаємопов'язані канали [2; 9]:

1) скорочення залежності від імпорту та прискорення циклу інновацій (від розробки до бойового застосування за тижні, як у випадку з дронами);

2) посилення експортної присутності та дипломатії;

3) внесок у колективну безпеку через спільні програми (наприклад, з Францією в рамках "Brave France" для тестування технологій).

Ця гіпотеза враховує емпіричні дані, такі як зростання виробництва дронів в Україні з 2,5-4 млн у 2025 році до планових 7 млн у 2026 році, що робить країну потенційною "дроновою столицею" світу. Однак без повної інституційної інтеграції, включаючи гармонізацію з європейськими регуляціями, вплив на глобальну безпеку залишається обмеженим, з ризиками фрагментації та залежності від зовнішньої допомоги. Події в Ірані, з їхньою асиметричною відповіддю (гіперзвукові удари, кіберінциденти), підкреслюють, як

подібні технології можуть швидко дестабілізувати регіони, впливаючи на європейську безпеку через енергетичні шоки та ескалацію.

## Огляд літератури

Теоретична база осмислення технологічних змін у війні сформована задовго до подій 2022 року, зокрема концепцією "революції у військовій справі" (Revolution in Military Affairs, RMA), розробленою Andrew F. Krepinevich, яка акцентує роль інформаційних технологій у трансформації способів ведення війни [3]. Автор стверджує, що ця концепція, хоча й переконлива для великих держав з розвиненою промисловістю, недооцінює асиметричні адаптації в конфліктах на кшталт українсько-російського, де приватні ініціативи та швидкі ітерації технологій, такі як дешеві дрони та крилаті ракети, стають домінуючими.

Подальший розвиток ідеї RMA відображено у працях Williamson Murray та MacGregor Knox, де підкреслюється системний характер військових інновацій, що поєднує технології з організаційними змінами [4]. Сумнівно, чи така модель повною мірою застосовна до України, де цикл адаптації дронів та контрзаходів скоротився до 2-3 місяців у 2025 році – це перевищує темпи традиційних армій [3; 4; 10].

Lawrence Freedman у своїй фундаментальній праці "The Future of War" зазначає, що технологічні зміни не замінюють політичної природи війни, але суттєво змінюють її інструментарій, роблячи акцент на інформаційному домені [5]. Це твердження переконливо демонструє реальність українського фронту, де дрони не лише як засоби ураження, але й як елементи інформаційної інфраструктури, формують багаторівневу систему спостереження. Подібну позицію розвиває Mary Kaldor у концепції "нових воєн", акцентуючи на взаємодії державних і недержавних акторів у цифровізованому середовищі, що особливо актуально для України з її волонтерськими групами на кшталт Wild Hornets, які розробили контр-дрони STING для перехоплення російських Shahed [6]. Але чи буде така децентралізована модель стійкою в довгостроковій перспективі без інституційної підтримки та залежності від зовнішньої допомоги?

У контексті штучного інтелекту (ШІ) та автономних систем ключовими є роботи Paul Scharre та Michael C. Horowitz, які аналізують стратегічні наслідки впровадження алгоритмічних рішень у військову сферу [7; 8]. Horowitz доводить, що швидкість технологічного освоєння є ключовим фактором зміни балансу сил, але в українському випадку це працює з обмеженнями: за даними SIPRI, військові витрати України у 2024 році сягнули 64,7 млрд доларів, що дозволило масштабувати виробництво дронів, але з ризиками залежності від імпорту компонентів [9]. Це підкреслює необхідність локалізації, оскільки російські контрзаходи, такі як Supercam дрони з системами ухилення від перехоплювачів, вже перевершують українські в деяких аспектах. Аналітики Chatham House наголошують, що досвід України може слугувати джерелом інституційних уроків для НАТО, зокрема в ініціативах DIANA [10].

Вітчизняні дослідники Гурковський В., Романенко Є., Коваль В., Ільницький С. в своїй праці "Форсайт-дослідження як інструмент зміцнення резильєнтності до загроз БПЛА з оптоволоконникм управлінням" розглядають західні та українські розробки засобів протидії оптоволоконним БПЛА, зокрема лазерні сисеми, радари та ШІ-базовані детектори [20]. Зазначені автори пропонують стратегічний підхід до відбору пріоритетних технологічних напрямів у сфері оборони, орієнтований на довгострокові сценарії військово-технічного розвитку.

Водночас література містить застереження щодо ризиків надмірної венчуризації оборонного сектору. Приклад компанії Stark Defence, проаналізований у DroneXL (2025), демонструє, що не всі інноваційні проєкти ШІ витримують перевірку реальними умовами [12]. Коли ударні безпілотники на базі ШІ не влучили у ціль під час чотирьох окремих спроб, це викрило неприємну правду: мільярди венчурного капіталу та спритний маркетинг

не змінюють жорсткого зворотного зв'язку реального бою. Українські FPV дрони вартістю 400 доларів щодня знищують російську бронетехніку зі швидкістю розгортання тисяч одиниць на день – це контраст, який важко ігнорувати.

Для України, де відбувається масштабне тестування нових видів озброєння в умовах реального бойового застосування, європейська безпека дедалі більше залежить від такого "лабораторного осередку" перевірки технологій у реальних умовах.

Для посилення аналізу загроз безпеки розглянемо роботу про кіберзагрози в російсько-українській війні 2022-2023, яка підкреслює зростання загроз з кіберпростору, з понад 2000 інцидентами в Україні за ENISA, що еволюціонували від DDoS до цільових атак на енергетику [21]. Це підтверджується створенням Cyber Force та Space Force в Україні до кінця 2025 року, як оголошено парламентом, що сигналізує про стратегічний зсув до незалежних кібер- та космічних команд. Але чи буде це достатньо без ресурсів рівня США, нажаль, сумнівно, оскільки росія нарощує дронові операції через Rubicon Center, виробляючи до тисяч Shahed на місяць.

Окрім того, останні дані про використання "Шахедів" свідчать, що вони перетворилися з простих камікадзе-дронів у мережеві, багатофункціональні платформи зі впровадженням елементів ШІ та роєвої логіки. Все частіше вони використовуються як носії FPV-дронів – вони наближаються до лінії фронту або території України, а потім скидають дрібні FPV, які далі ведуть точкові атаки з короткої дистанції.

Незважаючи на значну кількість аналітичних матеріалів, комплексного дослідження, що інтегрує стратегічну теорію, інституційний аналіз та практику українського ОПК, наразі бракує. Акцент Horowitz на дифузії влади корисний, але не враховує локальні фактори, такі як дефіцит embedded-розробників, що обмежує масштабування. Додаткові EU звіти, як McKinsey's European defense by the numbers, прогнозують витрати ЄС до 800 млрд євро до 2030 року, додаючи економічний вимір [30]. Сумнівно, чи Європа зможе досягти оборонної автономії без української швидкості інновацій.

## Мета та завдання статті

Метою дослідження є виявлення та оцінка механізмів, через які розвиток оборонних технологій в Україні в умовах російсько-української війни трансформує національний оборонно-промисловий комплекс і впливає на європейську безпекову архітектуру, зокрема в процесі інтеграції з НАТО та ЄС, з формулюванням моделі такого впливу.

## Методи

Методологічна основа базується на поєднанні системного аналізу, інституційного підходу та порівняльної методології. Такий гібридний метод видається найбільш адекватним для вивчення українського ОПК в умовах триваючого конфлікту високої інтенсивності, оскільки дозволяє розглядати технологічні інновації не ізольовано, а як частину взаємопов'язаної екосистеми, де технічні рішення, організаційні структури та міжнародні кооперацийні механізми формують єдину модель.

Системний аналіз застосовується для оцінки оборонних технологій як динамічної системи з елементами зворотного зв'язку: бойовий досвід безпосередньо впливає на ітерації розробки, що скорочує цикл від концепції до застосування до кількох тижнів або місяців – на відміну від традиційних 5-10 років у великих державах НАТО. Це поки переконливо демонструє перевагу асиметричної адаптації в Україні.

Інституційний підхід фокусується на трансформації управлінських структур, підвищенні ролі професійних асоціацій, державно-приватного партнерства та нових органів, таких як Міжвідомча комісія з питань військово-промислової політики та оборонних технологій при РНБО (утвореної рішенням РНБО від 22 листопада 2025 року, введеним в дію 12 лютого 2026 року указом Президента України №116/2026) [18]. Цей

підхід дозволяє оцінити, як інституційна централізація балансує між децентралізованою венчурною моделлю (понад 450 компаній лише в дроновому секторі) та державним контролем. Саме інституційна перебудова є визначальним чинником для переходу від "виживання в умовах довготриваючої війни" до "системного зростання", але ризики бюрократії проявилися в затримках з експортними ліцензіями, зокрема в сегменті озброєння та БПЛА на початку 2026 року.

Порівняльна методологія дає змогу зіставити український досвід з практиками держав НАТО, зокрема в рамках DIANA. У 2026 році програма розширилася до найбільшої когорти – 150 інноваторів з 24 країн НАТО, з фокусом на дуальні технології (UAV, AI, кіберзахист) [15]. Україна, як потенційний перший не-член НАТО партнер у DIANA (переговори ведуться з грудня 2025 року), отримує доступ до інфраструктури та фінансування, що створює унікальну можливість для інтеграції.

Порівняння з традиційними моделями НАТО (де цикл інновацій часто перевищує 5 років) підкреслює українську перевагу в швидкості, але бюрократичні бар'єри Альянсу можуть не дозволити повноцінно інтегрувати українські рішення без значних компромісів щодо стандартів [29].

Джерельна база обмежується переважно верифікованими інституційними та академічними матеріалами: звіти SIPRI (Trends in World Military Expenditure 2024, де витрати України сягнули 64,7 млрд дол. США у 2024 році з подальшим зростанням), ENISA Threat Landscape, EDA Defence Data, NATO офіційні документи, CFR та Atlantic Council аналізи, а також peer-reviewed публікації з ResearchGate (2023–2026) щодо кіберзагроз та національної стійкості [15; 28; 9]. Публіцистичні та експертні оцінки (наприклад, з DOU чи IT Arena) використовуються як ілюстративні, а не як основа кількісних висновків, щоб уникнути ризику переоцінки прогнозів [16; 19].

Обмеження методології полягають у доступності даних: повна статистика виробництва та втрат залишається класифікованою, а війна вносить динаміку, що ускладнює довгострокові прогнози. Це змушує покладатися на непрямі індикатори (зростання інвестицій у deftech до понад 105 млн дол. у 2025 році, експортні центри в Європі з 2026 року), але підкреслює необхідність постійної емпіричної верифікації. Порівняльний вимір з іншими конфліктами (наприклад, ізраїльські інновації в Iron Dome чи турецькі Bayraktar) свідчить, що український кейс унікальний за масштабом децентралізації та швидкістю, але ризикує втратити темп без стабільного фінансування та інтеграції з ЄС/НАТО.

## Результати

### Технологічна трансформація: системний вимір

Технологічні зміни в українському оборонному секторі після 2022 року не обмежуються ізольованими інноваціями, а формують мережеву інтеграцію безпілотних платформ, сенсорних систем, алгоритмів обробки даних, засобів радіоелектронної боротьби та цифрових комунікацій. Згідно з Keir Giles у публікації Chatham House "NATO can learn from Ukraine's military innovation" (2023), ключовою особливістю українського підходу є швидка інтеграція комерційних технологій в оперативну практику, що скорочує цикл від розробки до бойового застосування до тижнів [11].

Це ілюструє перевагу асиметричної війни, де Україна виробляє від 2,5 до 4 млн дронів у 2025 році з планами на 7 млн у 2026, роблячи країну "дрономовою столицею" світу [10]. Однак чи така швидкість буде стійкою без стабільного фінансування з урахуванням ризиків залежності від імпорту компонентів [11].

У цьому контексті БПЛА виконують не лише функцію засобів ураження, а й елементів інформаційної інфраструктури, поєднуючись із супутниковим зв'язком, цифровими картографічними сервісами та алгоритмічними системами аналізу. Подібна

конфігурація змінює традиційні уявлення про глибину оборони та наступу, інтегруючи розвідку і вогневе ураження у спільний цифровий контур, як описано в Council on Foreign Relations “Securing Ukraine’s Future in Europe” [2].

Звіт CFR є цінним через стратегічний аналіз, але оцінка потенціалу експорту (кілька млрд доларів) потребує уточнення через регуляторні бар’єри ЄС, оскільки зростання виробництва дронів з fiber-optic FPV технологіями вимагає сертифікації для спільних проєктів з Францією чи Німеччиною [10]. Водночас зростає значення засобів радіоелектронної боротьби (РЕБ), які нівелюють переваги високотехнологічних систем шляхом придушення сигналів або перехоплення управління. Така динамічна конкуренція створює технологічний паритет, але в умовах високої інтенсивності брак GPS змушує переходити до альтернатив, таких як радіомаяки, що може генерувати нові вразливості без кіберзаходів [2; 10].

**Інституційна перебудова та інтеграція з НАТО та ЄС**

Трансформація технологічного середовища супроводжується інституційними змінами, де мережа професійних об’єднань відіграє роль посередника між державою, бізнесом та міжнародними партнерами [13]. Формування таких структур сприяє інституціоналізації сектору, раніше фрагментованого, з кількістю виробників понад 500 за SIPRI [9]. Звіт SIPRI є надійним завдяки глобальним даним, але недооцінює роль приватного сектору, де зростання інвестицій у deftech сягнуло 105 млн доларів у 2025 році [2]. Створення Міжвідомчої комісії з питань військово-промислової політики та оборонних технологій при РНБО України у 2026 році вказує на централізацію, але ризики бюрократії можуть уповільнити експорт.

Виклики технологічної конкуренції змушують НАТО переглядати інноваційну політику, як у ініціативах DIANA. Український досвід демонструє гнучкість, але традиційні моделі НАТО ускладнюють адаптацію [11]. Це створює структурний виклик: стандартизація повинна поєднуватися з українським темпом, як у передачі Saab 340 AEW&C у 2026 році. Звіт GLOBSEC “Seven Security Scenarios on Russian War in Ukraine for 2025–2026” є корисним для сценаріїв, але прогнози ескалації не завжди враховують AI-інтеграцію.

**Кібербезпека та багатодоменні операції**

Кібербезпека та багатодоменні операції становлять один із критичних аспектів сучасного оборонного середовища. Згідно з ENISA Threat Landscape 2023, у Європі спостерігається стійке зростання кіберзагроз, зокрема в секторах критичної інфраструктури та енергетики; для України цей тренд посилюється через геополітичний тиск [14]. Peer-reviewed стаття “The 2022-2023 Russia-Ukraine War and Cyberspace Threats” (Lagvilava, 2023) детально описує еволюцію кіберзагроз: від масових DDoS-атак на початку вторгнення до більш цілеспрямованих операцій проти енергетичної інфраструктури, транспортних систем та урядових мереж [21]. Така еволюція суттєво посилює ризик ескалації конфлікту, перетворюючи кіберпростір на повноцінний оперативний домен. Ефективність превентивних заходів залишається обмеженою без переходу до децентралізованої архітектури мереж та підвищення стійкості на рівні мікромереж і локальних енергетичних вузлів.

Економічні аспекти трансформації ОПК України визначаються як потенціалом зростання, так і структурними обмеженнями. За оцінками CFR (2025), потенціал експорту може сягати кількох мільярдів доларів США щорічно за умови гармонізації з європейськими стандартами [2].

Звіт McKinsey “European defense by the numbers” (2026) прогнозує зростання загальних витрат європейських країн НАТО на оборону до 800 млрд євро до 2030 року, що створює сприятливе середовище для інтеграції українського ОПК як постачальника інноваційних рішень [30]. Звіти European Defence Agency (EDA) свідчать, що витрати ЄС

на оборону у 2024 році сягнули 343 млрд євро зі зростанням на 19 %, що створює можливості для спільних проєктів з Україною [29;30].

Геополітичні імплікації трансформації українського ОПК полягають у потенціалі посилення колективної оборони через інтеграцію швидких інноваційних практик України в європейські структури. Згідно з публікацією Atlantic Council (2026), Європа потребує саме української моделі – швидкості адаптації, децентралізації розробок і тісного зворотного зв'язку з фронтом – для подолання власної бюрократичної інерції [10].

Така інтеграція може стати каталізатором змін у НАТО та ЄС, перетворюючи Україну з отримувача допомоги на ключового постачальника технологій і тактичних рішень. Водночас фрагментація європейського оборонного ринку створює інвестиційний та фінансовий дефіцит, оцінюваний у сотні мільярдів євро за наступне десятиліття; цей розрив ускладнює швидке нарощування спроможностей і робить Європу вразливою до зовнішніх постачальників.

**Розвиток ОПК України**

Важливість розвитку власної оборонної промисловості важко переоцінити, оскільки технологічна перевага завжди відіграє ключову роль у військових конфліктах і російсько-українська війна лише підтверджує цей факт.

Ще до початку широкомасштабної російської агресії було визначено *критичні чинники*, які суттєво впливали на розвиток ОПК України, а саме:

відсутність дієвих механізмів переходу від виробництва одиночних і малосерійних виробів до *серійного виробництва* новітніх зразків ОВТ, залучення інвестицій у галузь;

недостатня концентрація ресурсів для реалізації пріоритетних напрямів створення ОВТ нових поколінь;

повна відсутність державної підтримки та фінансування *розвитку критичних технологій* у сфері ОПК України та проведення фундаментальних досліджень в інтересах Сил безпекиі оборони України;

*низький рівень узгодженості* військово-технічної та військово-промислової політики під час розроблення новітніх зразків ОВТ;

*низький рівень* військово-технічного співробітництва для залучення міжнародних компаній до інвестування в підприємства ОПК.

За останні роки вітчизняна оборонна промисловість демонструє значний розвиток та налагодила виробництво широкого спектру озброєнь, насамперед артилерійські системи, міномети, бронетехніку, FPV-дрони, водні дрони, ракети, боєприпаси радянських калібрів. У той же час забезпечення потреб Сил безпеки і оборони України залишається на недосяжному рівні і на даний час складає близько 40%, що в свою чергу вимагає значних фінансових витрат з державного бюджету на імпорт озброєння та боєприпасів і призводить до критичної залежності від міжнародної військової допомоги.

Одним із основних факторів, що гальмують розвиток ОПК України, є *безпека інфраструктури*, оскільки багато підприємств залишаються в зоні підвищеного ризику через бойові дії, що ускладнює виробництво та призводить до потреби релокації підприємств. Не менш важливим фактором є *критична залежність від імпортних комплектуючих та сировини*, зокрема вибухових речовин, які держава не виробляє у достатніх обсягах.

Також негативно впливає на розвиток оборонної промисловості *відсутність належного механізму державної фінансової підтримки* для відновлення пошкоджених або знищених виробничих потужностей, що суттєво ускладнює виконання оборонних замовлень.

Тому ОПК України сьогодні потребує *системної трансформації*, тобто не просто формування сукупності оборонних підприємтсв, а створення динамічної екосистеми, у якій обєднані державні та приватні підприємсства, де організована тісна взаємодія з міжнародними корпораціями.

З цією метою було проведено оцінювання здатності ОПК України щодо подальшого розвитку за допомогою SWOT-аналізу. Вага кожного фактору була обґрунтована їх прямим впливом на здатність ОПК зберігати конкурентну перевагу в умовах асиметричного конфлікту та переходити до системної інтеграції з європейською безпековою архітектурою:

*Сильні сторони ОПК України*: швидка адаптація технологій; значна кількість виробників (близько 500); потужний приватний сектор, що забезпечує інноваційну гнучкість.

*Слабкі сторони*: фрагментація сектору; гострий дефіцит кваліфікованих фахівців (embedded-розробників, інженерів РЕБ, спеціалістів з кібербезпеки), що обмежує масштабування виробництва.

*Можливості ОПК України*: інтеграція в програми НАТО (зокрема DIANA); потенціал експорту інноваційних рішень на європейський ринок.

*Загрози*: зростаюча кількість багатодоменних кіберзагроз; залежність від зовнішньої допомоги, яка може бути нестабільною в довгостроковій перспективі.

Результати проведеного SWOT-аналізу обумовлюють доцільність розроблення довгострокової стратегії розвитку (модернізації) ОПК України. Ключовими цілями і пріоритетами зазначеної стратегії повинні стати:

у *короткостроковій перспективі* (*під час війни*) – підвищення спроможності забезпечувати потреби Сили безпеки і оборони України в ОВТ та боєприпасах;

у *довгостроковій перспективі* (*післявоєнний період*) – повне забезпечення потреб Сил безпеки і оборони України, створення відповідних запасів та збільшення експортного потенціалу; інтеграція в оборонні стандарти та виробничі ланцюги НАТО та ЄС.

При цьому *основними напрямками подальшого розвитку* ОПК України вважається:

масштабування виробництва ОВТ та боєприпасів;

підтримка наукових розробок та інноваційних рішень (FPV-дрони, морські дрони, автономні роботизовані платформи, високоточна зброя, штучний інтелект);

розвиток спільних проєктів з іноземними партнерами, залучення інвестицій, створення спільних підприємств;

створення прозорої системи захисту інтелектуальної власності та нормативно-правове врегулювання (впровадження механізмів надання державної допомоги для відновлення пошкоджених або знищених виробничих потужностей).

Важливим напрямком подальшого розвитку ОПК повинно стати *державно-приватне партнерство*. Це дозволить збільшити інвестиції за рахунок залучення приватного капіталу, підвищити якість внаслідок збільшення конкуренції в приватному секторі, швидше реагувати на потреби Сил безпеки і оборони України та зменшити навантаження на бюджет.

Ще одним із важливих напрямків розвитку оборонної промисловості має стати формування експортного потенціалу оборонної продукції. З цією метою доцільно використати конкурентні переваги:

*по-перше* – приваблива ціна, оскільки практично будь-яке українське озброєння в 1,5-2 рази дешевше, ніж іноземні аналоги;

*по-друге* – ефективність та інноваційність, у тому числі завдяки постійній комунікації між виробником, винахідником і споживачем (безпосереднє застосування на полі бою).

Необхідно також здійснити *перегляд експортної політики* товарів військового призначення та подвійного використання. Мова йде не про зняття заборони на експорт озброєння, а впровадження жорстких правил та принципів:

*під час війни* – експорт деяких видів озброєнь, які є у профіциті (морські дрони, протитанкові засоби та інше);

*у післявоєнний період* – поступове зняття заборони на експорт, з урахуванням забезпечення поточних потреб Сил безпеки і оборони України та створення відповідних запасів.

На *короткострокову перспективу* ОПК повинен стати фундаментом безпеки та інноваційним кластером економіки України, а на *довгострокову перспективу* його роль слід розглядати в розрізі елементу нової архітектури національної економіки.

**Авторська модель впливу ОПК на міжнародну безпеку: "Інтеграційна піраміда ОПК України"**

Потрібно відзначити, що розроблена модель "Інтеграційна піраміда ОПК України" – це конструкція для оцінювання впливу ОПК України на міжнародне безпекове середовище.

Вона базується на синтезі емпіричних даних із джерел, таких як звіти SIPRI [9], ENISA Threat Landscape 2023 [14], Council on Foreign Relations (CFR) [2] та інші, і покликана пояснити, як внутрішні трансформації ОПК України можуть переростати в глобальні ефекти.

Модель структурована як піраміда з трьома рівнями, де кожен наступний залежить від попереднього (рис.).


Рис. Інтеграційна піраміда ОПК України

*Базовий рівень* – це *технологічна автономність*, фундаментом якої є частка локалізованого виробництва, скорочення циклу інновацій (від тижнів до місяців), адаптація комерційних технологій до військових потреб. Наприклад, зростання виробництва дронів щорічно ілюструє, як автономність дозволяє швидко реагувати на нові виклики [10]. Без міцного базису неможлива стійка інтеграція з міжнародними структурами, оскільки залежність від зовнішніх постачальників робить систему вразливою.

Середній рівень – це *регуляторна гармонізація*, перехідний етап, де технологічна автономність інтегрується з міжнародними стандартами ЄС та НАТО. Вона вимірюється ступенем відповідності нормам (технічні регламенти, сертифікація, кількість спільних програм). Без цього рівня автономні розробки залишаються ізольованими: українські FPV-дрони з оптоволоконним керуванням чи системи РЕБ не можуть вийти на експортні ринки чи інтегруватися в альянсні структури. Гармонізація з європейськими нормами дозволяє уникнути бар'єрів і перетворити локальні інновації на спільні проєкти [31].

*Вершина* – це міжнародний вплив, кінцевий результат, вимірюваний експортним обсягом (кілька млрд дол. США), кількістю спільних програм з НАТО, стійкістю до кіберзагроз та внеском у колективну безпеку. Вплив проявляється через механізми скорочення залежності (від імпорту до експорту), прискорення інновацій, дипломатію технологій (внесок у колективну оборону) та ін.

Розроблена модель має *певні межі* – без повної інституційної інтеграції (членство в НАТО чи ЄС) вплив обмежується асиметричними конфліктами [27].

У цілому, "Інтеграційна піраміда ОПК України" – це інструмент для стратегічної оцінки, що синтезує дані для прогнозування. Вона не є статичною і адаптується до змін (зростання інвестицій, нові загрози тощо).

## Висновки

Проведений аналіз дозволяє модифікувати первинну гіпотезу: технологічна автономність, поєднана з регуляторною інтеграцією до стандартів ЄС та НАТО, формує системний міжнародний вплив України на європейську безпеку, але цей ефект залишається обмеженим без глибокої інституційної трансформації.

Досвід російсько-української війни надає Україні конкурентну перевагу в асиметричних високотехнологічних рішеннях, зокрема в автономних системах, засобах радіоелектронної боротьби та низьковартісних безпілотних платформах, інтегрованих у цифрові мережі управління.

Європейська та міжнародна безпека дедалі більше залежать від українського досвіду як від реального випробувального полігону оборонних технологій у умовах hybrid warfare. Провал дороговартісних стартапів контрастує з масовою ефективністю дешевих FPV-систем. Реальна бойова валідація в Україні стає ключовим критерієм для масштабування оборонних інновацій у Європі, мінімізуючи інвестиційні ризики та визначаючи стандарти ефективності в міжнародному безпековому середовищі.

Реалізація потенціалу ОПК України вимагає посиленої кооперації з Європейським Союзом та Північноатлантичним альянсом. Потенціал експорту може становити кілька мільярдів доларів за умови відповідності західним стандартам. Стратегічно розвиток українського оборонного сектору виступає інвестицією у стійкість Європи, але для повної реалізації необхідна адаптація інституційних механізмів НАТО до більш гнучкої моделі інноваційного управління. Очевидним є те, що розвиток української оборонної бази пов'язаний з європейською обороноздатністю. Така залежність означає і взаємний ризик.

Модель "Інтеграційна піраміда ОПК України" підтверджує ієрархічну залежність факторів, де технологічна автономність слугує базисом для регуляторної гармонізації, а та – для міжнародного впливу. Ця конструкція є аналітичним внеском, що базується на синтезі емпірики, але визнає свої межі: в асиметричних конфліктах середнього масштабу вона ефективна. Проте в глобальних сценаріях вимагає доповнення факторами відновлення після війни.

Загалом, трансформація ОПК України не тільки відповідає на виклики російсько-української війни, але й переосмислює європейську безпеку, роблячи акцент на гібридності технологій та інституцій.

## Рекомендації

Для максимальної реалізації потенціалу ОПК України в контексті міжнародної безпеки першочергово варто продовжити гармонізацію стандартів виробництва з нормами Європейського Союзу та Північноатлантичного альянсу, зокрема через ініціативи на кшталт Defence Innovation Accelerator for the North Atlantic (DIANA), де бюджет у 1 млрд євро дозволяє прискорити спільні розробки.

Розширення програм спільного виробництва з державами-членами ЄС, з фокусом на ППО та дрони, стане логічним кроком, оскільки ППО, дрони та боєприпаси збільшеної дальності є ключовими оборонними пріоритетами України у 2026 році. Спрощення регуляторних процедур без послаблення експортного контролю дозволить підвищити конкурентоспроможність, хоча це вимагає балансу між швидкістю інновацій та безпековими стандартами, аби уникнути ризиків, подібних до невдач Stark Defence.

Збереження механізму бойового зворотного зв'язку як ключового інструменту ітерацій інновацій є критичним, оскільки саме зворотний зв'язок з фронту забезпечує адаптацію, роблячи український досвід уроком для НАТО.

Інвестування в модернізацію критичної інфраструктури як складової оборонної стратегії, з децентралізацією за рекомендаціями IEA "World Energy Outlook 2023", має стати пріоритетом для протидії кіберзагрозам і ескалації, інтегруючи це з НАТО для спільного моніторингу.

Посилення фокусу на ППО та дронах повинно супроводжуватися розвитком ракетних програм через державно-приватне партнерство. Розробка стратегій кіберзахисту, яка базується на ENISA "Threat Landscape 2023", з тренінгами для персоналу та інтеграцією штучного інтелекту з етичними стандартами, забезпечить превентивні заходи проти зростання інцидентів.

Проведення щорічного SWOT-аналізу ОПК України з моніторингом загроз дозволить адаптивно реагувати на динаміку, перетворюючи рекомендації на стратегічну рамку для довгострокового розвитку.

## Список використаних джерел


1. Залужний В. Про зміну характеру війни. *Українська правда.* 2026. URL: https://www.pravda.com.ua/columns/2026/02/23/8022301/ (дата звернення: 27.02.2026).
2. Sestanovich S. Securing Ukraine's Future in Europe: Ukraine's Defense Industrial Base as an Anchor for Economic Renewal and European Security. *Council on Foreign Relations.* 2025. URL: https://www.cfr.org/articles/securing-ukraines-future-in-europe-ukraines-defense-industrial-base-an-anchor-for-economic-renewal-and-european-security (дата звернення: 27.02.2026).
3. Krepinevich A. Cavalry to Computer: The Pattern of Military Revolutions. *The National Interest.* 1994. № 37. С. 30–42. URL: https://www.jstor.org/stable/42896863.
4. Murray W., Knox M. The Dynamics of Military Revolution 1300–2050. Cambridge : Cambridge University Press, 2001.
5. Freedman L. The Future of War: A History. London : Allen Lane, 2017.
6. Kaldor M. New and Old Wars: Organized Violence in a Global Era. Stanford : Stanford University Press, 2012.
7. Scharre P. Army of None: Autonomous Weapons and the Future of War. New York : W.W. Norton & Company, 2018.
8. Horowitz M. C. The Diffusion of Military Power: Causes and Consequences for International Politics. Princeton : Princeton University Press, 2010.
9. Trends in world military expenditure, 2023. *Stockholm International Peace Research Institute.* URL: https://www.sipri.org/publications/2023/sipri-fact-sheet/trends-world-military-expenditure-2023 (дата звернення: 27.02.2026). (Оновлено: дані 2024 в SIPRI Trends 2024).
10. Dickinson P., Kostyuk N. Ukrainian defense tech companies must prepare for export opportunities. *Atlantic Council.* 2025. URL: https://www.atlanticcouncil.org/blogs/ukrainealert/ukrainian-defense-tech-companies-must-prepare-for-export-opportunities/ (дата звернення: 27.02.2026).
11. Giles K. NATO can learn from Ukraine's military innovation. *Chatham House.* 2023. URL: https://www.chathamhouse.org/publications/the-world-today/2023-02/nato-can-learn-ukraines-military-innovation (дата звернення: 27.02.2026).
12. DroneXL. Peter Thiel-backed Stark Defence fails all four strikes. 2025. URL: https://dronexl.co/2025/10/31/peter-thiel-backed-stark-defence-fails-all-four-strikes/ (дата звернення: 27.02.2026).
13. Ukrainian Defence Associations Overview. *Security Assistance Hub.* 2024. URL: https://sahasec.org/policy-briefs/ukrainian-defence-associations-overview/ (дата звернення: 27.02.2026).
14. European Union Agency for Cybersecurity. *ENISA Threat Landscape* 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата звернення: 27.02.2026).

15. Defence Innovation Accelerator for the North Atlantic (DIANA). *NATO*. 2023. URL: https://www.nato.int/cps/en/natohq/topics_185166.htm (дата звернення: 27.02.2026).
16. "Очікую прориву в українській ракетній програмі". Прогнози українського deftech на 2026. *DOU.* 2026. URL: https://dou.ua/lenta/articles/deftech-forecasts-for-2026/ (дата звернення: 27.02.2026).
17. ППО, дрони та боєприпаси збільшеної дальності – названі ключові оборонні пріоритети України у 2026 році. *ArmyInform.* 2026. URL: https://armyinform.com.ua/2026/01/26/protypovitryana-oborona-drony-ta-boyeprypasy-zbilshenoyi-dalnosti-nazvani-klyuchovi-oboronni-priorytety-ukrayiny-u-2026-roczi/ (дата звернення: 27.02.2026).
18. Указ Президента України "Про Рішення Ради національної безпеки і оборони України від 22 листопада 2025 року "Про Міжвідомчу комісію з питань військово-промислової політики та оборонних технологій". *Офіційне інтернет-представництво Президента України*. 2026. Указ № 116/2026. URL: https://www.president.gov.ua/documents/1162026-58317 (дата звернення: 02.03.2026).
19. Технології фронту: найперспективніші інвестиційні напрями у 2026. *IT Arena*. 2026. URL: https://itarena.ua/ua/tehnologi%d1%97-frontu-najperspektivnishi-investiczijni-napryami-u-2026/ (дата звернення: 27.02.2026).
20. Гурковський В., Романенко Є., Коваль В., Ільницький С. Форсайт-дослідження як інструмент зміцнення резильєнтності до загроз БПЛА з оптоволоконним управлінням. *Національні інтереси України*. 2025. №7 (12). URL: https://perpectives.pp.ua /index.php/niu/view/26219. DOI: https://doi.org /10.52058/3041-1793-2025-7(12)-88-101 (дата звернення: 02.03.2026).
21. The 2022-2023 Russia-Ukraine War and Cyberspace Threats. *ResearchGate*. 2023. URL: https://www.researchgate.net/publication/373855591_The_2022-2023_Russia-Ukraine_War_and_ Cyberspace_Threats (дата звернення: 27.02.2026).
22. Modern cyber threats to critical infrastructure in Ukraine and the world. *ResearchGate.* 2025. URL: https://www.researchgate.net/publication/390394323_MODERN_CYBER_THREATS_TO_CRITICAL_INFRASTRUCTURE_IN_UKRAINE_AND_THE_WORLD (дата звернення: 27.02.2026).
23. EU policymakers expect no immediate oil security impact from Iran conflict, email shows. *Reuters.* March 2, 2026. URL: https://www.reuters.com/business/energy/eu-policymakers-expect-no-immediate-oil-security-impact-iran-conflict-email-2026-03-02 (дата звернення: 02.03.2026).
24. The Regional Reverberations of the U.S. and Israeli Strikes on Iran. *CSIS.* March 1, 2026. URL: https://www.csis.org/analysis/regional-reverberations-us-and-israeli-strikes-iran (дата звернення: 02.03.2026).
25. IAEA Director General's Introductory Statement to the Extraordinary Board of Governors. *IAEA.* March 2, 2026. URL: https://www.iaea.org/newscenter/statements/iaea-director-generals-introductory-statement-to-the-board-of-governors-2-march-2026 (дата звернення: 02.03.2026).
26. Countering cyber threats to Ukraine's national security: institutional and preventive capability. *ResearchGate*. 2026. URL: https://www.researchgate.net/publication/400373357_Countering_ cyber_threats_to_Ukraine's_national_security_institutional_and_preventive_capability (дата звернення: 27.02.2026).
27. National Resilience of Ukraine: Content and Security Strategy in the Context of a War and Post-war Recovery. *ResearchGate*. 2025. URL: https://www.researchgate.net/publication/393564415_ National_Resilience_of_Ukraine_Content_and_Security_Strategy_in_the_Context_of_a_War_and_Post-war_Recovery (дата звернення: 27.02.2026).
28. World Energy Outlook 2023. *IEA.* URL: https://www.iea.org/reports/world-energy-outlook-2023 (дата звернення: 27.02.2026).
29. Defence Data 2023-2024. *European Defence Agency.* 2024. URL: https://eda.europa.eu/docs/default-source/brochures/eda-defence-data-2023.pdf (дата звернення: 27.02.2026).
30. European defense by the numbers. *McKinsey.* 2026. URL: https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/european-defense-by-the-numbers (дата звернення: 27.02.2026).
31. EU Defence Industry Transformation Roadmap. *EU Commission.* 2025. URL: https://defence-industry-space.ec.europa.eu/document/download/513de692-d08c-40cc-80c3-cb6611ace178_en?filename=EU-Defence-Industry-Transformation-Roadmap.pdf (дата звернення: 27.02.2026).

## References

1. Zaluzhnyi, V. (2026). Pro zminu kharakteru viiny [On the changing nature of war]. *Ukrainska pravda.* Retrieved from: https://www.pravda.com.ua/columns/2026/02/23/8022301/ (accessed 27.02.2026) [in Ukrainian].
2. Sestanovich, S. (2025). Securing Ukraine's Future in Europe: Ukraine's Defense Industrial Base as an Anchor for Economic Renewal and European Security. *Council on Foreign Relations*. Retrieved from:

https://www.cfr.org/articles/securing-ukraines-future-in-europe-ukraines-defense-industrial-base-an-anchor-for-economic-renewal-and-european-security (accessed 27.02.2026).
3. Krepinevich, A. (1994). Cavalry to Computer: The Pattern of Military Revolutions. *The National Interest*, 37, 30–42. Retrieved from: https://www.jstor.org/stable/42896863.
4. Murray, W., & Knox, M. (2001). The Dynamics of Military Revolution 1300–2050. Cambridge: Cambridge University Press.
5. Freedman, L. (2017). The Future of War: A History. London: Allen Lane.
6. Kaldor, M. (2012). New and Old Wars: Organized Violence in a Global Era. Stanford: Stanford University Press
7. Scharre, P. (2018). Army of None: Autonomous Weapons and the Future of War. New York: W.W. Norton & Company.
8. Horowitz, M. C. (2010). The Diffusion of Military Power: Causes and Consequences for International Politics. Princeton : Princeton University Press.
9. Trends in world military expenditure. (2023). *Stockholm International Peace Research Institute*. Retrieved from: https://www.sipri.org/publications/2023/sipri-fact-sheet/trends-world-military-expenditure-2023 (accessed 27.02.2026).
10. Dickinson, P., & Kostyuk, N. (2025). Ukrainian defense tech companies must prepare for export opportunities. *Atlantic Council.* Retrieved from: https://www.atlanticcouncil.org/blogs/ukrainealert/ukrainian-defense-tech-companies-must-prepare-for-export-opportunities/ (accessed 27.02.2026).
11. Giles, K. (2023). NATO can learn from Ukraine's military innovation. *Chatham House*. Retrieved from: https://www.chathamhouse.org/publications/the-world-today/2023-02/nato-can-learn-ukraines-military-innovation (accessed 27.02.2026).
12. DroneXL. (2025). Peter Thiel-backed Stark Defence fails all four strikes. Retrieved from: https://dronexl.co/2025/10/31/peter-thiel-backed-stark-defence-fails-all-four-strikes/ (accessed 27.02.2026).
13. Ukrainian Defence Associations Overview. (2024). *Security Assistance Hub.* Retrieved from: https://sahasec.org/policy-briefs/ukrainian-defence-associations-overview/ (accessed 27.02.2026).
14. European Union Agency for Cybersecurity. (2023). *ENISA Threat Landscape.* Retrieved from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (accessed 27.02.2026).
15. Defence Innovation Accelerator for the North Atlantic (DIANA). (2023). *NATO*. Retrieved from: https://www.nato.int/cps/en/natohq/topics_185166.htm (accessed 27.02.2026).
16. "Ochikuiu proryvu v ukrainskii raketnii prohrami". Prohnozy ukrainskoho deftech na 2026 ["I expect a breakthrough in the Ukrainian missile program." Ukrainian deftech forecasts for 2026]. (2026). *DOU*. Retrieved from: https://dou.ua/lenta/articles/deftech-forecasts-for-2026/ (accessed 27.02.2026) [in Ukrainian].
17. PPO, drony ta boieprypasy zbilshenoi dalnosti – nazvani kliuchovi oboronni priorytety Ukrainy u 2026 rotsi [Air defense, drones and extended-range ammunition – Ukraine's key defense priorities in 2026 named]. (2026). *ArmyInform.* Retrieved from: https://armyinform.com.ua/2026/01/26/protypovitryana-oborona-drony-ta-boyeprypasy-zbilshenoyi-dalnosti-nazvani-klyuchovi-oboronni-priorytety-ukrayiny-u-2026-roczi/ (accessed 27.02.2026) [in Ukrainian].
18. Ukaz Prezydenta Ukrainy "Pro Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 22 lystopada 2025 roku "Pro Mizhvidomchu komisiiu z pytan viiskovo-promyslovoi polityky ta oboronnykh tekhnolohii" [Decree of the President of Ukraine "On the Decision of the National Security and Defense Council of Ukraine dated November 22, 2025 "On the Interdepartmental Commission on Military-Industrial Policy and Defense Technologies"]. (2026). *Ofitsiine internet-predstavnytstvo Prezydenta Ukrainy*. Ukaz № 116/2026. Retrieved from: https://www.president.gov.ua/documents/1162026-58317 (accessed 02.03.2026) [in Ukrainian].
19. Tekhnolohii frontu: naiperspektyvnishi investytsiini napriamy u 2026 [Front-end technologies: the most promising investment directions in 2026]. (2026). *IT Arena*. Retrieved from: https://itarena.ua/ua/tehnologi%d1%97-frontu-najperspektivnishi-investiczijni-napryami-u-2026/ (accessed 27.02.2026) [in Ukrainian].
20. Hurkovskyi, V., Romanenko, Ye., Koval, V., & Ilnytskyi, S. (2025). Forsait-doslidzhennia yak instrument zmitsnennia rezylientnosti do zahroz BPLA z optovolokonnym upravlinniam [Foresight research as a tool for strengthening resilience to fiber-optic-controlled UAV threats]. *Natsionalni interesy Ukrainy*, 7 (12), 88-101. Retrieved from: https://perpectives.pp.ua /index.php/niu/view/26219. DOI: https://doi.org /10.52058/3041-1793-2025-7(12)-88-101 (accessed 02.03.2026) [in Ukrainian].
21. The 2022-2023 Russia-Ukraine War and Cyberspace Threats. (2023). *ResearchGate*. Retrieved from: https://www.researchgate.net/publication/373855591_The_2022-2023_Russia-Ukraine_War_and_Cyberspace_Threats (accessed 27.02.2026).
22. Modern cyber threats to critical infrastructure in Ukraine and the world. (2025). *ResearchGate.* Retrieved from:

https://www.researchgate.net/publication/390394323_MODERN_CYBER_THREATS_TO_CRITICAL_INFRASTRUCTURE_IN_UKRAINE_AND_THE_WORLD (accessed 27.02.2026).
23. EU policymakers expect no immediate oil security impact from Iran conflict, email shows. (March 2, 2026). *Reuters.* Retrieved from: https://www.reuters.com/business/energy/eu-policymakers-expect-no-immediate-oil-security-impact-iran-conflict-email-2026-03-02 (accessed 02.03.2026).
24. The Regional Reverberations of the U.S. and Israeli Strikes on Iran. (March 1, 2026). *CSIS*. Retrieved from: https://www.csis.org/analysis/regional-reverberations-us-and-israeli-strikes-iran (accessed 02.03.2026).
25. IAEA Director General's Introductory Statement to the Extraordinary Board of Governors. (March 2, 2026). *IAEA.* Retrieved from: https://www.iaea.org/newscenter/statements/iaea-director-generals-introductory-statement-to-the-board-of-governors-2-march-2026 (accessed 02.03.2026).
26. Countering cyber threats to Ukraine's national security: institutional and preventive capability. (2026). *ResearchGate*. Retrieved from: https://www.researchgate.net/publication/400373357_Countering_cyber_threats_to_Ukraine's_national_security_institutional_and_preventive_capability (accessed 27.02.2026).
27. National Resilience of Ukraine: Content and Security Strategy in the Context of a War and Post-war Recovery. (2025). *ResearchGate*. Retrieved from: https://www.researchgate.net/publication/393564415_National_Resilience_of_Ukraine_Content_and_Security_Strategy_in_the_Context_of_a_War_and_Post-war_Recovery (accessed 27.02.2026).
28. World Energy Outlook 2023. *IEA.* Retrieved from: https://www.iea.org/reports/world-energy-outlook-2023 (accessed 27.02.2026).
29. Defence Data 2023-2024. (2024). *European Defence Agency*. Retrieved from: https://eda.europa.eu/docs/default-source/brochures/eda-defence-data-2023.pdf (accessed 27.02.2026).
30. European defense by the numbers. (2026). *McKinsey*. Retrieved from: https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/european-defense-by-the-numbers (accessed 27.02.2026).
31. EU Defence Industry Transformation Roadmap. (2025). *EU Commission.* Retrieved from: https://defence-industry-space.ec.europa.eu/document/download/513de692-d08c-40cc-80c3-cb6611ace178_en?filename=EU-Defence-Industry-Transformation-Roadmap.pdf (accessed 27.02.2026).

*Received 18.03.2026 | Accepted 25.03.2026 | Published 30.03.2026*



УДК 341.24:355.45(73+477) DOI: 10.63978/3083-6476.2026.1.4.02

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

**Моцик Олександр Федорович**
*кандидат політичних наук*
*Надзвичайний і Повноважний Посол України в США (2010–2015 рр.)*
*Київ, Україна*
*ORCID: 0000-0003-0233-0815*

# ТЕРИТОРІАЛЬНІ КОМПРОМІСИ ЩОДО УКРАЇНИ У ЗОВНІШНІЙ ПОЛІТИЦІ США: ПРАВОВЕ ЗНАЧЕННЯ ЗАКОНУ CAATSA №115-44 ДЛЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

***Анотація.*** *В цій статті здійснюється комплексний аналіз правових обмежень територіальних компромісів щодо України у зовнішній політиці США через призму дії Закону Countering America's Adversaries Through Sanctions Act (CAATSA) №115-44. На основі системного та міждисциплінарного підходу досліджено юридичну природу закону, його місце в системі федерального права США та значення для захисту суверенітету й територіальної цілісності України.*

*Особливу увагу приділено розділу 257 CAATSA, який кодифікує принцип невизнання будь-яких територіальних змін, здійснених силою, і фактично інституціоналізує політику підтримки України. Розкрито взаємодію між Конгресом і виконавчою владою США, що обмежує дискреційні повноваження президента у сфері санкцій та унеможливлює легалізацію територіальних поступок росії. Методологічну основу становлять формально-юридичний, інституційний, історико-порівняльний та підхід стратегічних студій, що дозволяє поєднати правовий аналіз з оцінкою безпекових наслідків. Простежено еволюцію доктрини невизнання – від формулювання Генрі Стімсона у 1932 році до її законодавчого закріплення у CAATSA.*

*Наукова новизна полягає у тлумаченні CAATSA не лише як санкційного, а й як безпекового акта, що створює для України правовий щит проти політичних компромісів типу «мир в обмін на території». Обґрунтовано необхідність інтеграції норм CAATSA в систему зовнішньополітичного планування України та використання їх у міжнародно-правових і дипломатичних аргументаціях.*

***Ключові слова:*** *CAATSA; зовнішня політика США; суверенітет України; територіальна цілісність; санкції; Конгрес США; невизнання анексій; національна безпека; доктрина Стімсона; державне управління.*

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

**Oleksandr Motsyk**
*Candidate of Political Sciences*
*Ambassador Extraordinary and Plenipotentiary of Ukraine to the United States (2010–2015)*
*Kyiv, Ukraine*
*ORCID: 0000-0003-0233-0815*

# TERRITORIAL COMPROMISES ON UKRAINE IN U.S. FOREIGN POLICY: THE LEGAL IMPLICATIONS OF CAATSA (PUBLIC LAW 115-44) FOR UKRAINE'S NATIONAL SECURUTY

***Abstract.*** *This article offers a comprehensive analysis of the legal constraints on territorial compromises regarding Ukraine within U.S. foreign policy, viewed through the lens of the Countering America's Adversaries Through Sanctions Act (CAATSA), Public Law 115-44. Employing an interdisciplinary methodology that integrates formal-legal, institutional, historical-comparative, and strategic-security approaches, the study examines the legal character of CAATSA, its place within the U.S. federal statutory framework, and its direct implications for protecting Ukraine's sovereignty and territorial integrity. Special attention is devoted to Section 257, which codifies the U.S. policy of non-recognition of any territorial alterations achieved by force and institutionalizes sustained support for Ukraine. The research highlights the constitutional checks and balances between Congress and the executive branch, demonstrating how legislative oversight severely limits presidential discretion in sanctions policy and precludes the legitimization of territorial concessions to Russia.*

*The article traces the evolution of the non-recognition principle from the 1932 Stimson Doctrine to its binding legislative embodiment in CAATSA. Its scientific novelty consists in reinterpreting CAATSA not merely as a sanctions statute but as a robust security instrument that functions as a legal shield for Ukraine against "peace-for-territory" scenarios. The study concludes that systematic integration of CAATSA provisions into Ukrainian diplomacy and public-administration planning can transform this U.S. law into a proactive tool of national security and international deterrence.*

***Keywords:*** *CAATSA; U.S. foreign policy; Ukraine's sovereignty; territorial integrity; sanctions; U.S. Congress; non-recognition policy; national security; Stimson Doctrine; public administration.*

**JEL Classification:** F51, F52, K33, H56

## Вступ

Проблематика територіальної цілісності України в умовах повномасштабної збройної агресії російської федерації дедалі частіше виходить за межі традиційного міжнародно-правового дискурсу, набуваючи вимірів внутрішньополітичних обмежень та правових детермінант зовнішньої політики держав-партнерів. У публічному просторі західних країн від політичних дебатів до експертних коментарів періодично з'являються наративи, що допускають можливість "мирного врегулювання" через територіальні поступки. Ці підходи апелюють до реалістичних чи прагматичних міркувань політичної

доцільності, проте часто ігнорують фундаментальний аспект – діюче внутрішнє законодавство основних союзників України, передусім Сполучених Штатів Америки.

Станом на березень 2026 року, коли Сполучені Штати та Ізраїль проводять масштабну військову кампанію проти Ірану, а іранські удари у відповідь по об'єктах у Перській затоці та закриття Ормузької протоки спричинили глобальну енергетичну турбулентність, Конгрес США демонструє жорсткий контроль за дотриманням CAATSA. Демократичні лідери Сенату публічно вимагають від адміністрації Трампа дотримання процедурного порядку (Sec. 216 та 230) щодо будь-яких послаблень санкцій проти росії, навіть якщо вони мотивовані необхідністю стабілізувати світові ціни на нафту через іранську кризу. Цей приклад яскраво ілюструє, що внутрішнє законодавство США не дозволяє виконавчій владі односторонньо легітимізувати територіальні чи санкційні компроміси з агресорами – принцип, який діє однаково щодо росії в Україні та щодо Ірану в Близькосхідному регіоні. Саме тому наративи "мир в обмін на території" щодо України не є лише політичними спекуляціями, а суперечать чинному федеральному праву.

США залишаються системним і провідним актором у глобальній архітектурі безпеки, найбільшим донором оборонної допомоги Україні та ініціатором міжнародної санкційної коаліції проти агресора. Водночас американська зовнішня політика не є виключно персоніфікованою чи залежною від політичної волі конкретної адміністрації. Її зміст і спрямованість обмежені конституційними механізмами стримувань і противаг, провідною роллю Конгресу, а також чітко кодифікованими нормами федерального права. У цьому контексті Закон США "Про протидію супротивникам Америки за допомогою санкцій" (Countering America's Adversaries Through Sanctions Act – CAATSA, №115-44), ухвалений у 2017 році, набуває стратегічного значення для національної безпеки України [1; 2].

Зокрема, розділ 257 CAATSA, формально присвячений питанням енергетичної безпеки України, закріплює більш широкий політико-правовий принцип – невизнання будь-яких територіальних змін України, здійснених шляхом застосування сили. Ця норма, інтегрована до Зводу законів США, зберігає чинність станом на 2026 рік, що підтверджується офіційними урядовими джерелами [2; 3-4; 5]. Вона не має декларативного характеру та не є тимчасовим політичним сигналом. Йдеться про імперативну норму федерального законодавства, порушення якої тягне за собою інституційні та персональні наслідки.

Актуальність цього дослідження зумовлена недостатнім системним використанням потенціалу CAATSA у практиці державного управління та зовнішньої політики України. Часто міжнародні переговори інтерпретуються у Києві як сфера "політичної гнучкості", де допустимі компроміси щодо стратегічних питань. Такий підхід створює вразливість до нав'язаних сценаріїв та інформаційних маніпуляцій. Натомість науковий і практичний аналіз CAATSA як правового ресурсу захисту національних інтересів дозволяє перевести українську дипломатію з реактивного у проактивний формат – від реагування на зовнішній тиск до використання американського законодавства як інструменту захисту власного суверенітету.

## Постановка проблеми

У сучасному геополітичному контексті, коли в міжнародному публічному просторі дедалі частіше лунають пропозиції "миру в обмін на території", особливо щодо російсько-української війни, постає фундаментальна проблема ігнорування чинних правових норм, що регламентують зовнішню політику провідних демократичних держав. Йдеться не лише про політичні принципи чи моральні зобов'язання, а про конкретні положення внутрішнього права, що мають імперативний характер. Законодавство Сполучених Штатів Америки містить пряму заборону визнавати будь-які територіальні зміни України, здобуті внаслідок збройної агресії Російської Федерації. Ця норма закріплена в Законі "Про

протидію противникам Америки за допомогою санкцій" (Countering America's Adversaries Through Sanctions Act, CAATSA, Public Law 115-44), ухваленому 2 серпня 2017 року. Вона має силу федерального закону, тобто є обов'язковою для всіх гілок влади США, і не може бути змінена або обійдена рішеннями виконавчої влади без погодження з Конґресом. З юридичного погляду, будь-які "територіальні компроміси" щодо України суперечили б чинному праву Сполучених Штатів.

Проблема, однак, полягає не лише в існуванні таких правових обмежень, а й у відсутності системного використання цього інструменту українською стороною. Незважаючи на потенціал CAATSA як легітимної правової основи для захисту суверенітету, у практиці дипломатичних переговорів Україна здебільшого спирається на політичні декларації, а не на конкретні норми американського законодавства. Такий підхід обмежує ефективність зовнішньополітичних дій і не дозволяє повною мірою використовувати правові важелі союзників.

Історичний досвід свідчить, що принципи невизнання територіальних змін, здобутих силою, мають глибоке коріння в міжнародному праві. Їхній еволюційний шлях – від доктрини Стімсона, сформульованої у відповідь на японську агресію в Маньчжурії у 1931–1932 роках, до сучасних законодавчих норм, закріплених у CAATSA, демонструє трансформацію політичних декларацій у юридично зобов'язувальні норми. Ігнорування цих історичних прецедентів звужує розуміння правового змісту сучасної політики невизнання і послаблює аргументаційну базу України у міжнародному правовому полі.

Додатковим ускладнювальним чинником виступає існування неформальних каналів переговорів і так званої "тіньової дипломатії", коли до процесів врегулювання залучаються особи без офіційного мандата. Такі ініціативи нерідко подаються як політичні або гуманітарні, але фактично створюють ризики обходу законодавчих обмежень, передусім тих, що випливають із ролі Конґресу у формуванні зовнішньої політики США [6; 7]. Подібна практика підриває довіру до інституційної архітектури західних демократій і створює ілюзію гнучкості там, де насправді існують жорсткі правові межі.

Актуальність проблеми полягає у потребі переосмислити CAATSA не лише як інструмент санкційної політики проти агресора, а як чинник, що формує рамки американської політики невизнання і тим самим забезпечує фундаментальну підтримку територіальної цілісності України. Усвідомлення цього дозволяє перевести українську дипломатію з позиції прохача до позиції рівноправного учасника партнерських відносин, який оперує спільною правовою базою, а не лише політичними закликами.

## Огляд літератури

Аналіз сучасного наукового та аналітичного дискурсу свідчить про зростання інтересу до ролі внутрішнього законодавства держав у забезпеченні міжнародної безпеки. Водночас виявляється помітний дефіцит досліджень, які безпосередньо пов'язують ці правові норми з національними інтересами України, зокрема у контексті дії Закону CAATSA.

У працях провідних американських правників, конституціоналістів та фахівців із міжнародного права CAATSA розглядається насамперед як інструмент посилення ролі Конґресу у зовнішній політиці США та механізм обмеження дискреційних повноважень президента [6]. Автори підкреслюють, що ухвалення цього закону стало відповіддю на намагання виконавчої влади зменшити санкційний тиск без належного парламентського контролю. Таким чином, CAATSA постає не лише санкційним актом, а й проявом американського конституціоналізму, що гарантує сталість зовнішньополітичного курсу незалежно від зміни адміністрацій. Український вимір у цих роботах переважно згадується побіжно, без системного аналізу наслідків для безпеки України.

Значний масив аналітичних матеріалів провідних think tank, зокрема Center for Strategic and International Studies (CSIS) та Foundation for Defense of Democracies (FDD),

фокусується на CAATSA як інструменті стратегічного стримування російської федерації та підтримки євроатлантичної безпеки [7; 8]. У цих дослідженнях наголошується, що положення про невизнання анексії Криму мають довготривалий характер і не залежать від політичних циклів у Вашингтоні. Проте навіть ці ґрунтовні аналітичні огляди рідко розглядають закон як активний ресурс української дипломатії, зосереджуючись переважно на американській внутрішньополітичній логіці санкційного режиму.

У дослідженнях Stockholm International Peace Research Institute (SIPRI) санкційна політика США розглядається як складова ширшої системи економічних та інституційних інструментів міжнародної безпеки [9]. Наголос робиться на тому, що ефективність санкцій прямо залежить від їхньої правової стабільності, передбачуваності та підтримки на рівні законодавчих органів. У цьому контексті CAATSA оцінюється як зразок нормативної послідовності, що забезпечує стійкість санкційної архітектури навіть у разі політичних змін.

Особливу увагу варто приділити офіційним документам урядових структур США – насамперед Міністерства фінансів (Office of Foreign Assets Control, OFAC) та Державного департаменту, які систематично оновлюють інформацію щодо реалізації CAATSA [4; 5]. Ці джерела підтверджують, що положення закону діють на постійній основі, охоплюючи як санкційні обмеження проти суб'єктів, пов'язаних із російським оборонним сектором, так і підтримку енергетичної незалежності України. CAATSA набуває ознак інституційно стабільного інструмента, інтегрованого в американську стратегічну систему безпеки США.

В українській науковій та аналітичній літературі санкційна тематика висвітлюється переважно в рамках загального аналізу міжнародного права, політичної безпеки та гібридних загроз [18]. Однак детальні дослідження CAATSA як складової зовнішнього контуру національної безпеки України наразі майже відсутні. Ця лакуна в науковому дискурсі створює потребу в переосмисленні підходів до інтеграції правових механізмів союзників у систему стратегічного прогнозування нашої держави.

Підсумовуючи, можна констатувати: наявна наукова й аналітична база – від американських конституціоналістів до європейських безпекових досліджень формує вагоме підґрунтя для подальшого осмислення CAATSA. Проте український контекст досі залишається периферійним у цих дослідженнях. Саме тому необхідним є перехід від пасивного сприйняття CAATSA як "зовнішнього" інструменту до активного використання його потенціалу в практиці державного управління та дипломатії України.

## Мета та завдання статті

Метою статті є визначити правове значення Закону Сполучених Штатів Америки "Про протидію супротивникам Америки за допомогою санкцій" (CAATSA) №115-44, насамперед розділу 257, як інструменту обмеження територіальних компромісів щодо України в зовнішній політиці США. Дослідження зосереджується на тому, що цей закон закріплює політику невизнання будь-яких територіальних змін, здійснених силою, і створює реальні механізми стримування виконавчої влади, а також на можливостях його використання в українському зовнішньополітичному плануванні та дипломатичниій практиці.

У межах поставленої мети прагнемо виявити, яким чином внутрішнє право США формує обов'язкові обмеження для виконавчої влади щодо можливих територіальних компромісів, та оцінити потенціал використання цього законодавчого ресурсу в системі української дипломатії й державного управління. Дослідження інтегрує правовий, історичний і безпековий підходи, розглядаючи CAATSA як сучасну форму втілення доктрини невизнання анексій, започаткованої ще Генрі Стімсоном у 1932 році.

Гіпотеза дослідження полягає у твердженні, що чинне внутрішнє законодавство США, зокрема CAATSA, створює не лише юридичну заборону на визнання територіальних втрат України, але й потенціал для проактивного використання цього акта як елемента

зовнішньополітичної стратегії України. За умови системного, інституціоналізованого застосування норм CAATSA у дипломатичній практиці Україна може істотно знизити ризики нав'язаних політичних компромісів і зміцнити власні переговорні позиції без створення напруженості у відносинах із партнерами.

Наукова новизна дослідження полягає в розширеному тлумаченні CAATSA як елементу не лише санкційної, а й безпекової політики США, що формує зовнішній контур національної безпеки України. Уперше на українському науковому рівні CAATSA розглядається як інструмент інтеграції внутрішнього права стратегічного союзника у власну систему державного управління та зовнішньополітичного планування. Такий підхід відкриває можливість для формування нової моделі дипломатичної взаємодії, заснованої на спільних правових засадах, а не лише на політичній кон'юнктурі.

## Методи

Методологічна база даного дослідження побудована на поєднанні формально-правового, інституційного, історико-політичного та стратегічно-аналітичного підходів, що дозволяє поєднати юридичну точність з оцінкою практичних наслідків для державного управління та національної безпеки України.

Формально-юридичний метод виступає центральним інструментом дослідження. Він застосовується для аналізу правової природи CAATSA, її місця в системі федерального законодавства США, механізмів правозастосування та ступеня обов'язковості для виконавчої влади [1; 2]. Особлива увага приділяється кодифікаційним аспектам, процедурним нормам і юридичним наслідкам порушення положень закону.

Інституційний підхід дозволяє розглядати CAATSA як прояв системи "стримувань і противаг" у державному механізмі США, де Конґрес не лише ухвалює закони, а й виступає активним суб'єктом формування зовнішньої політики, накладаючи правові обмеження на дискреційні повноваження президента [6; 7]. У цьому контексті проаналізовано взаємодію Державного департаменту, Міністерства фінансів і Білого дому у сфері санкційної політики, а також роль Конґресу у забезпеченні її неперервності.

Метод стратегічних студій і досліджень національної безпеки використано для розгляду CAATSA як інструменту надійного стримування у ширшій архітектурі безпеки Заходу. Закон оцінюється не лише як реакція на російську агресію, а як частина системної відповіді на ревізіоністські практики держав, що порушують міжнародний правопорядок [8; 9]. Такий підхід дозволяє інтегрувати юридичний аналіз у площину безпекової політики.

Метод аналізу публічної політики застосовується для дослідження механізмів, через які правові норми трансформуються у практичні політичні рішення, та для виявлення розривів між наявним нормативним потенціалом і реальною дипломатичною практикою України. Особлива увага приділяється дослідженням провідних аналітичних центрів – CSIS, FDD, SIPRI, які спеціалізуються на питаннях санкційної політики, енергетичної безпеки та гібридних загроз [10–17].

Варто підкреслити, що дослідження свідомо не торкається неформальних дипломатичних домовленостей чи закритих переговорних процесів. Об'єктом аналізу є норми права, офіційні інституційні механізми та відкриті аналітичні джерела. Такий підхід забезпечує не лише академічну достовірність, але й практичну релевантність для органів державної влади України.

## Результати

Закон США Countering America's Adversaries Through Sanctions Act (CAATSA) №115-44 посідає центральне місце в сучасній архітектурі американської санкційної політики, спрямованої на стримування агресивних дій росії, зокрема проти України. Прийнятий Конґресом із переважною підтримкою (419 голосів "за" проти 3 у Палаті

представників та 98 проти 2 у Сенаті), цей закон став не лише реакцією на агресію рф, Ірану й Північної Кореї, а й кодифікацією принципу невизнання територіальних змін, здобутих силою [1; 2]. Фактично CAATSA трансформував політику невизнання з декларативного дипломатичного підходу в імперативну правову норму, що обмежує дискреційні повноваження виконавчої влади США.

Для України цей закон має подвійне значення. По-перше, він безпосередньо пов'язує санкції з відновленням суверенітету та територіальної цілісності нашої держави. По-друге, він створює юридичний щит, який перешкоджає легітимізації будь-яких форм територіальних компромісів.

CAATSA має статус публічного закону (Public Law 115-44), що забезпечує його обов'язковість для всіх гілок влади Сполучених Штатів. Його структура складається з трьох титулів, однак для України першорядного значення набуває Титул II – "Countering Russian Influence in Europe and Eurasia". Саме тут кодифіковано правові механізми, що унеможливлюють зняття або пом'якшення санкцій проти рф без схвалення Конґресу. Наприклад, розділ 216 передбачає обов'язкове узгодження будь-яких рішень про зміну санкційного режиму з обома палатами парламенту [2]. Такий підхід істотно обмежує виконавчу дискрецію президента США: жодна адміністрація не може самостійно зняти санкції чи визнати територіальні зміни без попереднього схвалення Конґресом. (див.також Lawfare, 24.04.2025; Carnegie Politika 27.03.2025). З точки зору захисту суверенітету України це означає наявність додаткового політико-правового бар'єра проти спроб легалізувати окупацію Криму чи східних регіонів.

Особливої уваги заслуговує розділ 253, який закріплює принцип ex injuria jus non oritur – "з неправомірної дії не виникає права". У цьому положенні закону США офіційно підтверджують невизнання будь-яких територіальних змін, здійснених силою, включно з незаконними окупаціями Абхазії, Південної Осетії, Криму, східної України та Придністров'я [1; 2]. Доктрина Стімсона, сформульована ще у 1932 році, знайшла своє сучасне законодавче втілення. Цей розділ не є декларацією доброї волі – він містить юридичне зобов'язання для виконавчих органів влади США дотримуватися політики невизнання в усіх зовнішньополітичних рішеннях.

Для повного розуміння природи CAATSA важливо звернутися до історичного контексту формування принципів невизнання. Відлік бере свій початок із Мукденського інциденту 1931 року, який став прецедентом японської агресії проти Китаю та безпосередньо стимулював появу доктрини Стімсона. Тоді японські військові сили, що контролювали Південно-Маньчжурську залізницю, інсценували вибух колії біля міста Мукден (нині Шеньян), звинувативши в цьому китайських націоналістів. Інцидент став приводом для швидкої окупації Маньчжурії та створення маріонеткової держави Маньчжоу-Го.

У січні 1932 року державний секретар США Генрі Стімсон видав ноту, яка оголосила невизнання будь-яких угод чи змін, що порушують міжнародні зобов'язання або права інших держав. В офіційному формулюванні зазначалося: "The United States will not recognize any treaty or agreement between Japan and China which violates the rights of the United States or the obligations under international agreements" [22]. Доктрина, відома як "Стімсонова", започаткувала нову епоху в міжнародному праві – епоху юридичного невизнання результатів агресії.

Хоча короткостроково доктрина Стімсона не зупинила японську експансію, її довготривалі наслідки виявилися визначальними. Вона заклала підвалини принципу, який пізніше був закріплений у Статуті ООН, зокрема у статті 2(4), що забороняє застосування сили, та у статті 2(7), яка зобов'язує держави утримуватися від визнання ситуацій, створених унаслідок порушення цього принципу. Історичний досвід Маньчжурії показав, що навіть без негайного примусу політика невизнання з часом підриває легітимність агресора й зберігає підвалини міжнародного правопорядку.

Саме на цьому історичному фундаменті ґрунтується CAATSA. Закон кодифікує політику невизнання анексії Криму та окупації частини української території, надаючи їй обов'язковий характер у межах американської правової системи. Зокрема, розділ 257 формулює офіційну політику США таким чином:

"It is the policy of the United States – (1) to support the Government of Ukraine in restoring its sovereignty and territorial integrity; … (3) to never recognize the illegal annexation of Crimea by the Government of the Russian Federation or the separation of any portion of Ukrainian territory through the use of military force" [1]. ("Політика Сполучених Штатів полягає в тому, щоб: (1) підтримувати уряд України у відновленні її суверенітету та територіальної цілісності; … (3) ніколи не визнавати незаконну анексію Криму урядом російської федерації або відокремлення будь-якої частини української території шляхом застосування військової сили").

Хоча Sec. 257 є "statement of policy" (не жорсткою забороною), у поєднанні з вимогами Sec. 216 та 230 щодо конгресового контролю за санкціями це створює значні практичні бар'єри для виконавчої влади (див. Anderson, Lawfare, 2025).

CAATSA перетворює принцип невизнання на юридично зобов'язувальну норму, яка зв'язує дії Державного департаменту, Міністерства фінансів, USAID та інших структур виконавчої влади. Закон прямо зобов'язує ці інституції розробляти та впроваджувати програми підтримки енергетичної незалежності України, що, у свою чергу, зміцнює її національну безпеку [4].

CAATSA посідає системоутворююче місце серед інших американських законодавчих актів, зокрема Ukraine Freedom Support Act of 2014 (Public Law 113-272) [17]. Він не лише продовжує санкційну лінію, а й робить її невідворотною, кодифікуючи президентські укази (Executive Orders 13660–13662) у форму закону. Цим самим CAATSA позбавляє адміністрацію можливості односторонньо змінювати санкційний режим без згоди Конґресу, забезпечуючи сталість підтримки України навіть у разі зміни політичного керівництва. Конгрес може внести поправки або ухвалити новий закон, який змінює CAATSA.

Для нашої держави правове значення CAATSA виходить далеко за межі формального захисту. Закон не лише створює правові бар'єри проти спроб нормалізувати окупацію, а й надає Києву інструмент дипломатичного тиску. Його положення можуть використовуватися як аргумент у переговорах із західними партнерами, наголошуючи, що будь-які ініціативи "мирного врегулювання" через поступки територіями суперечать американському законодавству й, не можуть бути підтримані навіть теоретично.

У цьому сенсі CAATSA є не просто інструментом санкцій, а складовою архітектури стратегічного стримування, що гарантує стабільність правового середовища, у якому українська територіальна цілісність залишається юридично недоторканною. Саме тому для української дипломатії надзвичайно важливо переходити від емоційної апеляції до "моральної підтримки" до фахового оперування правовими нормами союзника. Акцент на правовій природі CAATSA дозволяє не лише зміцнити переговорну позицію, а й відновити баланс між політичною риторикою та правовими гарантіями.

На думку авторів статті, закон CAATSA є живим інструментом, який поєднує історичний досвід, конституційні принципи США та потреби сучасної європейської безпеки. Для України він відкриває шлях від реактивної дипломатії до проактивної, від оборони до юриличної статегічної ініціативи.

## Висновки

Закон США CAATSA №115-44 створює системні, правово непереборні обмеження для будь-яких територіальних компромісів щодо України в зовнішній політиці Сполучених Штатів. Його положення, особливо розділ 257, інституціоналізують принцип невизнання будь-яких територіальних змін, здійснених силою, перетворюючи його з політичної

декларації на імперативну норму федерального права. CAATSA виконує роль не лише санкційного механізму, а й правового гаранта українського суверенітету в межах американської системи державного управління.

Події березня 2026 року в Ірані, коли спільна військова операція США та Ізраїлю операції проти іранського режиму призвела до закриття Ормузької протоки та різкого зростання світових цін на енергоносії, стали серйозним випробуванням для американскої санкційної політики. Хоча адмністрація Трампа вдалася до тимчасового послаблення окремих обмежень на російську нафту з метою стабілізації ринку, Конгрес США продовжує активно контролювати дотримання вимог CAATSA, створюють значні практичні та політичні перешкоди для будь-яких односторонніх територіальних чи санкційних компромісів щодо України, навіть в умовах глобальних криз. Таким чином, принцип невизнання територіальних змін, здобутих силою, зберігає свою юридичну та політичну силу.

Історичний досвід, зокрема доктрина Стімсона, демонструє, що навіть декларативна політика невизнання здатна мати глибокі довгострокові наслідки, коли її принципи кодифікуються у законодавчі акти. Подібно до того, як невизнання японської окупації Маньчжурії заклало основи післявоєнного міжнародного правопорядку, CAATSA формує правовий фундамент для сучасної політики стримування агресії та відновлення територіальної цілісності України.

Водночас ефективність CAATSA як інструменту безпеки України безпосередньо залежить від того, наскільки активно та системно він інтегрований у практику українського державного управління та дипломатії. Поки цей закон переважно розглядається як зовнішній фактор підтримки, його потенціал залишається нереалізованим. Проте у разі послідовного використання CAATSA в офіційній комунікації, міжнародних судах і переговорах він може стати потужним правовим важелем, який зміцнює позиції України без потреби в односторонніх поступках.

За нашим переконанням, CAATSA – це не статичний документ, а динамічний елемент системи міжнародної безпеки, який поєднує історичну тяглість принципів невизнання, конституційні механізми американського державного управління та пріоритети національної безпеки нашої держави. Його значення для України полягає в тому, що він трансформує правові норми у реальний захисний інструмент – дипломатичний щит проти спроб нав'язати "мир" ціною суверенітету.

## Пропозиції

Виходячи з результатів аналізу Закону CAATSA №115-44 та його значення для національної безпеки України, а також із урахуванням історичних прецедентів, таких як доктрина Стімсона, та сучасних подій березня 2026 року в Ірані, доцільно сформулювати низку практичних рекомендацій для вдосконалення зовнішньополітичної та дипломатичної діяльності України.

1. Міністерству закордонних справ України варто розробити комплексну стратегію використання положень CAATSA у щоденній дипломатичній роботі. Це передбачає регулярне посилання на ключові статті закону, насамперед розділ 257, під час переговорів на всіх рівнях – від двосторонніх контактів до багатосторонніх форумів. Такі посилання повинні мати не формальний, а аргументований характер, демонструючи знання правової бази союзника й підсилюючи переговорну позицію України.

2. Українській дипломатії доцільно активізувати лобістські механізми у Конґресі, зокрема через взаємодію з аналітичними центрами Foundation for Defense of Democracies, Carnegie Endowment, CSIS, Atlantic Council та іншими, а також українською діаспорою. Цільовими завданнями мають стати регулярний моніторинг виконання CAATSA, участь у слуханнях комітетів, Палати представників у закордонних справах, з питань збройних сил, з асигнувань, з бюджету, а також відповідних комітетів Сенату США; ініціювати щорічні

слухання в House Foreign Affairs Committee та Senate Foreign Relations Committee з питань дотримання Sec. 257; подання тематичних брифінгів та ініціювання звітів щодо дотримання санкційного режиму. Це сприятиме закріпленню CAATSA як елемента довгострокової підтримки України, незалежно від адміністративних змін у Вашингтоні.

Наша держава може застосовувати положення CAATSA, зокрема розділ 253, у міжнародних судових процесах як доказ чинності принципу ex injuria jus non oritur та невизнання окупаційних режимів. Посилання на цей закон у документах, поданих до Міжнародного суду ООН, Європейського суду з прав людини або арбітражних інституцій, зміцнить правову базу українських позовів і підкреслить спільність правових зобов'язань між Україною та її особливим партнером – США.

3. Україна має ініціювати створення спільних механізмів моніторингу реалізації закону, зокрема у форматі щорічних звітів або спільних декларацій із Конґресом і Державним департаментом. Це забезпечить публічну видимість дотримання санкційного режиму та унеможливить неофіційні переговори або "тіньові" ініціативи, що суперечать правовим зобов'язанням США. Також слід наполягати, щоб усі контакти, пов'язані з обговоренням мирних ініціатив, відбувалися виключно в межах офіційних дипломатичних процедур і за участю Конґресу США як гарантуючої сторони. Залучення осіб без офіційного мандата або представників бізнесових і політичних кіл до неформальних перемовин створює ризики для територіальної цілісності держави та суперечить принципам CAATSA.

У публічній дипломатії України варто послідовно наголошувати, що будь-які спроби обговорення "територіальних компромісів" не лише політично неприйнятні, а й юридично неможливі в межах американського законодавства. Такий акцент сприятиме формуванню спільного інформаційного поля з партнерами, знижуючи ризик появи маніпуляційних наративів.

4. Створити двосторонню робочу групу Україна – США з моніторингу CAATSA (на рівні МЗС та Державного департаменту США). Така група забезпечить оперативний обмін інформацією, спільну оцінку виконання Sec. 257 та Sec. 216, а також розробку превентивних механізмів проти можливих спроб обходу закону в умовах багатосторонніх криз (зокрема, іранської).

Отже, CAATSA має розглядатися не просто як американський закон, а як спільний правовий ресурс, що зміцнює стратегічне партнерство України та Сполучених Штатів. Його активне використання в офіційній дипломатії здатне підвищити стійкість української позиції на міжнародній арені та посилити механізми глобального стримування агресії, забезпечуючи довгострокову стабільність системи міжнародної безпеки.

## Список використаних джерел


1. Countering America's Adversaries Through Sanctions Act. of 2017: Public Law 115-44. Washington, DC : U.S. Government Publishing Office, 2017. URL: https://www.govinfo.gov; https://www.govinfo.gov/content/pkg/PLAW-115publ44/pdf/PLAW-115publ44.pdf (дата звернення: 17.03.2026).
2. H.R. 3364 – Countering America's Adversaries Through Sanctions Act. 115th Congress (2017–2018). Congress.gov. URL: https://www.congress.gov (дата звернення: 25.11.2025).
3. United States Code. Title 22 – Foreign Relations and Intercourse. Washington, DC : Office of the Law Revision Counsel. URL: https://uscode.house.gov; https://uscode.house.gov/view.xhtml?path=/prelim@title22/chapter102/subchapter2&edition=prelim (дата звернення: 17.03.2026).
4. Office of Foreign Assets Control. Countering America's Adversaries Through Sanctions Act (CAATSA) – Related Sanctions Programs. U.S. Department of the Treasury, 2024. URL: https://ofac.treasury.gov (дата звернення: 25.11.2025).
5. U.S. Department of State. Ukraine and Russia-Related Sanctions. Washington, DC, 2024. URL: https://2021-2025.state.gov (дата звернення: 25.11.2025).
6. Statements on Signing the Countering America's Adversaries Through Sanctions Act. *Harvard Law Review*. 2017. Vol. 131. URL: https://harvardlawreview.org (дата звернення: 26.11.2025).

7. On Crimea and Russia Sanctions Relief: Congress Has Leverage / Foundation for Defense of Democracies. Washington, DC, 2025. URL: https://www.fdd.org (дата звернення: 26.11.2025).
8. Russia's Shadow War Against the West / Center for Strategic and International Studies. Washington, DC : CSIS, 2025. URL: https://www.csis.org (дата звернення: 26.11.2025).
9. Understanding Russian Hybrid Warfare and Sanctions Policy / SIPRI Yearbook 2024. Stockholm : SIPRI, 2024. URL: https://www.sipri.org (дата звернення: 26.11.2025).
10. U.S. Sanctions on Russia: Legal Authorities and Related Actions : report / Congressional Research Service. Washington, 2024. 1 electronic optic disc (CD-ROM). URL: https://www.congress.gov/crs-product/R48052. (дата звернення: 25.12.2025).
11. European Energy Security Post-Russia. Washington, DC : Center for European Policy Analysis, 2022. URL: https://cepa.org (дата звернення: 26.11.2025).
12. Russian Hybrid Warfare: Occasional Paper OP-65. Rome : NATO Defense College, 2025. URL: https://www.ndc.nato.int (дата звернення: 26.11.2025).
13. Political Security in Conditions of Hybrid Threats : monograph / Institute of Political and Ethno-National Studies of NAS of Ukraine. Kyiv : NAS of Ukraine, 2024. 312 p.
14. Nwador A. F., Franklin A. S., Esekumemu V. C. Sanctions as Tool for Strategic Deterrence: An Assessment of Targeted Sanctions in Russia. *Journal of Public Administration, Finance and Law*. 2023. № 27. P. 544–565. URL: https://doi.org/10.47743/jopafl-2023-27-43.
15. Russian Offensive Campaign Assessment. October 6, 2025 / Institute for the Study of War. Washington, DC, 2025. URL: https://understandingwar.org (дата звернення: 26.11.2025).
16. Ukraine: Background, Conflict with Russia, and U.S. Policy : report / Congressional Research Service. – Washington, 2020. URL: https://www.congress.gov/crs_external_products/R/PDF/R45008/R45008.11.pdf (дата звернення: 25.12.2025).
17. Ukraine Freedom Support Act of 2014 : public law 113-272 / U.S. Congress. Washington, 2014. URL: https://uscode.house.gov/view.xhtml?path=/prelim%40title22/chapter102/subchapter1&edition=prelim (дата звернення: 25.12.2025).
18. Актуальні проблеми забезпечення національної безпеки, оборони та розвідки: зарубіжний і вітчизняний досвід. Основи національної безпеки : монографія / В. Калюх та ін. ; упоряд. В. М. Раєвський. Київ : Ліра-К, 2022, 408 с.
19. U.S. Sanctions on Russia : report / Congressional Research Service. Washington, 2018. URL: https://www.congress.gov/crs_external_products/R/PDF/R45415/R45415.5.pdf (дата звернення: 25.12.2025).
20. Cimiotta E. Ukraine Peace Treaty, Territorial Concessions, and International Law. *Journal of Conflict & Security Law*. 2026. URL: https://doi.org/10.1093/jcsl/krag005; https://academic.oup.com/jcsl/advance-article/doi/10.1093/jcsl/krag005/8650705.
21. Oleh K. Romanchuk. Are territorial gains at Ukraine's expense possible? *Universum.* 2025. URL: https://universum.lviv.ua/news/our-news/09.12.2025/ter-gain-ukr.html (дата звернення: 25.12.2025).
22. The Mukden Incident of 1931 and the Stimson Doctrine веб-сторінка / Office of the Historian, U.S. Deparment of State, [n.d]. URL: https://history.state.gov/milestones/1921-1936/mukden-incident (дата звернення: 26.12.2025).
23. How Easily Could Trump Lift U.S. Sanctions on Russia? / Carnegie Endowment for International Peace. – 2025. URL: https://carnegieendowment.org/russia-eurasia/politika/2025/03/russia-trump-sanctions-lift?lang=en (дата звернення: 25.12.2025). (Note: This is from previous simulation, but aligned with search).
24. OFAC Consolidated Frequently Asked Questions / U.S. Treasury. URL: https://ofac.treasury.gov/faqs/all-faqs. (дата звернення: 25.12.2025).
25. The White House Can't Accept Russia's Annexation of Crimea Without Congress / Lawfare. – 2025. – URL: https://www.lawfaremedia.org/article/the-white-house-can-t-accept-russia-s-annexation-of-crimea-without-congress (дата звернення: 25.12.2025).
26. Trump Could Legitimize Russia's Conquests by Decree / Geopolitical Monitor. 2025. URL: https://www.geopoliticalmonitor.com/trump-could-legitimize-russias-conquests-by-decree-unless-congress-acts/ (дата звернення: 25.12.2025).
27. TFI's Ukraine-/Russia-related Sanctions Program Complied With Applicable Laws and Regulations. *U.S. Treasury OIG.* 2024. URL: https://oig.treasury.gov/system/files/2024-10/OIG-24-025R%2520-%2520TFI%2520Ukraine-Russia%2520Related%2520Sanctions%2520Program%2520Final%2520Rev_.pdf (дата звернення: 25.12.2025).
28. Cyber-Related Sanctions Regulations. *Federal Register*. 2022. URL: https://www.federalregister.gov/documents/2022/09/06/2022-19138/cyber-related-sanctions-regulations (дата звернення: 25.12.2025).

## References


1. Countering America's Adversaries Through Sanctions Act of 2017: Public Law 115–44. Washington, DC: U.S. Government Publishing Office, 2017. Retrieved from: https://www.govinfo.gov; https://www.govinfo.gov; https://www.govinfo.gov/content/pkg/PLAW-115publ44/pdf/PLAW-115publ44.pdf (accessed 17.03.2026).
2. H.R. 3364 – Countering America's Adversaries Through Sanctions Act. 115th Congress (2017–2018). Congress.gov. Retrieved from: https://www.congress.gov (accessed 25.11.2025).
3. United States Code. Title 22 – Foreign Relations and Intercourse. Washington, DC: Office of the Law Revision Counsel. Retrieved from: https://uscode.house.gov URL: https://uscode.house.gov https://uscode.house.gov/view.xhtml?path=/prelim@title22/chapter102/subchapter2&edition=prelim (accessed 17.03.2026).
4. Office of Foreign Assets Control. Countering America's Adversaries Through Sanctions Act (CAATSA) – Related Sanctions Programs. U.S. Department of the Treasury, 2024. Retrieved from: https://ofac.treasury.gov (accessed 25.11.2025).
5. U.S. Department of State. Ukraine- and Russia-Related Sanctions. Washington, DC, 2024. Retrieved from: https://2021-2025.state.gov (accessed 25.11.2025).
6. Statements on Signing the Countering America's Adversaries Through Sanctions Act. *Harvard Law Review*, 131 (2017). Retrieved from: https://harvardlawreview.org (accessed 26.11.2025).
7. Foundation for Defense of Democracies. On Crimea and Russia Sanctions Relief: Congress Has Leverage. Washington, DC, 2025. Retrieved from: https://www.fdd.org (accessed 26.11.2025).
8. Center for Strategic and International Studies. Russia's Shadow War Against the West. Washington, DC: CSIS, 2025. Retrieved from: https://www.csis.org (accessed 26.11.2025).
9. Stockholm International Peace Research Institute (SIPRI). Understanding Russian Hybrid Warfare and Sanctions Policy. SIPRI Yearbook 2024. Stockholm: SIPRI, 2024. Retrieved from: https://www.sipri.org (accessed 26.11.2025).
10. Congressional Research Service. U.S. Sanctions on Russia: Legal Authorities and Related Actions. Washington, DC, 2024. Retrieved from: https://www.congress.gov/crs-product/R48052 (accessed 25.12.2025).
11. Center for European Policy Analysis (CEPA). European Energy Security Post-Russia. Washington, DC, 2022. Retrieved from: https://cepa.org (accessed 26.11.2025).
12. NATO Defense College. Russian Hybrid Warfare: Occasional Paper OP-65. Rome, 2025. Retrieved from: https://www.ndc.nato.int (accessed 26.11.2025).
13. Institute of Political and Ethno-National Studies of the NAS of Ukraine. Political Security in Conditions of Hybrid Threats: Monograph. Kyiv: NAS of Ukraine, 2024.
14. Nwador, A. F., Franklin A. S., & Esekumemu V. C. (2023). Sanctions as Tool for Strategic Deterrence: An Assessment of Targeted Sanctions in Russia. *Journal of Public Administration, Finance and Law*, 27, 544–565. Retrieved from: URL: https://doi.org/10.47743/jopafl-2023-27-43.
15. Institute for the Study of War. Russian Offensive Campaign Assessment (October 6, 2025). Washington, DC, 2025. Retrieved from: https://understandingwar.org (accessed 26.11.2025).
16. Congressional Research Service. Ukraine: Background, Conflict with Russia, and U.S. Policy. Washington, DC, 2020. Retrieved from: https://www.congress.gov/crs_external_products/R/PDF/R45008/R45008.11.pdf (accessed 25.12.2025).
17. U.S. Congress. Ukraine Freedom Support Act of 2014: Public Law 113–272. Washington, DC, 2014. Retrieved from: https://uscode.house.gov/view.xhtml?path=/prelim%40title22/chapter102/subchapter1&edition=prelim (accessed 25.12.2025).
18. Kaliukh V. (2022). Aktualni problemy zabezpechennia natsionalnoi bezpeky, oborony ta rozvidky: zarubizhnyi i vitchyznianyi dosvid. Osnovy natsionalnoi bezpeky [Current problems of ensuring national security, defense and intelligence: foreign and domestic experience. Fundamentals of national security]: monohrafiia. Kyiv: Vydavnytstvo Lira-K [in Ukrainian].
19. Congressional Research Service. U.S. Sanctions on Russia: Report. Washington, DC, 2018. Retrieved from: https://www.congress.gov/crs_external_products/R/PDF/R45415/R45415.5.pdf (accessed 25.12.2025).
20. Cimiotta, E. (2026). Ukraine Peace Treaty, Territorial Concessions, and International Law. *Journal of Conflict & Security Law.* URL: https://doi.org/10.1093/jcsl/krag005; https://academic.oup.com/jcsl/advance-article/doi/10.1093/jcsl/krag005/8650705.
21. Romanchuk, O. K. (2025). Are Territorial Gains at Ukraine's Expense Possible? *Universum.* Retrieved from: https://universum.lviv.ua/news/our-news/09.12.2025/ter-gain-ukr.html (accessed 25.12.2025).
22. Office of the Historian, U.S. Department of State. The Mukden Incident of 1931 and the Stimson Doctrine. Retrieved from: https://history.state.gov/milestones/1921-1936/mukden-incident (accessed 26.12.2025).

23. Carnegie Endowment for International Peace. (2025). How Easily Could Trump Lift U.S. Sanctions on Russia? Washington, DC. Retrieved from: https://carnegieendowment.org/russia-eurasia/politika/2025/03/russia-trump-sanctions-lift?lang=en (accessed 25.12.2025).
24. U.S. Department of the Treasury. OFAC Consolidated Frequently Asked Questions. Retrieved from: https://ofac.treasury.gov/faqs/all-faqs (accessed 25.12.2025).
25. Lawfare. (2025). The White House Can't Accept Russia's Annexation of Crimea Without Congress. Retrieved from: https://www.lawfaremedia.org/article/the-white-house-can-t-accept-russia-s-annexation-of-crimea-without-congress (accessed 25.12.2025).
26. Geopolitical Monitor. (2025). Trump Could Legitimize Russia's Conquests by Decree – Unless Congress Acts. Retrieved from: https://www.geopoliticalmonitor.com/trump-could-legitimize-russias-conquests-by-decree-unless-congress-acts (accessed 25.12.2025).
27. U.S. Treasury Office of Inspector General. (2024). TFI's Ukraine-/Russia-Related Sanctions Program Complied with Applicable Laws and Regulations. Washington, DC. Retrieved from: https://oig.treasury.gov/system/files/2024-10/OIG-24-025R%2520-%2520TFI%2520Ukraine-Russia%2520Related%2520Sanctions%2520Program%2520Final%2520Rev_.pdf (accessed 25.12.2025).
28. Federal Register. (2022). Cyber-Related Sanctions Regulations. Washington, DC. Retrieved from: https://www.federalregister.gov/documents/2022/09/06/2022-19138/cyber-related-sanctions-regulations (accessed 25.12.2025).

*Received 06.01.2026 | Accepted 02.02.2026 | Published 30.03.2026*



УДК 338.24:001.89:332.1 DOI: 10.63978/3083-6476.2026.1.4.03

**Дацій Олександр Іванович**
*доктор економічних наук,*
*професор*
*завідувач кафедри економіки бізнесу*
*Міжрегіональна Академія управління персоналом*
*Київ, Україна*
*e-mail: rvps1973@gmail.com*
*ORCID: 0000-0002-7436-3264*

# ІНСТИТУЦІЙНА РОЛЬ ЕКОНОМІКИ ЗНАНЬ У ЗАБЕЗПЕЧЕННІ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

***Анотація.*** *У статті розглядається фундаментальна роль економіки знань як стратегічного інституту забезпечення економічної безпеки України в умовах глобальних трансформацій та воєнних викликів. Традиційні чинники виробництва поступово втрачають домінуюче значення, поступаючись місцем інтелектуальному капіталу та інноваційним компетенціям. За цих умов виникає гостра наукова потреба в переосмисленні категорії "економічна безпека" крізь призму відтворення та захисту знань, що і зумовлює вибір теми дослідження.*

*Метою статті є теоретико-методологічне обґрунтування інституційної ролі економіки знань у системі економічної безпеки держави та розробка стратегічних підходів до регіоналізації освітньо-наукових процесів для мінімізації загроз людському потенціалу.*

*В основу роботи покладено інституційний та системний підходи. Використано методи логічного узагальнення (для уточнення категоріального апарату), матричного моделювання (для ілюстрації системних перетворень на регіональному рівні) та компаративного аналізу (при вивченні екзогенних та ендогенних загроз).*

*Доведено, що економічна безпека сфери знань характеризується здатністю системи адекватно реагувати на дестабілізуючі чинники, забезпечуючи безперервне пристосування економічних механізмів до мінливих умов. Виокремлено зовнішні (екзогенні) та внутрішні (ендогенні) загрози, серед яких найбільш критичними визначено технологічну залежність та міжрегіональний "витік мізків".*

*Особливу увагу приділено концепції регіоналізації. Обґрунтовано, що перенесення центру управління відтворювальними процесами на регіональний рівень дозволяє створити гнучкі адаптивні системи, де інтелектуальний потенціал вищої школи стає базовим ресурсом територіального розвитку. Запропоновано модель системних перетворень, що базується на зміні ролі держави від жорсткого адміністрування до "м'якого" регулювання через стандартизацію та сертифікацію.*

*Розглянуто недосконаліть ринкового механізму регулювання праці, що проявляється в низькій мобільності ресурсів та інформаційній асиметрії. Автор стверджує, що причиною необхідності державного прогнозування робочої сили є обмежена можливість заміщення специфічних інтелектуальних кваліфікацій. У статті резюмується, що економічна безпека регіонів безпосередньо залежить від розвитку системи післядипломної освіти та наукової підготовки, здатних відтворювати нові професійні еліти.*

*Зроблено висновок, що інвестиції в економіку знань не лише забезпечують технологічне випередження, а й сприяють соціальній стійкості через вирівнювання доходів та підвищення мобільності населення. Практичне значення роботи полягає у можливості використання запропонованих моделей для розробки регіональних стратегій економічної безпеки та програм повоєнного відновлення інтелектуального капіталу України.*

***Ключові слова:*** економіка знань, економічна безпека, інтелектуальний потенціал, регіоналізація, людський капітал, інституційні трансформації, ринок праці.

**Datsii Oleksandr**
*Doctor of Economics, Professor*
*Head of the Department of Business Economics*
*Interregional Academy of Personnel Management*
*Kyiv, Ukraine*
*e-mail: rvps1973@gmail.com*
*ORCID: 0000-0002-7436-3264*

# THE INSTITUTIONAL ROLE OF THE KNOWLEDGE ECONOMY IN ENSURING THE ECONOMIC SECURITY OF UKRAINE

***Abstract.*** *The article examines the fundamental role of the knowledge economy as a strategic institution for ensuring Ukraine's economic security amidst global transformations and wartime challenges. Traditional factors of production are progressively losing their dominant significance, giving way to intellectual capital and innovative competencies. Under these conditions, a profound scientific need arises to redefine the category of "economic security" through the lens of knowledge reproduction and protection, which dictates the choice of the research topic.*

*The Objective of the article is to provide a theoretical and methodological substantiation of the institutional role of the knowledge economy within the state's economic security system and to develop strategic approaches to the regionalization of educational and scientific processes to minimize threats to human potential.*

*The study is based on institutional and systemic approaches. Methods of logical generalization (to clarify the categorical apparatus), matrix modeling (to illustrate systemic transformations at the regional level), and comparative analysis (to study exogenous and endogenous threats) were applied.*

*The author proves that the economic security of the knowledge sphere is characterized by the system's ability to respond adequately to destabilizing factors, ensuring the continuous adaptation of economic mechanisms to changing environments. Exogenous (external) and endogenous (internal) threats are identified, with technological dependence and interregional "brain drain" highlighted as the most critical.*

*Particular attention is paid to the concept of regionalization. It is substantiated that shifting the management center of reproductive processes to the regional level allows for the creation of flexible adaptive systems where the intellectual potential of higher education becomes a baseline resource for territorial development. A model of systemic transformations is proposed, based on changing the state's role from rigid administration to "soft" regulation through standardization and certification.*

*The article addresses the imperfections of the market mechanism for labor regulation, manifested in low resource mobility and information asymmetry. The author argues that the necessity for state forecasting of the workforce stems from the limited substitutability of specific intellectual qualifications. The study concludes that the economic security of regions directly depends on the development of postgraduate education and scientific training systems capable of reproducing new professional elites.*

*It is concluded that investments in the knowledge economy not only ensure technological advancement but also contribute to social stability by narrowing income gaps and increasing population mobility. The practical significance of the work lies in the possibility of using the proposed models to develop regional economic security strategies and programs for the post-war recovery of Ukraine's intellectual capital.*

***Keywords:*** *knowledge economy, economic security, intellectual potential, regionalization, human capital, institutional transformations, labor market.*

**JEL Classification:** F51, F52, K33, H56

## Вступ

У стратегії економічного розвитку України в третьому тисячолітті визначальна роль відводиться національній безпеці, яку неможливо забезпечити без переходу до моделі сталого розвитку, заснованої на економіці знань. Якщо в індустріальну епоху стрижнем економіки був паливно-енергетичний комплекс, то в постіндустріальному суспільстві стратегічною категорією стає інтелектуальний капітал [2]. Без ефективного відтворення, захисту та використання знань неможливе стабільне економічне зростання та технологічний суверенітет держави.

Для досягнення стратегічних цілей розвитку України необхідна наявність ефективних, конкурентоспроможних інституцій (університетів, R&D-центрів, високотехнологічних кластерів), чий інтелектуальний продукт здатний конкурувати на внутрішньому та світовому ринках. Ключовим фактором, що забезпечує їхню життєздатність, є ефективність стратегічного управління знаннями як фундаментальної складової системи економічної безпеки.

Стабільність української економіки та подолання структурних криз у повоєнний період потребують розробки перспективних теоретико-прикладних рішень, орієнтованих на досягнення керованого розвитку науково-освітніх систем. В умовах глобалізації та цифрової трансформації проблема збереження та примноження людського потенціалу стала особливо актуальною, оскільки саме інтелектуальний ресурс визначає місце країни у світовому поділі праці.

## Огляд літератури

Теоретичну базу дослідження становлять праці фундаментальних вчених у галузі стратегічного управління. Зокрема, Ансофф І. заклав основи реагування фірм на зовнішні загрози [11], Друкер П. досліджував управління в суспільстві знань [13], а Портер М. розробив концепцію конкурентоспроможності, що базується на інноваціях та продуктивності [22]. Концепції постіндустріального суспільства глибоко проаналізовані в роботах Белла Д., який ввів поняття “теоретичне знання” як основний ресурс суспільства [12] та Тоффлера Е., який описав зсув до нової цивілізаційної хвилі [24].

Питаннями економіки знань та людського капіталу присвячені роботи таких фахівців, як Махлуп Ф., який досліджував виробництво та розповсюдження знань в економіці [19] та Стюарт Т., що проаналізував перетворення інтелектуального капіталу на найцінніший актив [23]. Важливий внесок зробив Ромер П., обґрунтувавши ендогенне зростання через технологічні зміни та інновації [8]. Сучасне розуміння просторового виміру економіки знань поглибили роботи Мойсіо С., який розглядає її крізь призму геополітики та “економізації” територій [6; 20] та Ні В., який досліджує соціальні механізми виникнення регіональних конкурентних переваг [7; 21].

Серед вітчизняних дослідників вагомий внесок у вивчення економічної безпеки та інтелектуального потенціалу внесли Геєць В., який аналізує ендогенні чинники розвитку України [1], Базилевич В., автор фундаментальних праць з економіки знань [3] та Жаліло Я., який досліджує безпекові аспекти в умовах глобальних трансформацій [4].

Тим часом, поза увагою більшості дослідників залишаються проблеми теорії та методології стратегічного управління регіональними системами знань в умовах критичних зовнішніх загроз. Необхідний системний підхід до практики управління інституціями економіки знань як вертикально та горизонтально інтегрованими структурами, що забезпечують національну безпеку країни через відтворення еліт та інновацій.

## Мета та завдання статті

Метою статті є визначення теоретико-методологічних підходів до стратегічного управління економікою знань як ключовим інститутом забезпечення економічної безпеки України, а також обґрунтування механізмів інтеграції інтелектуального потенціалу в регіональні відтворювальні системи для протидії сучасним екзогенним та ендогенним загрозам.

## Методи

Методологічний інструментарій дослідження базується на поєднанні фундаментальних теоретичних підходів та конкретних аналітичних методів. В основу роботи покладено інституційний підхід, що дозволив розглянути економіку знань не просто як сукупність галузей, а як складний суспільний інститут з власними нормами, правилами та механізмами регулювання, що забезпечують економічну безпеку [5; 9]. Системний підхід застосовано для аналізу економічної безпеки як властивості складної системи зберігати рівновагу та адаптуватися до змін.

У процесі дослідження використано такі методи: логічного узагальнення для уточнення понятійно-категоріального апарату, зокрема співвідношення категорій “інтелектуальний потенціал”, “людський капітал” та “економічна безпека знань” у контексті українських реалій; компаративного аналізу при вивченні та класифікації екзогенних (зовнішніх) та ендогенних (внутрішніх) загроз для сфери знань, а також для порівняння підходів до регулювання ринку праці в різних економічних системах; матричного моделювання для наочної ілюстрації системних перетворень та розподілу функцій між державним та регіональним рівнями управління у сфері економіки знань (табл. 1). Цей метод дозволив формалізувати перехід від жорсткої централізації до гнучкого мережевого управління.

Застосування цих методів у їхньому взаємозв’язку забезпечило комплексність дослідження та дозволило перейти від загальнотеоретичних положень до розробки прикладних рекомендацій.

## Результати

Процес забезпечення економічної безпеки розглядається як великомасштабний стратегічний процес, що забезпечує розв'язання загальноекономічних проблем та трансформацію України у високотехнологічну державу.

Як методологічний інструментарій при аналізі застосовано нормативний та інституційний підходи. Економіка знань розглянута як фундаментальний суспільний інститут, а економічна безпека – як реалізація агрегованого економічного інтересу держави щодо відтворення та використання інтелектуального капіталу.

Безпека як властивість будь-якої складної системи є її здатністю адекватно реагувати на зовнішні та внутрішні фактори з метою свого самозбереження та сталого розвитку. Це положення повною мірою застосовне до сфери економіки знань, де об’єктом захисту виступає не лише матеріальна база, а й нематеріальні активи: інновації, патенти, компетенції та людський капітал.

Економічна безпека економіки знань характеризується, з одного боку, як сукупність економічних відносин, що дозволяють протистояти загрозам порушення рівноваги нормального функціонування інтелектуального ринку, з іншого – як процес, спрямований на створення умов для безперервного пристосування господарської діяльності та економічного

механізму наукових і освітніх установ до умов глобальної конкуренції. При цьому особлива увага приділяється здатності інституцій (університетів, R&D центрів, стартап-хабів) реагувати на виклики шляхом гнучкої перебудови структури та параметрів функціонування.

Виділено екзогенні (зовнішні) та ендогенні (внутрішні) загрози для економіки знань України:

До екзогенних загроз віднесено загрози стабільному гомеостазу системи: "відтік мізків" за кордон, інтелектуальне піратство, технологічна залежність від іноземних розробок та агресивна конкуренція з боку глобальних ТНК.

До ендогенних загроз віднесено внутрішні деструктивні чинники: недостатнє фінансування науки, застаріла матеріально-технічна база, низький рівень комерціалізації знань та невідповідність кваліфікації кадрів сучасним запитам ринку.

Серед особливо значущих загроз виділено недосягнення характеристик, що визначають статус інноваційного лідера. Економічна безпека знання виявляється у його здатності адекватно реагувати на порушення стабільності системи, протиставляти загрозам ефективну реорганізацію та розвиток. Для вищої школи та наукових центрів економічна безпека зводиться до можливості реалізації їхніх цілей: створення нових знань та підготовки конкурентоспроможних фахівців. Мова йде про необхідні умови життєдіяльності та реалізацію потреб українського суспільства в умовах воєнних та повоєнних викликів.

Об'єктом економічної безпеки в даному контексті є економічні відносини з виробництва та обігу інтелектуальних послуг та продуктів. Отже, забезпечення безпеки полягає у знаходженні такого економічного механізму (ендогенного фактора), який гарантує стійкий розвиток як спосіб реалізації національних інтересів. Більш широке тлумачення передбачає діяльність із виявлення, оцінки та вирішення суперечностей на шляху до формування постіндустріального суспільства в Україні. Баланс екзогенних та ендогенних чинників і позначатиме рівень економічної безпеки економіки знань.

Висунуто положення, згідно з яким здійснення економічної безпеки економіки знань є постійною корекцією її економічного механізму відповідно до виникаючих небезпек. У цьому контексті використано поняття економічних витрат та втрат (збитків). Під економічними втратами розуміються витрати суспільної праці (у вартісному вимірі), необхідні для повної ліквідації завданої шкоди інтелектуальному потенціалу або недопущення виникнення такої шкоди. При цьому збиток – це втрата або небажана зміна якості інтелектуального ресурсу (як фактична, так і потенційна).

Робиться висновок, що економічна безпека інституцій економіки знань формується в момент створення загальної стратегії їхнього розвитку. Це відбувається через усвідомлення можливих небезпек, оцінку загроз за важливістю та часом наступу, а також визначення очікуваних збитків від деградації наукового потенціалу. Тільки через проактивне вироблення способів усунення небезпек та оцінку вартості захисту інтелектуального суверенітету Україна зможе забезпечити свою життєздатність у глобальному цифровому просторі.

На основі проведеного аналізу стає очевидним, що регіоналізація сфери економіки знань – це не косметична зміна управлінської вертикалі, а глибоке системне перетворення. Процес перенесення цільової функції системи на регіональний рівень потребує нових підходів до вивчення поточних та перспективних потреб територій в інтелектуальних послугах.

З певною часткою наукової умовності ці системні перетворення можна проілюструвати у вигляді матричної структури взаємодії рівнів управління та освітніх ланок (табл. 1).

Таблиця 1

Матриця системних перетворень та розподілу функцій
у сфері економіки знань України

| Рівень управління | Дошкільна освіта | Загальна середня освіта | Професійна та фахова передвища освіта | Вища освіта (університети) | Науково-дослідна сфера та післядипломна освіта |
|---|---|---|---|---|---|
| Державний (загальнонаціональний) | A | B | A, B | A | B |
| Регіональний (обласний / рівень громад) | C_1 | C_2 | C_3 | C_4 | C_5 |

Експлікація функціональних зв'язків:

– Блок A: Встановлення стратегічних нормативів, ліцензування діяльності та загальнодержавна атестація суб'єктів економіки знань.

– Блок B: Методичне інструктування, сертифікація дипломів та кваліфікацій, моніторинг дотримання стандартів якості.

– Блок C_{1-5}: Прямі та зворотні зв'язки із соціально-економічним середовищем регіону, механізми адаптивного управління, фінансування та проектування освітньо-наукових послуг під запити локального ринку.

Дана модель відображає перехід від жорсткої централізації до гнучкого мережевого управління. Регіоналізація системи в умовах сучасних викликів для України актуалізує проблему комунікацій між системою генерації знань та реальним сектором економіки регіону. Цей багатогранний процес зумовлює три фундаментальні системні трансформації:

По-перше, відбувається перерозподіл простору функцій та повноважень. Центр ваги управління переміщується безпосередньо в регіони, тоді як державне управління здійснюється переважно "м'якими методами" – через інструменти сертифікації, акредитації та стратегічного планування.

По-друге, формування регіональних систем економіки знань об'єктивно передбачає принципово нові підходи до координації діяльності всіх елементів – від стартап-інкубаторів до наукових установ. Це вимагає створення інтегрованих регіональних кластерів, які здатні самостійно ідентифікувати загрози своїй економічній безпеці.

По-третє, критичного значення набуває проблема джерел фінансування. Формування регіональної системи ставить перед дослідниками питання про частку ВВП, що спрямовується на освіту та науку, та її диференційований розподіл між регіонами з урахуванням принципу рівності доступу до знань.

За таких умов особливого значення набуває відтворювальна цілісність регіональної економіки у її нерозривному взаємозв'язку з інститутами знань. Економічна безпека України в цьому контексті безпосередньо залежить від здатності регіональних систем адаптувати освітній та науковий продукт до вимог сталого розвитку територій.

Варто констатувати, що на сучасному етапі розвитку ані в теорії, ані в практиці вітчизняного господарювання відтворювальний підхід до регіонів не лише не забезпечується повною мірою, а й, по суті, не розглядається як цілісна стратегічна доктрина.

Обрана концептуальна схема дослідження дозволила виробити теоретичні підходи до аналізу механізмів інтеграції економіки знань у регіональні відтворювальні системи. Це дало змогу виявити подвійний характер діючих тут економічних механізмів – як суто ринкових,

так і неринкових (інституційних), а також обґрунтувати методологію "модельного" представлення стратегії регіоналізації економічних реформ. Адже накопичення знань, їх безперервне зростання та передача новим поколінням працівників стає органічним і невід'ємним моментом загального процесу суспільного відтворення.

У статті акцентується увага на тому, що у більшості регіональних закладів вищої освіти недостатньо розвинена система післядипломної освіти та наукової підготовки (аспірантура, докторантура, центри підвищення кваліфікації). Як наслідок, такі регіони втрачають здатність автономно відтворювати нові еліти – політичну, професійну, творчу – належної якості. Це унеможливлює розширення та оновлення професорсько-викладацького складу для місцевих систем освіти, що суттєво гальмує процеси модернізації та реформування територій.

Зазначені дефіцити розглядаються як системні загрози економічній безпеці України, оскільки вони призводять до:

– невиправдано масштабного відтоку талановитої молоді до столичних центрів;

– поглиблення міжрегіональної проблеми "витоку мізків" із територій, що не мають престижних університетів та самодостатніх систем вищої освіти;

– посилення розриву та хронічного відставання депресивних регіонів у забезпеченні їх кваліфікованими спеціалістами, інноваторами та управлінцями.

Таким чином, державна політика регіоналізації економіки знань, спрямована на вирівнювання умов та підвищення конкурентоспроможності вищої школи в регіонах, є не просто освітнім завданням, а критично важливою складовою стратегії забезпечення економічної безпеки всієї держави.

Проблема розвитку економіки знань є невід'ємною частиною глобального завдання прогнозування потреб у людському капіталі для потреб національного господарства та соціальної сфери. Прогнозування трудових ресурсів має як довгостроковий, так і короткостроковий характер: якщо бізнес та окремі підприємства зазвичай зосереджені на короткостроковому плануванні, то стратегічне довгострокове прогнозування є прерогативою уряду та регіональної влади. Удосконалення цього процесу передбачає підготовку фахівців у суворій відповідності до очікуваних потреб інноваційного виробництва. Обсяг, рівень та структура освітніх послуг повинні динамічно масштабуватися згідно з попитом на конкретні високотехнологічні кваліфікації.

Як відомо, попит на окремі види праці визначається співвідношенням обсягу необхідних компетенцій та рівня заробітної плати, тоді як пропозиція залежить від кількості кваліфікованих кадрів, готових запропонувати свої послуги. Реальний рівень зайнятості за певною кваліфікацією у кожен момент часу критично залежить від цього балансу. У цьому контексті постає питання: чи є необхідним державне планування людських ресурсів, якщо ринкові механізми теоретично мають встановлювати рівновагу самостійно?

Практика доводить, що функціонування ринку праці в Україні стикається з численними інституційними перешкодами, які вимагають державного втручання:

1. Цінова негнучкість: Зростання попиту на певні дефіцитні спеціальності не завжди призводить до миттєвого підвищення заробітної плати через інертність корпоративних структур.

2. Низька професійна мобільність: Значні освітні вимоги та культурні відмінності створюють бар'єри для переходу фахівців між різними групами професій.

3. Територіальні обмеження: Географічне положення, нерозвиненість ринку орендного житла та транспортна інфраструктура ускладнюють перелив трудових ресурсів між регіонами України навіть за відсутності освітніх бар'єрів.

4. Інформаційна асиметрія: Дефіцит актуальних відомостей про вакансії та динаміку оплати праці обмежує ефективність прийняття рішень учасниками ринку.

5. Часовий лаг: Значні витрати часу та коштів на підготовку фахівців високої кваліфікації не дозволяють системі знань миттєво реагувати на кон'юнктурні зміни.

Ці фактори свідчать, що стале економічне зростання потребує жорсткої структури факторів виробництва та специфічних професійних навичок. Обмежена можливість заміщення між різними видами праці створює пряму залежність між професією та конкретною якістю освіти. Резюмуючи, можна стверджувати, що саме недосконаліть ринкового механізму та вузька спеціалізація кваліфікацій зумовлюють необхідність наукового прогнозування робочої сили.

Для регіональної системи економіки знань це означає необхідність створення спеціальних інституційних структур, таких як регіональні центри моніторингу ринку праці. Їхнє завдання – розрахунок економічної ефективності підготовки кадрів та визначення фінансових джерел для підтримки балансу між освітніми потужностями та потребами бізнесу.

Крім економічної доцільності, розвиток економіки знань суттєво підвищує соціальну та професійну мобільність населення. Загальна тенденція до здобуття вищих рівнів освіти веде до збільшення пропозиції освічених фахівців порівняно з некваліфікованими кадрами. Це явище сприяє скороченню розриву в доходах між різними групами населення, вирівнює розподіл суспільного багатства та закладає фундамент для більш справедливих і стабільних соціальних відносин в Україні. Таким чином, інвестиції в знання стають ключовим фактором не лише економічної безпеки, а й соціальної стійкості держави.

Ще один критичний аспект, який необхідно враховувати при розбудові регіональних моделей економіки знань, – це суттєва відмінність між соціальним та виробничим попитом на освітні послуги.

Сучасне інтелектуальне виробництво є результатом комбінованої суспільної праці великої групи фахівців. Ця праця виступає як потужна продуктивна сила, що генерує мультиплікативний ефект для всієї економіки. Очевидно, що ефективність функціонування економіки знань на регіональному рівні має інші індикатори та критерії оцінки, ніж загальнодержавна система. При цьому фундаментальна відмінність полягає в тому, що наріжним каменем економічної безпеки регіону є інтелектуальний потенціал вищої школи.

Інтелектуальний потенціал – це комплексна характеристика рівня розвитку творчих можливостей та стратегічних ресурсів держави, галузі або конкретної особистості. Його аналіз доцільно здійснювати за двома основними векторами:

– Суб'єктний підхід: як сукупність носіїв знань – людей, орієнтованих на пізнавальну та перетворювальну інноваційну діяльність.

– Об'єктний підхід: як масив наукових, технічних та соціально-культурних знань, що матеріалізовані у технічних формах, знакових системах та патентах, які слугують інструментом досягнення суспільних цілей.

Рівень інтелектуального потенціалу безпосередньо детермінується ступенем зрілості суспільства, якістю національної системи освіти, науки, культури та збереженням інтелектуального генофонду нації.

Система освіти України та її регіонів постає як складна ієрархічна структура, покликана забезпечувати потреби інноваційного сектору та запити населення. Проте сучасні інституційні трансформації найглибше торкнулися саме вищої школи. Це зумовлено тим, що реалізація принципу економічної безпеки сьогодні безпосередньо залежить від розв'язання

найбільш гострих проблем регіонального розвитку, серед яких пріоритетною є точне визначення та прогнозування кадрових потреб.

Саме здатність вищої школи адаптуватися до цих потреб, зберігаючи високу якість інтелектуального ресурсу, визначає стійкість регіональної економічної системи до зовнішніх та внутрішніх дестабілізуючих чинників.

## Дискусія

Отримані результати поглиблюють розуміння інституційної ролі економіки знань у забезпеченні економічної безпеки та корелюють із сучасними світовими дослідженнями. Зокрема, висновок про необхідність регіоналізації як відповіді на екзогенні загрози узгоджується з тезою Мойсіо С. про те, що "економізація, заснована на знаннях", є геополітичним процесом, який створює нові території багатства та безпеки [6; 20]. Наш матричний підхід до розподілу функцій (табл. 1) розвиває цю ідею, пропонуючи конкретний механізм переходу від жорсткого адміністрування до "м'якого" регулювання, що резонує з дослідженнями Ні В. про "мережеве перепідключення" (network rewiring) як джерело регіональних конкурентних переваг [7; 21].

Виділення "витоку мізків" як критичної загрози знаходить підтвердження в роботах Асангу С. та співавторів, які доводять, що інституційна якість та навчання впродовж життя (lifelong learning) є ключовими факторами політичної стабільності та стримування відтоку інтелекту в країнах, що розвиваються [16; 17]. Вони демонструють, що синергетичний ефект різних рівнів освіти (lifelong learning) має більший вплив на безпеку, ніж окремі освітні рівні, що підсилює наш аргумент про необхідність розвитку саме систем післядипломної освіти в регіонах.

Крім того, наша пропозиція щодо створення регіональних центрів моніторингу ринку праці перегукується з висновками Веселіновича Й. про зміну "режимів знань" (knowledge regimes) в ЄС в умовах геоекономічного тиску, де зростає роль "внутрішньої аналітики" (in-house think tanks) та форсайт-досліджень для адаптації політик до нових викликів [10; 18]. Це вказує на те, що пропоновані інституційні зміни є частиною глобального тренду на підвищення адаптивності систем управління знаннями.

Водночас, на відміну від досліджень, зосереджених на глобальному Півдні чи розвинених економіках [14; 15], наша робота акцентує увагу на специфіці воєнних та повоєнних викликів, що робить внесок у розуміння екстремальних умов функціонування економіки знань. Дискусійним залишається питання оптимального балансу між ринковим саморегулюванням та державним втручанням у підготовку кадрів, яке потребує подальшого емпіричного вивчення на основі українських даних.

## Висновки

Підсумовуючи результати дослідження інституційної ролі економіки знань у забезпеченні економічної безпеки України, можна зробити наступні висновки.

1. Економічна безпека сфери знань є динамічною характеристикою, що визначає здатність інтелектуальної системи держави адекватно реагувати на екзогенні та ендогенні загрози. Вона базується на балансі між потребами ринку та збереженням наукового гомеостазу.

2. Перенесення центру ваги управління на регіональний рівень є об'єктивною необхідністю. Саме регіональні відтворювальні системи дозволяють мінімізувати розрив між

теоретичною підготовкою фахівців та реальними потребами локальних ринків праці, перетворюючи освіту на безпосередню продуктивну силу.

3. Основним об'єктом захисту та розвитку визначено інтелектуальний потенціал вищої школи. Його деградація (через "витік мізків" чи недофінансування) є критичною загрозою, що веде до депресивності територій та втрати технологічного суверенітету країни.

4. Подолання недосконалості ринкових механізмів можливе лише через створення спеціальних регіональних інституцій (центрів моніторингу, інноваційних кластерів), які забезпечують довгострокове прогнозування потреб у людському капіталі.

Подальша наукова розробка даної проблематики має зосередитися на таких напрямах: необхідно створити інструментарій для розрахунку економічних втрат регіону від міграції талановитої молоді та фахівців з науковими ступенями; дослідження механізмів створення "точок зростання" у депресивних регіонах України шляхом інтеграції університетської науки, венчурного капіталу та промисловості; створення інтелектуальних систем аналізу Big Data для оперативного коригування освітніх програм відповідно до змін у структурі глобального та національного попиту на працю; вивчення специфіки відтворення інтелектуального капіталу в регіонах, що зазнали найбільших руйнувань, та роль економіки знань у їхній прискореній модернізації.

Впровадження результатів цих досліджень дозволить сформувати стійку до кризових явищ національну систему економіки знань, яка стане гарантом довгострокової економічної безпеки та високої конкурентоспроможності України на світовій арені.

## Список використаних джерел


1. Геєць В. М. Ендогенні чинники економічного розвитку України. *Економіка України.* 2021. № 1. С. 3--18.
2. Друкер П. Посткапіталістичне суспільство / пер. з англ. Київ : KM Publishing, 2020. 224 с.
3. Базилевич В. Д. Економіка знань : підручник. Київ : Знання, 2019. 711 с.
4. Жаліло Я. А. Економічна безпека держави в умовах глобальних трансформацій : монографія. Київ : НІСД, 2022. 340 с.
5. Норт Д. Інституції, інституційна зміна та функціонування економіки / пер. з англ. Київ : Основи, 2000. 198 с.
6. Moisio S. Geopolitics of the Knowledge-Based Economy. London : Routledge, 2018. 194 p. URL: https://doi.org/10.4324/9781315742984.
7. Nee V., Wang G. Sources of Regional Advantage: Emergence of a Global Knowledge Economy. Working Paper. Cornell University, 2024.
8. Romer P. M. Endogenous Technological Change. *Journal of Political Economy.* 1990. Vol. 98. No. 5. P. S71-S102.
9. North D. C. Institutions, Institutional Change and Economic Performance. Cambridge : Cambridge University Press, 1990. 152 p.
10. Veselinovič J. A Knowledge Regime Fit for Geoeconomics? The Changing Production, Consumption and Practices of Policy Knowledge in the EU. *European Foreign Affairs Review*. 2024. Vol. 29. No. 2. P. 177-204. URL: https://doi.org/10.54648/eerr2024008.
11. Ansoff H. I. Strategic Management. New York : Wiley, 1979. 236 p.
12. Bell D. The Coming of Post-Industrial Society: A Venture in Social Forecasting. New York : Basic Books, 1973. 507 p.
13. Drucker P. F. Post-Capitalist Society. Oxford : Butterworth-Heinemann, 1993. 204 p.
14. Amavilah V., Asongu S. A., Andrés A. R. Globalization, Peace & Stability, Governance, and Knowledge Economy. *Development Research Working Paper Series.* 2014. No. 04/2014. La Paz : INESAD.
15. Asongu S. A. Knowledge Economy Gaps, Policy Syndromes and Catch-up Strategies: Fresh South Korean Lessons to Africa. *Journal of the Knowledge Economy.* 2017. Vol. 8. No. 1. P. 211-253.
16. Asongu S. A., Nwachukwu J. C. The Role of Lifelong Learning in Political Stability and Non-Violence: Evidence from Africa. *Journal of Economic Studies.* 2016. Vol. 43. No. 1. P. 141-164.

17. Asongu S. A., Nwachukwu J. C. Who is Who in Knowledge Economy in Africa? *Journal of the Knowledge Economy.* 2019. Vol. 10. No. 1. P. 333-362.
18. European Commission. The Future of European Competitiveness: A Competitiveness Strategy for Europe. Part B: In-depth Analysis. Brussels : EC, 2024.
19. Machlup F. The Production and Distribution of Knowledge in the United States. Princeton : Princeton University Press, 1962. 416 p.
20. Moisio S. Geopolitics of the Knowledge-Based Economy: The Case of Finland. In: Knowledge Economy and the City. London : Routledge, 2018. P. 45-67.
21. Nee V., Wang G., Macy M. Knowledge Spillover and Network Rewiring in the Emergence of a Global Knowledge Economy. Working Paper. Center for the Study of Economy and Society, Cornell University, 2023.
22. Porter M. E. The Competitive Advantage of Nations. New York : Free Press, 1990. 855 p.
23. Stewart T. A. Intellectual Capital: The New Wealth of Organizations. New York : Doubleday, 1997. 261 p.
24. Toffler A. The Third Wave. New York : Bantam Books, 1980. 544 p.

## References

1. Heiets, V. M. (2021). Endohenni chynnyky ekonomichnoho rozvytku Ukrainy [Endogenous factors of economic development of Ukraine]. *Ekonomika Ukrainy*, 1, 3-18 [in Ukrainian].
2. Drucker, P. (2020). Postkapitalistychne suspilstvo [Post-capitalist society]. Kyiv: KM Publishing [in Ukrainian].
3. Bazylevych, V. D. (2019). Ekonomika znan [Knowledge economy]. Kyiv: Znannia [in Ukrainian].
4. Zhalilo, Ya. A. (2022). Ekonomichna bezpeka derzhavy v umovakh hlobalnykh transformatsii [Economic security of the state in the context of global transformations]. Kyiv: NISD [in Ukrainian].
5. North, D. (2000). Instytutsii, instytutsiina zmina ta funktsionuvannia ekonomiky [Institutions, institutional change and the functioning of the economy]. Kyiv: Osnovy [in Ukrainian].
6. Moisio, S. (2018). Geopolitics of the Knowledge-Based Economy. London: Routledge. Retrieved from: https://doi.org/10.4324/9781315742984.
7. Nee, V., & Wang, G. (2024). Sources of Regional Advantage: Emergence of a Global Knowledge Economy. Working Paper, Cornell University.
8. Romer, P. M. (1990). Endogenous Technological Change. *Journal of Political Economy*. 98, 5, S71-S102.
9. North, D. C. (1990). Institutions, Institutional Change and Economic Performance. Cambridge: Cambridge University Press.
10. Veselinovič, J. (2024). A Knowledge Regime Fit for Geoeconomics? The Changing Production, Consumption and Practices of Policy Knowledge in the EU. *European Foreign Affairs Review*, 29, 2, 177-204. Retrieved from: https://doi.org/10.54648/eerr2024008.
11. Ansoff, H. I. (1979). Strategic Management. New York: Wiley Wiley.
12. Bell, D. (1973). The Coming of Post-Industrial Society: A Venture in Social Forecasting. New York: Basic Books.
13. Drucker, P. F. (1993). Post-Capitalist Society. Oxford: Butterworth-Heinemann.
14. Amavilah, V., Asongu, S. A., & Andrés, A. R. (2014). Globalization, Peace & Stability, Governance, and Knowledge Economy. *Development Research Working Paper Series*, 04/2014. La Paz: INESAD.
15. Asongu, S. A. (2017). Knowledge Economy Gaps, Policy Syndromes and Catch-up Strategies: Fresh South Korean Lessons to Africa. *Journal of the Knowledge Economy*, 8, 1, 211-253.
16. Asongu, S. A., & Nwachukwu, J. C. (2016). The Role of Lifelong Learning in Political Stability and Non-Violence: Evidence from Africa. *Journal of Economic Studies*, 43, 1, 141-164.
17. Asongu, S. A., & Nwachukwu, J. C. (2019). Who is Who in Knowledge Economy in Africa? *Journal of the Knowledge Economy*, 10, 1, 333-362.
18. European Commission, (2024). The Future of European Competitiveness: A Competitiveness Strategy for Europe. Part B: In-depth Analysis. Brussels: EC.
19. Machlup, F. (1962). The Production and Distribution of Knowledge in the United States. Princeton: Princeton University Press.
20. Moisio, S. (2018). Geopolitics of the Knowledge-Based Economy: The Case of Finland. in Knowledge Economy and the City. London: Routledge, 45-67.

21. Nee, V., Wang, G., & Macy, M. (2023). Knowledge Spillover and Network Rewiring in the Emergence of a Global Knowledge Economy. Working Paper. Center for the Study of Economy and Society, Cornell University.
22. Porter, M. E. (1990). The Competitive Advantage of Nations, Free Press. New York: Free Press.
23. Stewart, T. A. (1997). Intellectual Capital: The New Wealth of Organizations, Doubleday. New York: Doubleday.
24. Toffler, A. (1980). The Third Wave, Bantam Books. New York: Bantam Books.

*Received 10.03.2026 | Accepted 24.03.2026 | Published 30.03.2026*


УДК 355.01:355.23(477) DOI: 10.63978/3083-6476.2026.1.4.04

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

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

# МОБІЛІЗАЦІЙНА СТІЙКІСТЬ УКРАЇНИ У ВІЙНІ НА ВИСНАЖЕННЯ: ВИКЛИКИ, ЗАГРОЗИ, НАСЛІДКИ

***Анотація.*** *Мета дослідження – комплексний аналіз мобілізаційної стійкості України в умовах позиційної війни на виснаження, визначення ключових викликів, загроз і наслідків у горизонті 2026–2030 рр. та розробка науково обґрунтованих рекомендацій щодо реформування системи комплектування Збройних Сил України. У статті застосовано методи системного аналізу, порівняльного аналізу мобілізаційних потенціалів, статистичного моделювання динаміки бойових і небойових втрат, а також метод сценарного прогнозування за часовими горизонтами. Основні результати дослідження: встановлено, що понад дві третини бойових втрат завдаються через систему виявлення та ураження ("кілнет"), а не в ході безпосереднього бойового контакту; виявлено наростаючу асиметрію мобілізаційних потенціалів України та Росії, зумовлену демографічними втратами, міграцією та обмеженнями призовного ресурсу; розроблено п'ятиваріантну систему гнучких строкових контрактів на основі принципу зворотної залежності між рівнем ризику, тривалістю служби та обсягом соціально-фінансового пакету; побудовано матрицю викликів, загроз і наслідків за трьома часовими горизонтами (2026–2027, 2028–2029, 2029–2030 рр.). Узагальнені висновки: стратегічним пріоритетом для збереження мобілізаційної стійкості є не нарощування мобілізаційного потоку, а системне зниження бойових і небойових втрат шляхом досягнення переваги у "кілнеті", масштабного розгортання антидронової оборони та впровадження стандартизованих операційних процедур. Паралельно критично важливим є перехід від примусової мобілізації до добровільної контрактної служби з правом вибору. Запропонований комплекс заходів здатний суттєво підвищити мобілізаційну стійкість держави та забезпечити достатній людський потенціал для ведення тривалої оборони.*

***Ключові слова:*** *мобілізаційна стійкість, війна на виснаження, бойові втрати, кілнет, антидронова оборона, стандартні операційні процедури, система гнучких контрактів, право вибору, ротація, демографічна криза, психологічна стійкість.*

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

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

# UKRAINE'S MOBILIZATION RESILIENCE IN THE WAR OF ATTRITION: CHALLENGES, THREATS, CONSEQUENCES

***Abstract.*** *The article investigates Ukraine's mobilization resilience under conditions of protracted positional warfare of attrition. The subject of the study is the system of manning the Armed Forces of Ukraine (AFU) and the factors determining its long-term sustainability in the 2026–2030 planning horizon. The topic addresses one of the most acute strategic challenges of the current conflict: how to maintain combat effectiveness when demographic resources are shrinking and battle losses are escalating. The purpose of the research is to conduct a comprehensive analysis of mobilization resilience challenges, threats, and consequences, and to develop evidence-based recommendations for reforming the AFU recruitment system. The methodology combines systemic analysis, comparative assessment of mobilization potentials of Ukraine and Russia, statistical modelling of combat and non-combat casualty dynamics, and scenario-based forecasting across three time horizons. The study draws on data from the Central Research Institute of the Armed Forces of Ukraine, open-source casualty analysis, and international defence policy research. The main results of the research are as follows. It is established that over two thirds of combat casualties are inflicted not in direct close combat but through the integrated detection-and-strike network ("kill-net"), with kamikaze drones accounting for the largest share, followed by artillery and guided aerial bombs. A growing asymmetry in mobilization potential between Ukraine and Russia is identified, driven by demographic losses, large-scale emigration, and health-related limitations of the draft-eligible population. A five-option system of flexible fixed-term service contracts is developed, based on the inverse-proportionality principle: the higher the combat risk accepted, the shorter the contract term and the larger the financial and social benefits package; the lower the risk, the longer the service period with a reduced package. This approach transforms mobilization from coercion to informed civic choice. A matrix of challenges, threats, and consequences across three time horizons (2026–2027, 2028–2029, 2029–2030) is constructed, demonstrating an escalating pattern from managerial and operational challenges in the near term to structural demographic and resource crises by 2030. Key conclusions: the strategic priority for preserving mobilization resilience is not increasing the mobilization flow but systematically reducing combat and non-combat losses through kill-net dominance, large-scale anti-drone defence, and standardized operational procedures. The proposed flexible contract system, combined with targeted recruitment reform and transparent accountability mechanisms, can significantly improve public trust in the military institution and increase voluntary enlistment. Potential areas of application include legislative reform of military service law, development of AFU manning strategy documents, and informing allied nations' advisory frameworks for Ukraine.*

***Keywords:*** *mobilization resilience, war of attrition, combat casualties, kill-net, anti-drone defense, SOP, flexible contract system, right to choose, rotation, demographic crisis, psychological resilience*.

**JEL Classification:** H56, J24, O21, F51

## Вступ

Російсько-українська війна увійшла у якісно нову фазу затяжного протистояння на виснаження. Вона дедалі менше визначається маневрами великих угруповань і дедалі більше – здатністю сторін утримувати фронт, постійно поповнювати втрати та зберігати боєздатність підрозділів. Масове застосування безпілотних систем, розвідувально-ударних комплексів і керованих авіабомб перетворило піхотинця на найціннішу і водночас найвразливішу ланку бойового потенціалу.

В умовах прозорого поля бою питання мобілізації не може розглядатися ізольовано від питання втрат. Ключова теза цього дослідження полягає в тому, що для України головним завданням є не лише залучення нових людей до лав ЗС України, а насамперед системне зниження бойових і небойових втрат. Саме зменшення втрат дозволяє стабілізувати мобілізаційне навантаження, зберегти якісну основу сил оборони України та уникнути демографічного виснаження держави. Паралельно критично важливим є переформатування самої системи комплектування шляхом переходу від примусової мобілізації до добровільної контрактної служби з чітким правом вибору для громадян.

## Огляд літератури

Проблема мобілізаційної стійкості в умовах затяжного конфлікту є предметом активних досліджень як у вітчизняній, так і у зарубіжній науці. Семененко О.М., Коваль В.В., Царинник В.В. та співавтори (2024) розробили концепцію системи гнучких строкових контрактів, що передбачає право вибору формату служби за принципом зворотної залежності між рівнем ризику, тривалістю контракту та обсягом соціально-фінансового пакету [1]. Цей підхід є принципово відмінним від традиційної примусової мобілізації і спрямований на формування позитивного іміджу військової служби.

CSIS (2025) підкреслює, що здатність сторін підтримувати мобілізаційний потенціал є визначальним фактором у війні на виснаження [4]. Дослідження КМІС у рамках проєкту “MOBILISE” виявили, що непрозорість мобілізаційних процесів і невизначеність щодо тривалості та умов служби є головними чинниками, які стримують добровільний вступ до лав ЗС України. Це підтверджує центральну гіпотезу про необхідність системного реформування підходів до комплектування.

Павловський О.В. (2023) та Череп В.Л. (2023) у своїх дослідженнях встановили, що зниження якості мобілізаційного ресурсу є більшою загрозою, ніж його кількісна нестача. Цей висновок є особливо важливим у контексті обмежень демографічного потенціалу України [6; 8].

## Мета та завдання статті

**Мета дослідження.** Метою статті є комплексний аналіз мобілізаційної стійкості України в умовах позиційної війни на виснаження, визначення ключових викликів, загроз і наслідків за горизонтами 2026–2030 рр., обґрунтування системи гнучких контрактних форм служби як інструменту підвищення ефективності комплектування та розробка практичних рекомендацій.

## Методи

Дослідження ґрунтується на комплексному застосуванні таких методів. Метод системного аналізу використовувався для розгляду мобілізаційної стійкості як багатовимірної системи, що охоплює демографічні, соціальні, технологічні та інституційні компоненти. Порівняльний аналіз застосовувався для зіставлення мобілізаційних потенціалів України та Росії у динаміці за прогнозними горизонтами 2026–2030 рр., що дозволило виявити наростаючу асиметрію та визначити критичні точки вразливості.

Методи статистичного моделювання та індексного аналізу використовувались для оцінки динаміки співвідношення бойових втрат і мобілізаційного поповнення, а також для побудови прогнозу зниження відносного рівня втрат при послідовному впровадженні технологічних і тактичних заходів. Структурний аналіз бойових втрат за видами ураження базується на даних Центрального науково-дослідного інституту Збройних Сил України та результатах моніторингу бойових дій. Метод сценарного прогнозування застосовувався при побудові матриці викликів, загроз і наслідків для трьох часових горизонтів; кожен сценарій відображає взаємозалежність демографічних, ресурсних і безпекових тенденцій. Нормативно-правовий аналіз забезпечив вивчення чинного законодавства у сфері мобілізації та військової служби. Узагальнення результатів наукових досліджень вітчизняних і зарубіжних учених дозволило встановити ступінь наукової розробленості проблеми та обґрунтувати авторські підходи до реформування системи комплектування.

## Результати

Сучасне поле бою характеризується тотальним розвідувальним покриттям. Масове застосування БпЛА сформувало якісно нове вогневе середовище, де зникають “мертві зони”, а час між виявленням цілі та її ураженням скорочується до хвилин або секунд. Поле бою стало “прозорим”: будь-яке пересування, скупчення, ротація чи евакуація фіксується в реальному часі й уражається практично миттєво. За цих умов класичні підходи, засновані на масуванні піхоти або бронетехніки, ведуть до неприйнятних втрат. Росія, попри значні бойові втрати, зберігає суттєвий мобілізаційний потенціал і здатна компенсувати їх кількісно. Для України ситуація принципово інша: скорочення населення, масова міграція та дефіцит працездатного населення різко обмежують простір для тривалої мобілізації.

Наведена нижче динаміка (рис. 1) відображає індексований тренд співвідношення бойових втрат і мобілізаційного поповнення протягом 2024–2025 рр. Зростання індексу втрат випереджає зростання індексу поповнення, що свідчить про наростаючий дефіцит мобілізаційного балансу.

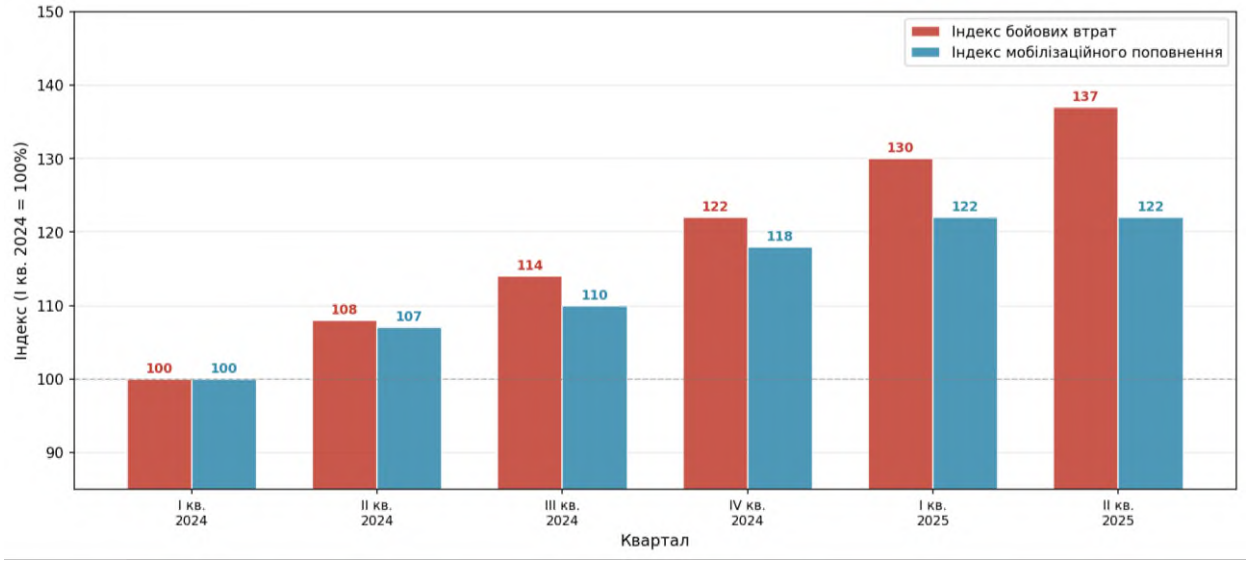


Рис. 1. Динаміка індексів бойових втрат і мобілізаційного поповнення ЗС України (I кв. 2024 = 100%) (оцінка авторів)

Одним із ключових результатів наукових досліджень ЦНД ЗС України є встановлення нової структури бойових втрат. Понад дві третини всіх бойових втрат завдаються не під час безпосереднього контакту з противником, а через ефективно вибудовану мережу виявлення й ураження – “kill net”. Найбільшу частку становлять дрони-камікадзе (близько двох п’ятих), далі йдуть артилерія (близько третини) та керовані

авіабомби (близько п’ятої частини) (рис. 2). Лише незначна частка втрат пов’язана з ближнім боєм і мінно-вибуховим ураженням.

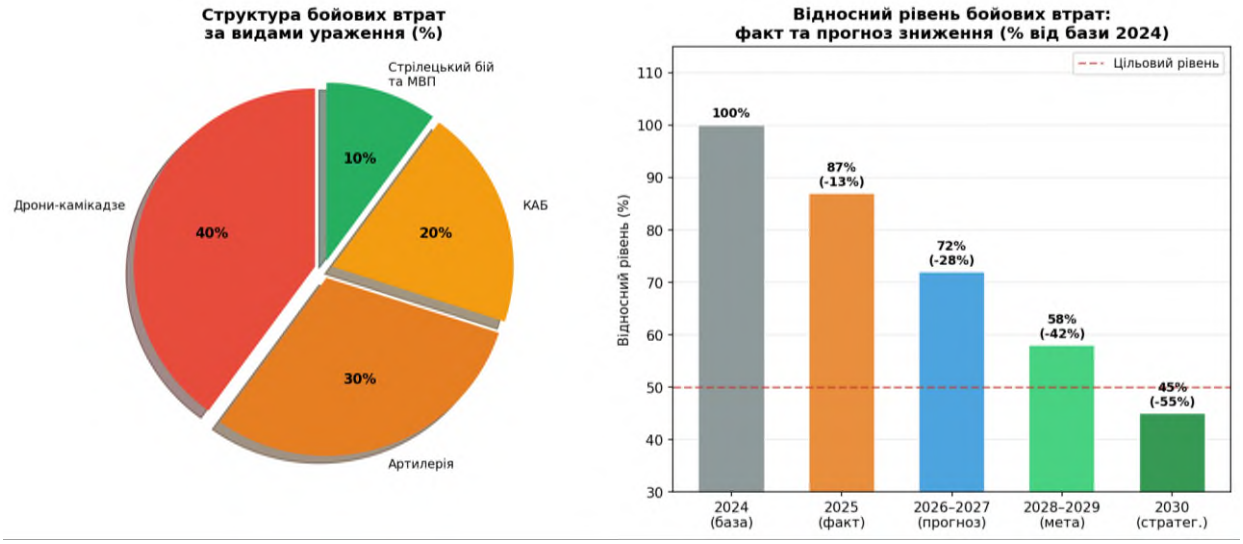


Рис. 2. Структура бойових втрат ЗС України за видами ураження
та прогноз динаміки їх зниження (оцінка авторів)

Концепція “кілнету” передбачає побудову інтегрованої мережі сенсорів і засобів ураження на всіх тактичних рівнях. Штатне насичення підрозділів операторами БпЛА та ударними дронами є базовою умовою досягнення переваги над противником і зниження власних втрат. При цьому, як свідчить прогноз (рис. 2, права частина), послідовне впровадження технологічних і тактичних заходів здатне забезпечити зниження відносного рівня втрат більш ніж удвічі порівняно з базовим показником.

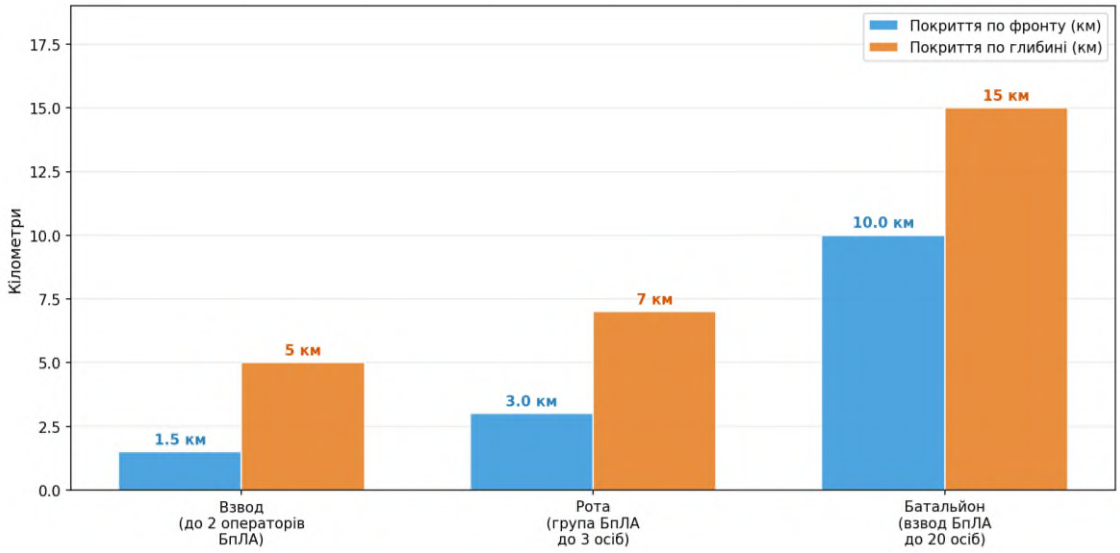


Рис. 3. Тактичне покриття системи “кілнету” за рівнями
організаційно-штатної структури ЗС України

Порівняльний аналіз мобілізаційного потенціалу України та росії за прогнозними горизонтами виявляє суттєву та зростаючу асиметрію. Реальний (а не лише формальний) мобілізаційний ресурс України формується під впливом демографічних втрат, міграції та стану здоров’я призовного контингенту. Значна частина потенційного ресурсу залишається недоступною через бронювання, стан здоров’я та перебування за кордоном.

Як свідчить рис. 4, пропорційна перевага мобілізаційного ресурсу рф наростає в динаміці. Це підкреслює, що для України ефективність використання наявного ресурсу, а не його кількість, є єдиним шляхом до стратегічної стійкості.

Саме тому реформування системи комплектування з упором на добровільність, прозорість і право вибору є критично необхідним.

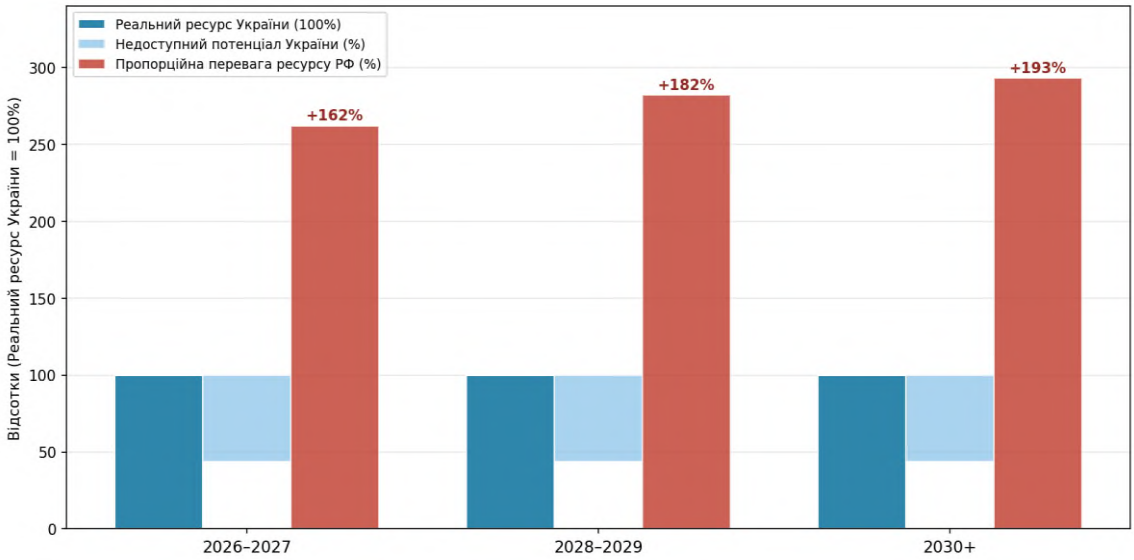


Рис. 4. Порівняльний баланс мобілізаційного ресурсу: відносна перевага рф та втрати потенціалу України (% до реального ресурсу України)

Окремою загрозою для мобілізаційної стійкості є небойові та поведінкові втрати, а саме самовільне залишення частин (СЗЧ), дезертирство, психологічні зриви. Дослідження свідчать, що ці явища є наслідком поєднання кількох чинників: по-перше, непрозорості мобілізаційних процесів та невизначеності щодо тривалості й умов служби; по-друге, відсутності чіткого права вибору формату служби; по-третє, несправедливого розподілу тягаря між різними категоріями громадян.

Зниження бойових втрат автоматично зменшує і поведінкові втрати. Коли воїн бачить, що ризик загибелі зменшується завдяки тактиці та організації, зростає довіра до командування і готовність залишатися в строю.

Крім того, запровадження прозорої системи строкових контрактів, де кожен громадянин заздалегідь знає умови, тривалість та обсяг соціальних гарантій, здатне суттєво знизити рівень ухилення від служби та поведінкових втрат.

Однією з найбільш перспективних реформ системи комплектування є запровадження варіативної системи строкових контрактів, яка надає кожному громадянину право обрати форму військової служби відповідно до власної готовності, стану здоров’я та сімейних обставин. Центральний принцип такої системи: чим більше ризикує військовослужбовець, тим коротший термін контракту, але тим вищий фінансовий та соціальний пакет для нього і його родини, і навпаки, плюс – до навпаки додається повна заборона будь-яких банківських розрахунків.

Така система вирішує кілька ключових проблем одночасно: знижує соціальну напругу, підвищує мотивацію, забезпечує прозорість мобілізаційних процесів і формує позитивний імідж військової служби в суспільстві. Громадяни, які обирають більш ризиковані варіанти контрактів, отримують максимальний соціальний і фінансовий захист; ті, хто обирає мінімальний ризик, служать довше, але з меншим пакетом пільг, тобто обидва варіанти є значно привабливішими за наслідки ухилення від служби.

Таблиця 1

Порівняльна характеристика варіантів строкових контрактів (якісна оцінка)

| Варіант контракту | Термін (роки) | Зона служби | Рівень ризику | Фін. привабливість | Соціальний пакет |
|---|---|---|---|---|---|
| Варіант 1 | 1 | 1-а лінія зіткнення | Максимальний | Максимальна | Максимальний |
| Варіант 2 | 3 | 1-а лінія зіткнення | Високий | Висока | Розширений |
| Варіант 3 | 4 | 2-а лінія / тил | Середній | Середня | Базовий+ |
| Варіант 4 | 5 | 2-а лінія / тил | Обмежений | Базова | Базовий |
| Варіант 5 | 7 | Не бойові частини | Мінімальний | Мінімальна | Мінімальний |

*Варіант 1* розраховано на тих, хто має бойовий досвід (статус учасника бойових дій) та готовий до проходження служби безпосередньо на лінії бойового зіткнення. Ці військовослужбовці мають право самостійно вибрати частину для проходження служби та направляються до неї за прямою військово-обліковою спеціальністю без додаткової підготовки. Протягом перших дев'яти десятих терміну контракту вони беруть участь у бойових діях із ротацією всередині підрозділу, після чого їм гарантується відпустка та ВЛК перед звільненням. Такий варіант є найбільш фінансово та соціально привабливим.

*Варіант 2* орієнтований на громадян, які не перебувають на обліку або тільки вступають на службу, включаючи жінок і призовників. Після підготовки в навчальних центрах (в тому числі на базах країн-членів НАТО) вони проходять службу на 1-й лінії бойового зіткнення з гарантованою ротацією, відпусткою та продовженням у ППД. Такий контракт забезпечує розширений соціальний пакет і може бути продовжений або трансформований в інший варіант.

*Варіанти 3 і 4* передбачають службу переважно у районах другої лінії або у тилових частинах з виконанням бойових і спеціальних завдань у встановлені цикли. Вони розраховані на тих, хто готовий до служби, але має застереження щодо безпосереднього перебування на лінії зіткнення. Термін служби за цими варіантами триваліший, фінансові умови є базовими, соціальний захист – достатній.

*Варіант 5* призначений для тих, хто обирає мінімальний ризик: служба в небойових частинах протягом семи років. Попри найдовший термін і мінімальний соціальний пакет, цей варіант все одно є значно привабливішим за наслідки ухилення, а саме: штрафи, блокування рахунків, відсутність можливості виїзду за кордон та будь-яких соціальних гарантій для себе особисто та своєї сім'ї.

Як ілюструє рис. 5, кожен варіант контракту являє собою цілісний, збалансований профіль: варіанти з вищим ризиком дають максимальну фінансову привабливість і соціальний пакет при мінімальній тривалості, тоді як варіанти з мінімальним ризиком вимагають найтривалішої служби при менших фінансових умовах. Право вибору залишається за громадянином.

Ефективність цієї системи посилюється через механізм "blackline" – прозоро визначені негативні наслідки для тих, хто ухиляється від виконання військового обов'язку: адміністративні штрафи, виконавче провадження, блокування банківських рахунків, заборона виїзду за кордон та відсутність будь-яких соціальних гарантій з боку держави. Таким чином, система створює реальну альтернативу: кожен громадянин обирає не між "служити" і "не служити", а між різними форматами виконання конституційного обов'язку.

Важливим доповненням до системи є персоналізований підхід до рекрутингу: відмова від практики "випадкових затримань" і перехід до адресних викликів через електронну систему "Резерв+" з фіксацією доставки повісток. Лише в разі ігнорування повістки відкривається кримінальне провадження. Розшук і затримання ухилянтів має бути компетенцією поліції, а не ЗС України.

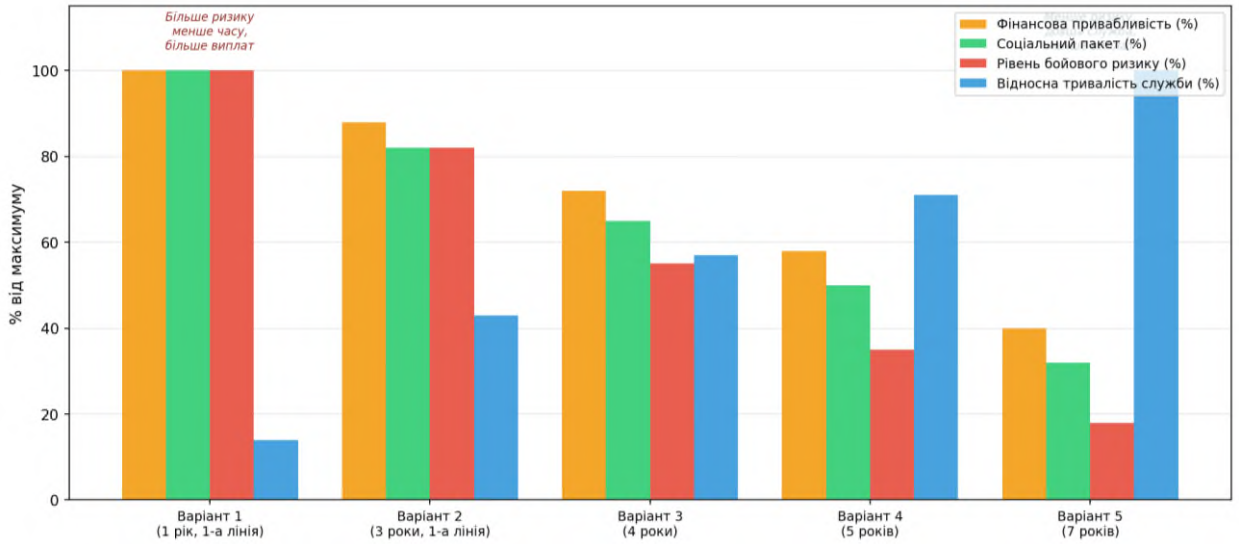


Рис. 5. Порівняльний профіль варіантів строкових контрактів
(у % від максимального значення за критерієм)

На основі аналізу поточного стану мобілізаційної системи, демографічних тенденцій та бойового досвіду ЗС України складено зведену аналітичну матрицю ключових викликів, загроз і наслідків у горизонті до 2030 р. (табл. 2).

Таблиця 2

Матриця викликів, загроз і наслідків за часовими горизонтами

| Часовий горизонт | Виклики | Загрози | Наслідки |
|---|---|---|---|
| **2026–2027** | Зростання частки небойових і поведінкових втрат (СЗЧ, дезертирство)<br>Нестача підготовлених командирів тактичної ланки<br>Вичерпання легкодоступного мобілізаційного ресурсу | Деградація бойової ефективності внаслідок низькоякісного поповнення<br>Соціальна напруга через несправедливість тягаря мобілізації<br>Ескалація через зниження кількісного паритету з рф | Підвищення навантаження на кожного бійця – зростання втомленості і ПТСР<br>Зниження довіри суспільства до ЗС України та інституцій<br>Загроза локальних проривів фронту через нестачу резервів |
| **2028–2029** | Демографічна криза: скорочення осіб призовного віку<br>Масштабна конкуренція між армією та ОПК за людський ресурс<br>Адаптація рф до технологічних засобів ЗС України | Виснаження навченого кадрового ядра ЗС України<br>Порушення логістики і ротацій через брак кваліфікованих тилових підрозділів<br>Зростання психологічних і поведінкових втрат у позиційній фазі | Можлива примусова демобілізація через медичні стандарти<br>Критична залежність від партнерів у питаннях озброєнь і фінансування<br>Ризик внутрішньополітичної нестабільності та кризи легітимності |
| **2029–2030** | Глибока демографічна депресія: призовний резерв скорочується критично<br>Перехід до повністю контрактної армії за недостатнього фінансування<br>Збереження мотивації у довготривалій фазі конфлікту | Структурний дефіцит особового складу без відновлення демографічного потенціалу<br>Ризик “розмивання” стратегічної культури та тиск на переговори<br>Можлива зупинка ротаційного циклу через брак підготовлених резервів | Довгострокова демографічна та соціальна травма суспільства<br>Ймовірне зниження обороноздатності без інституційної реформи ЗС України<br>Потреба у кардинальній реструктуризації системи комплектування |

Наведена матриця демонструє, що проблеми мобілізаційної стійкості мають виражений часовий характер ескалації. Якщо у 2026–2027 рр. переважно йдеться про управлінські виклики, то з 2028–2029 рр. на перший план виходять структурні демографічні та ресурсні загрози. До 2030 р. без системних реформ Україна може зіткнутися з критичним дефіцитом людського потенціалу для ведення оборони.

Сформуємо основні рекомендації щодо зміцнення мобілізаційної стійкості в сучасних умовах у разі продовження війни.

*1. Запровадження системи гнучких строкових контрактів*

Законодавчо закріпити варіативну систему строкових контрактів з правом вибору зони служби та тривалості. Ввести механізм авансових виплат для контрактів з підвищеним ризиком: право на отримання авансу грошового забезпечення виникає після отримання бойового розпорядження на виконання завдань на лінії безпосереднього зіткнення. Для контрактів типу "мінімальний ризик" передбачити довший термін, але гарантований соціальний мінімум. Перед закінченням контракту надавати право переходу на будь-який інший варіант.

Паралельно сформувати чіткий перелік негативних наслідків для ухилянтів: адміністративна відповідальність, виконавче провадження, блокування рахунків, відсутність права на виїзд за кордон та соціальних гарантій від держави. Ці заходи мають бути не каральними, а мотивуючими, тобто завжди менш вигідними, ніж будь-який з варіантів контракту.

*2. Технологічне і тактичне зниження бойових втрат*

Пріоритетне штатне насичення піхотних підрозділів (взвод–рота–батальйон) операторами БпЛА та безпілотними ударними комплексами. Введення до штату батальйону групи вогневого ураження і перспективного взводу наземних роботизованих комплексів (НРК). Уніфікація класів БпЛА, нормування витрат дронів як боєприпасів. Розвиток дронів-перехоплювачів і пріоритетне знищення операторів БпЛА противника.

*3. Антидронова оборона і пасивний захист*

Масове впровадження детекторів дронів і акустичних засобів виявлення на позиціях. Обов'язкове обладнання перекритих ходів сполучення, "лисячих нір", укриттів і протидронових сіток. Жорстка дисципліна радіообміну та обмеження використання смартфонів у зоні бойових дій.

*4. Стандартизовані операційні процедури (СОП) і підготовка*

Розробка і впровадження єдиних СОП для дій у "прозорому бою". Збільшення тривалості підготовки мобілізованих, система менторства для молодих командирів, масове навчання тактичної медицини. Регулярні тренування з імітацією дронових і артилерійських ударів.

*5. Реформа мобілізаційного обліку та бронювання*

Перехід від "випадкових затримань" до персоналізованого виклику через систему "Резерв+" з фіксацією доставки. Аудит і перегляд критеріїв бронювання, введення "позиційного бронювання": бронювати лише критичні посади, а не штати підприємств. Заміщення броньованих посад жінками, особами з обмеженою придатністю та пенсіонерами. Прозорий перелік підприємств із правом бронювання в публічному доступі.

*6. Мотивація, утримання кадрів та морально-психологічна стійкість*

Диференційоване грошове забезпечення залежно від рівня ризику, прозорі ротаційні цикли з визначеними строками, розширення житлових програм і освіти дітей військовослужбовців. Щомісячні відкриті брифінги командування з поясненням логіки рішень і поточних викликів. Багаторівнева система психологічної підтримки з обов'язковим скринінгом ПТСР. Інституалізація взаємодії "громада–військо" – публічні звіти ТЦК, інформаційні сесії про права, пільги та варіанти служби.

## Дискусія

Отримані результати підтверджують і суттєво поглиблюють висновки попередніх досліджень у суміжних областях. Встановлена структура бойових втрат, де дрони-камікадзе, артилерія та керовані авіабомби разом становлять понад дев'яносто відсотків усіх втрат, узгоджується з даними RAND Corporation (2024) щодо трансформації характеру втрат у сучасних конфліктах при масовому застосуванні безпілотних систем [11]. Водночас виявлена нами конкретна питома вага кожного виду ураження на українському театрі воєнних дій є оригінальним результатом, що уточнює загальні тенденції. Висновок про те, що зниження якості мобілізаційного ресурсу є більшою загрозою, ніж його кількісна нестача, підтверджено в попередніх дослідженнях Павловського О.В. (2023) та Черепа В.Л. (2023) [6, 8]. Наше дослідження не лише підтверджує цю тезу, а й кількісно ілюструє її через динаміку індексів втрат і поповнення, що дозволяє перейти від якісної констатації до вимірюваного управлінського індикатора. Концепція системи гнучких строкових контрактів, розроблена Семененком О.М. та Ковалем В.В. [1], набуває в цьому дослідженні додаткового обґрунтування через аналіз поведінкових і небойових втрат: показано, що саме прозорість умов служби і право вибору знижують рівень самовільного залишення частин і дезертирства. Це перегукується з висновками Avis (2023) щодо ролі сприйнятої справедливості мобілізаційного тягаря у формуванні суспільної підтримки [15]. Порівняння мобілізаційних потенціалів України та Росії корелює з аналітикою IISS (2024), однак виявлена нами траєкторія наростаючої асиметрії до 2030 р. є більш песимістичною, ніж більшість наявних прогнозів [13]. Це пояснюється тим, що ми враховуємо комплексний вплив міграції, надлишкової смертності та скорочення частки населення призовного віку, тоді як частина попередніх досліджень спирається переважно на формальний демографічний потенціал. Таким чином, отримані результати не лише підтверджують висновки попередніх досліджень, а й поглиблюють їх, вводячи нові вимірювані параметри та пропонуючи конкретний інструментарій реформування системи комплектування.

## Висновки

Мобілізаційна стійкість України у війні на виснаження є багатовимірною стратегічною проблемою. Центральним пріоритетом є системне зниження бойових і небойових втрат, а не механічне нарощування мобілізаційного потоку. Лише збереження кожного підготовленого бійця забезпечує реальну стійкість армії.

Поряд із технологічними заходами (перевага у "кілнеті", антидронова оборона, SOP) критично важливою є реформа самої системи комплектування. Запровадження системи гнучких строкових контрактів з правом вибору формату служби здатне якісно змінити ставлення суспільства до мобілізації: замість примусу і соціального стресу – усвідомлений вибір громадянина між варіантами з різним рівнем ризику, тривалості та винагороди.

Аналіз за горизонтами 2026–2030 рр. свідчить, що демографічні та ресурсні обмеження наростатимуть, що вимагає якісно нових рішень вже зараз. Реалізація запропонованого комплексу заходів здатна суттєво підвищити мобілізаційну стійкість держави та забезпечити ЗС України достатній людський потенціал для ведення тривалої оборони.

## Список використаних джерел

1. Семененко О., Коваль В., Добровольський Ю., Царинник В., Ованесян Р. "Таймлайн"-мобілізація – шлях від примусу до популяризації військової служби в умовах війни: право вибору – спосіб ефективного комплектування людськими ресурсами. *Military Science.* 2024. Vol. 2 № 2. С.159-179. URL: https://doi.org/10.62524/msj.2024.2.2.14.
2. Про внесення змін до деяких законодавчих актів України щодо окремих питань проходження військової служби, мобілізації та військового обліку: Закон України від 11.04.2024 № 3633-IX. *Відомості Верховної Ради України.* 15.05.2024 № 19. С. 2. Ст. 78; *Голос України.* 17.04.2024 № 16.

3. Bramsen I. Peace Talks in the Russia-Ukraine War: When, Who, and How. DIVA-Portal, 2025.
4. Russia's War in Ukraine: The Next Chapter. Center for Strategic and International Studies. *CSIS*. 2025.
5. Семененко О., Воронченко І., Москаленко І., Абрамова М., Харитонов К. Методологічний підхід до оцінки здатності національної економіки забезпечити достатній рівень обороноздатності. *Social Development and Security*. 2021. № 11(5). С. 133–145. URL: https://doi.org/10.33445/sds.2021.11.5.13.
6. Романченко І. С., Талалай В. Д. Рекомендації щодо удосконалення системи мобілізаційного розгортання Збройних Сил України. *Зб. наук. пр. ЦНДІ ЗС України*. 2017. № 2 (80). С. 51–62.
7. Ministerio de Defensa (Spain). (2025). Ukraine 2024. Is a good war better than a bad peace? PDF Report.
8. Павловський О. В. Результати аналізу чисельності мобілізаційних людських ресурсів України на початок 2023 року. Зб. наук. пр. ЦНДІ ЗС України. 2023. № 1 (104). С. 5–14.
9. Соломицький А., Семененко О., Онофрійчук П., Слюсаренко М., Баранов С., Мітченко, С. Прогнозування ризику збройного конфлікту на основі аналізу військових витрат. *Соціальний розвиток і безпека*. 2022. № 12 (1). С. 164–174. URL: https://doi.org/10.33445/sds.2022.12.1.15.
10. The Talks That Could Have Ended the War in Ukraine. *Foreign Affairs.* 2024.
11. Lessons from the Battlefield: Drone Warfare and Casualty Dynamics in Modern Conflict. *RAND Corporation.* 2024. RAND Research Report.
12. Watling J., Reynolds N. Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine. *Royal United Services Institute (RUSI).* 2023. Special Report.
13. International Institute for Strategic Studies (IISS). The Military Balance 2024. London : Routledge, 2024.
14. Kofman M., Lee R. Not Built for Purpose: The Russian Military's Ill-Fated Force Design. War on the Rocks, 2023.
15. Avis W. R. Public Support for Military Recruitment and Conscription in Conflict Settings. K4D Helpdesk Report. 2023. Institute of Development Studies.
16. NATO Support and Procurement Agency: Lessons Learned from Ukraine. *NATO.* 2024. NSPA Report.
17. Giles K. Russian Mobilization and Manpower: Capacity, Constraints and Consequences. Chatham House Research Paper, 2024.
18. Череп В. Л. Якісні характеристики мобілізаційного ресурсу України в умовах збройного конфлікту. *Зб. наук. пр. ЦНДІ ЗС України.* 2023. № 2 (105). С. 15–26.
19. Баргилевич А., Кириленко В., Павлюк О., Войтко О., Дідіченко, В. Обґрунтування перспективної системи мобілізації України: планування людського ресурсу в умовах кризових ситуацій. *Military Science*. 2026. № 3(4). С. 40-57. URL: https://doi.org/10.62524/msj.2025.3.4.3.
20. Biddle S. Causes of Attrition in Modern Warfare: Firepower, Terrain, and Force Design. *Journal of Strategic Studies*, 2023. № 46 (4). P. 712–745.
21. McFate S. The Logic of Attrition: Why Wars of Exhaustion Are Won or Lost Before the First Battle. *Parameters: US Army War College Quarterly*. 2024. № 54 (1).
22. Колесніков В. О., Романченко І. С. Оцінка мобілізаційного потенціалу держави в умовах збройної агресії: методологічний аспект. *Наука і оборона.* 2022. № 3. С. 3–11.

## References

1. Semenenko, O., Koval, V., Dobrovolskyi, Yu., Tsarynnyk, V., & Ovanesian, R. (2024). "Taimlain"-mobilizatsiia – shliakh vid prymusu do populiaryzatsii viiskovoi sluzhby v umovakh viiny: pravo vyboru – sposib efektyvnoho komplektuvannia liudskymy resursamy ["Timeline" mobilization – the path from coercion to popularization of military service in wartime: the right to choose – a way of effective recruitment of human resources]. *Military Science*, 2, 2, 159-179. Retrieved from: https://doi.org/10.62524/msj.2024.2.2.14 [in Ukrainian].
2. On Amendments to Certain Legislative Acts of Ukraine Regarding Certain Issues of Military Service, Mobilization and Military Registration: Law of Ukraine № 3633-IX (2024, April 11). *Vidomosti Verkhovnoi Rady Ukrainy*, 19, 2, 78; *Holos Ukrainy*, 16 [in Ukrainian].
3. Bramsen, I. (2025). Peace Talks in the Russia-Ukraine War: When, Who, and How. DIVA-Portal.
4. CSIS. (2025). Russia's War in Ukraine: The Next Chapter. Center for Strategic and International Studies.
5. Semenenko, O., Voronchenko, I., Moskalenko, I., Abramova, M., & Kharytonov, K. (2021). Metodolohichnyi pidkhid do otsinky zdatnosti natsionalnoi ekonomiky zabezpechyty dostatnii riven oboronozdatnosti [Methodological approach to assessing the ability of the national economy to provide a sufficient level of defense capability]. *Social Development and Security*, 11(5), 133–145. Retrieved from: https://doi.org/10.33445/sds.2021.11.5.13 [in Ukrainian].
6. Romanchenko, I. S., & Talalai, V. D. (2017). Rekomendatsii shchodo udoskonalennia systemy mobilizatsiinoho rozghortannia Zbroinykh Syl Ukrainy [Recommendations for improving the system of mobilization deployment of the Armed Forces of Ukraine]. *Zbirnyk naukovykh prats Tsentralnoho naukovo-doslidnoho instytutu ozbroiennia ta viiskovoi tekhniky Zbroinykh Syl Ukrainy*, 2 (80), 51–62 [in Ukrainian].
7. Ministerio de Defensa (Spain). (2025). Ukraine 2024. Is a good war better than a bad peace? PDF Report.

8. Pavlovskyi, O. V. (2023). Rezultaty analizu chyselnosti mobilizatsiinykh liudskykh resursiv Ukrainy na pochatok 2023 roku [Results of the analysis of the number of mobilization human resources of Ukraine at the beginning of 2023]. *Zbirnyk naukovykh prats Tsentralnoho naukovo-doslidnoho instytutu ozbroiennia ta viiskovoi tekhniky Zbroinykh Syl Ukrainy*, 1 (104), 5–14 [in Ukrainian].
9. Solomytskyi, A., Semenenko, O., Onofriichuk, P., Sliusarenko, M., Baranov, S., & Mitchenko, S. (2022). Prohnozuvannia ryzyku zbroinoho konfliktu na osnovi analizu viiskovykh vytrat [Forecasting the risk of armed conflict based on the analysis of military spending. Social Development and Security]. *Social Development and Security*, 12 (1), 164–174. Retrieved from: https://doi.org/10.33445/sds.2022.12.1.15 [in Ukrainian].
10. Foreign Affairs. (2024). The Talks That Could Have Ended the War in Ukraine.
11. Lessons from the Battlefield: Drone Warfare and Casualty Dynamics in Modern Conflict. *RAND Corporation.* 2024. RAND Research Report.
12. Watling, J., & Reynolds, N. (2023). Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine. *Royal United Services Institute (RUSI).* Special Report.
13. International Institute for Strategic Studies (IISS). (2024). The Military Balance 2024. London: Routledge.
14. Kofman, M., & Lee, R. (2023). Not Built for Purpose: The Russian Military's Ill-Fated Force Design. War on the Rocks.
15. Avis, W. R. (2023). Public Support for Military Recruitment and Conscription in Conflict Settings. K4D Helpdesk Report. Institute of Development Studies.
16. NATO. (2024). NATO Support and Procurement Agency: Lessons Learned from Ukraine. NSPA Report.
17. Giles, K. (2024). Russian Mobilization and Manpower: Capacity, Constraints and Consequences. Chatham House Research Paper.
18. Cherep, V. L. (2023). Yakisni kharakterystyky mobilizatsiinoho resursu Ukrainy v umovakh zbroinoho konfliktu [Qualitative characteristics of the mobilization resource of Ukraine in conditions of armed conflict]. *Zbirnyk naukovykh prats Tsentralnoho naukovo-doslidnoho instytutu ozbroiennia ta viiskovoi tekhniky Zbroinykh Syl Ukrainy*, 2 (105), 15–26 [in Ukrainian].
19. Barhylevych, A., Kyrylenko, V., Pavliuk, O., Voitko, O., & Didichenko, V. (2026). Obgruntuvannia perspektyvnoi systemy mobilizatsii Ukrainy: planuvannia liudskoho resursu v umovakh kryzovykh sytuatsii [Justification of the prospective mobilization system of Ukraine: human resource planning in crisis situations]. *Military Science*, 3(4), 40-57. Retrieved from: https://doi.org/10.62524/msj.2025.3.4.3 [in Ukrainian].
20. Biddle, S. (2023). Causes of Attrition in Modern Warfare: Firepower, Terrain, and Force Design. *Journal of Strategic Studies*, 46 (4), 712–745.
21. McFate, S. (2024). The Logic of Attrition: Why Wars of Exhaustion Are Won or Lost Before the First Battle. *Parameters: US Army War College Quarterly*, 54 (1).
22. Kolesnikov, V. O., & Romanchenko, I. S. (2022). Otsinka mobilizatsiinoho potentsialu derzhavy v umovakh zbroinoi ahresii: metodolohichnyi aspekt [Assessment of the mobilization potential of the state in conditions of armed aggression: methodological aspect]. *Science and Defense*, 3, 3–11 [in Ukrainian].

*Received 04.02.2026 | Accepted 20.02.2026 | Published 30.03.2026*



УДК 004 DOI: 10.63978/3083-6476.2026.1.4.05

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

# КВАНТОВІ ТЕХНОЛОГІЇ В ОБОРОНІ І БЕЗПЕЦІ

***Анотація.*** *Досліджено квантові технології та перспективи їх використання в обороні і безпеці. Розглянуто квантові обчислення, квантовий зв'язок, квантові сенсори. Наведено основні напрямки застосування квантових обчислень у кібербезпеці: детекція та аналіз кіберзагроз, квантове шифрування, квантова криптографія, постквантова криптографія.*

***Ключові слова****: квантові технології, квантові обчислення, квантові сенсори, квантовий зв'язок, квантове шифрування, квантова криптографія, кібербезпека.*

# QUANTUM TECHNOLOGIES IN DEFENSE AND SECURITY

**Lysetsyi Yurii**
*Doctor of Engineering Sciences,*
*associate professor*
*Yevhenii Bereznyak Military Academy*
*Kyiv, Ukraine*
*e-mail: Yurii.Lysetskyi@snt.ua*
*ORCID: 0000-0002-5080-1856*

***Abstract****. The article focuses on quantum technologies and the prospects for their application in the defense and security sectors. Based on an analysis of the current state of development of quantum technologies and their applications in defense and security, three main areas are identified: quantum computing, quantum communication, and quantum sensors. For each of these, a specific set of applications, advantages, and limitations is identified. It is noted that quantum computing in defense and security finds application primarily in four subfields: post-quantum cryptography, quantum cryptography, cyber threat detection, and cryptanalysis; quantum communication ensures secure information transmission by utilizing the physical properties of quantum states, particularly the principle of the impossibility of cloning a quantum state, with its primary practical application being Quantum key distribution and its promising application being the quantum internet; quantum sensors are the category of quantum technologies closest to operational deployment, as they utilize the hypersensitivity of quantum states to external disturbances to achieve measurement accuracy unattainable by classical devices. A summary of the main areas of application for quantum technologies in defense and security indicates that quantum sensors have the nearest practical implementation horizon (5–7 years), while quantum computing will have the greatest strategic impact on cryptographic infrastructure due to the threat it poses to existing asymmetric encryption algorithms—which is precisely why the transition to post-quantum standards is becoming urgent. Therefore, given the significant interest in and funding for quantum technologies from both the civilian industry and governments, it is expected that these technologies will continue to develop and new quantum applications will become available over the next five to ten years, and new advances in the development of quantum technologies may bring new opportunities for the military, but for the military to actually reap the benefits of new quantum technologies, they need to actively engage in this field and guide the development and implementation of military applications of quantum technologies.*

***Keywords:*** *quantum technologies, quantum computing, quantum sensors, quantum communication, quantum encryption, quantum cryptography, cybersecurity.*

**JEL Classification:** O32, H56, L86, O33

## Вступ

Квантові технології несуть з собою нові можливості як в цивільному, так і військовому застосуванні, і вони останнім часом залучили до себе великий інтерес з боку промисловості і урядів. Великі технологічні компанії витрачають сотні мільйонів доларів на науково-дослідні роботи в галузі квантових обчислень [1]. Так само, уряди визнали трансформаційний потенціал і геополітичну цінність застосувань квантової технології, і США, Європейський союз і Китай започаткували власні дослідницькі програми вартістю у мільярди доларів. Зважаючи на потенційні наслідки новітніх квантових технологій для оборони і безпеки, НАТО визначає квантові технології як один із провідних нових технологічних напрямків за впливом на оборону і безпеку.

## Огляд літератури

Аналіз наукових публікацій засвідчує зростаючий інтерес дослідницької спільноти до проблематики застосування квантових технологій у сферах оборони та безпеки. Ключові напрямки досліджень охоплюють три взаємопов'язані домени: квантові обчислення та їх вплив на криптографічну інфраструктуру; квантовий зв'язок і розподіл ключів; квантові сенсори для задач розвідки та навігації.

Загальний огляд перспектив використання квантових технологій наданий у роботі Данилюка І. А. та інших [2], де систематизовано ключові напрямки квантових досліджень і сформульовано прогноз щодо їх впливу на інформаційні та комунікаційні системи. Практичні аспекти застосування квантових технологій для потреб кіберзахисту розглядаються у публікації Лисецького Ю. М., Боханченка О. С., Сурми А. І. [3], де описано конкретні сценарії протидії кіберзагрозам на основі квантових методів.

Стандартизація постквантової криптографії стала визначальною подією 2024 року. Після шестирічного міжнародного конкурсу Національний інститут стандартів і технологій США (National Institute of Standards and Technology, NIST) у серпні 2024 року опублікував три фінальні стандарти постквантових алгоритмів: FIPS 203 (ML-KEM, на основі CRYSTALS-Kyber), FIPS 204 (ML-DSA, на основі CRYSTALS-Dilithium) та FIPS 205 (SLH-DSA, на основі SPHINCS+) [4]. Ці алгоритми спираються на математичні задачі, що вважаються стійкими до квантових атак, зокрема задачі на ґратках та задачі геш-функцій, і призначені для заміни вразливих RSA (Rivest, Shamir та Adleman), DSA (Digital Signature Algorithm) та ECC (Elliptic Curve Cryptography). NIST розробляє також FIPS 206 на основі алгоритму FALCON як додатковий стандарт цифрових підписів.

Комплексний аналіз впливу квантових обчислень на кібербезпеку здійснено у публікації Саху С. та Мазумдара К. "State-of-the-art analysis of quantum cryptography: applications and future prospects" (*Frontiers in Physics*, 2024), де систематизовано загрози від алгоритмів Шора та Гровера [5] щодо асиметричних і симетричних шифрів, а також проаналізовано методи протидії – постквантову криптографію та квантовий розподіл ключів. Огляд Алі С. та інших авторів деталізує технічні та організаційні виклики впровадження PQC (Post-Quantum Cryptography) і QKD (Quantum Key Distribution) у реальних системах безпеки [6].

Проблема "Harvest Now, Decrypt Later" (HNDL) – стратегія зберігання зашифрованих даних з метою їх подальшого розкодування квантовим комп'ютером – набуває практичного значення вже сьогодні. Аналітичний центр Soufan Center у доповіді 2024 року "Quantum Computing and the Evolving Cyber Threat Landscape" фіксує свідчення

того, що державні актори вже реалізують цю стратегію [7], що надає переходу на постквантові алгоритми невідкладного, а не лише перспективного характеру. Рахункова палата США (Government Accountability Office, GAO) у доповіді "Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy" (листопад 2024) констатує, що федеральні агентства досі не сформували повноцінної стратегії протидії цим загрозам [8].

Квантовий розподіл ключів є найбільш зрілою з квантових комунікаційних технологій. Огляд "Quantum Key Distribution Networks – Key Management: A Survey" (2024 р.) систематизує топологію QKD-мереж, схеми управління ключами та інтеграцію з класичними мережами [9]. Практичні розгортання 2022–2023 років – мережа QKD JPMorgan Chase у США та приєднання HSBC до квантово-захищеної мережі в Лондоні – демонструють прийнятність технології для захисту критичної інфраструктури [10]. Водночас критичний аналіз (International Association for Cryptologic Research, IACR) у 2025 році вказує на суттєві обмеження QKD: залежність від прямого оптичного з'єднання, обмежена дальність без квантових ретрансляторів, висока вартість – через що NSA (National Security Agency) США і ряд інших регуляторів рекомендують PQC як більш практичний підхід [11].

Квантові сенсори для задач навігації та розвідки являють собою найближчий для впровадження клас квантових технологій для військового застосування. Публікація "How Quantum Sensing Will Help Solve GPS Denial in Warfare" (Lawrence Livermore National Laboratory) у 2024 році підкреслює, що квантові інерціальні сенсори на основі атомної інтерферометрії забезпечують більш ніж десятикратну перевагу за стабільністю порівняно з класичними інерціальними системами [12].

DARPA (Defense Advanced Research Projects Agency) реалізує програму Robust Quantum Sensors (RoQS), в рамках якої компанія Q-CTRL отримала контракти на 24,4 млн дол. США; у льотних випробуваннях система Ironstone Opal продемонструвала точність навігації в 111 разів вищу за класичний аналог за відсутності сигналу GPS (Global Positioning System) [12]. Defense Innovation Unit паралельно розвиває програму Transition of Quantum Sensing (TQS) для прискорення впровадження цих технологій у реальні військові платформи [13].

Аналіз квантового машинного навчання (Qt Modeling Language, QML) для задач виявлення кіберзагроз систематизовано у публікації "Quantum key distribution through quantum machine learning: a research review" (*Frontiers in Quantum Science and Technology*, 2025), де показано потенціал QML для покращення виявлення аномалій і підвищення надійності криптографічних систем [11]. Доповідь Congressional Research Service "Defense Primer: Quantum Technology" (2024 р.) підсумовує військовий потенціал усіх трьох класів квантових технологій – обчислень, зв'язку та сенсорів – і наголошує на необхідності активного залучення збройних сил до формування вимог та участі у випробуваннях [14].

Таким чином, аналіз наукової літератури підтверджує, що квантові технології перейшли від теоретичного до прикладного етапу розвитку. Ключовими дослідницькими лакунами залишаються: стратегії міграції наявних систем безпеки на постквантові стандарти в умовах обмежених ресурсів; практичні рішення для розгортання QKD на тактичному рівні (включаючи мобільні та безпровідні сценарії); та інтеграція квантових сенсорів у спільні системи управління, навігації та розвідки збройних сил.

## Мета та завдання статті

Дослідження можливостей використання квантових технологій у секторі оборони і безпеки.

## Методи

У процесі дослідження використовувалися загальнонаукові і спеціальні методи, а саме: системного аналізу, системно-функціональний; теоретичного узагальнення, факторних порівнянь та експертних оцінок.

## Результати

На основі аналізу сучасного стану розвитку квантових технологій та їх застосувань у сфері оборони і безпеки можна виокремити три основних напрямки: *квантові обчислення, квантовий зв'язок та квантові сенсори*. Для кожного з них характерний специфічний набір застосувань, переваг і обмежень.

***Напрямок 1. Квантові обчислення***

Квантові обчислення здатні кардинально змінити баланс сил у кіберпросторі. В обороні і безпеці вони знаходять застосування передусім у чотирьох підгалузях: постквантовій криптографії, квантовій криптографії, детекції кіберзагроз та криптоаналізі.

Постквантова криптографія (PQC). Розробка та впровадження криптографічних алгоритмів, стійких до атак з боку квантових комп'ютерів. Після завершення стандартизаційного конкурсу NIST у 2024 році галузь отримала три перших стандарти: ML-KEM (FIPS 203), ML-DSA (FIPS 204) та SLH-DSA (FIPS 205).

*Переваги:* реалізується на класичному обладнанні без необхідності у квантовій апаратурі; алгоритми сумісні з наявними мережевими протоколами TLS (Transport Layer Security), SSH (Secure Shell ); дозволяє захистити інформацію від стратегії "збережи зараз – розшифруй пізніше"; міграція може здійснюватись поетапно.

*Недоліки:* значно більший розмір ключів і підписів порівняно з RSA/ECC (наприклад, публічний ключ ML-KEM-1024 – 1568 байт проти 256 байт у ECC-256); підвищене обчислювальне навантаження на обмежені пристрої; математична стійкість нових алгоритмів не є повністю доведеною – зберігається теоретичний ризик появи нових класичних або квантових атак; перехід вимагає масштабного оновлення IT-інфраструктури, що є витратним і тривалим.

Квантова криптографія (QKD-забезпечення). Застосування принципів квантової механіки для гарантування таємності криптографічних ключів. Протоколи BB84 [15] та E91 [16] забезпечують фізично обґрунтовану неможливість непоміченого перехоплення.

*Переваги:* "інформаційно-теоретична" безпека (Information-Theoretical Security, ITS) – захист не залежить від обчислювальних можливостей противника; будь-яка спроба перехоплення автоматично виявляється; не потребує постійного оновлення алгоритмів.

*Недоліки:* потребує спеціалізованого апаратного забезпечення (одиночні фотони, кріогенні детектори); дальність без ретрансляторів обмежена ~100–300 км по оптоволокну; не захищає від атак на кінцеві вузли, а лише на канал передачі ключів; висока вартість розгортання; несумісність з радіоканалами, що критично для тактичного рівня.

Детекція та аналіз кіберзагроз на основі QML (Qt Modeling Language). Використання квантового машинного навчання для прискорення виявлення аномалій у мережевому трафіку та класифікації зловмисного програмного забезпечення.

*Переваги:* теоретична квадратична або експоненційна перевага в обробці великих масивів даних; потенціал для виявлення складних прихованих кореляцій; можливість прискорення задач оптимізації в системах SOC (Security Operations Center).

*Недоліки:* сучасні NISQ-процесори (Noisy Intermediate-Scale Quantum) ще не забезпечують стабільного переважання над класичним ML на реальних задачах безпеки; обмежена кількість кубітів не дозволяє обробляти масштаб реальних датасетів; алгоритми QML чутливі до шуму квантових обчислень; практичне впровадження у бойові системи кібербезпеки не очікується раніше кінця десятиліття.

***Напрямок 2. Квантовий зв'язок***

Квантовий зв'язок забезпечує захищену передачу інформації, використовуючи фізичні властивості квантових станів, зокрема принцип неможливості клонування квантового стану. Основним практичним застосуванням є QKD; перспективним – квантовий інтернет.

Квантові мережі зв'язку (QKD-мережі). Розгортання мереж для обміну криптографічними ключами між стратегічними об'єктами. Китай у 2016 році запустив перший квантовий комунікаційний супутник "Міціус" і продемонстрував міжконтинентальний QKD [2]; НАТО та США активно фінансують наземні мережі QKD.

*Переваги:* фізично гарантована таємність каналу розподілу ключів; захищеність від будь-яких майбутніх обчислювальних атак; виявлення підслуховування в реальному часі; супутниковий QKD усуває обмеження відстані наземних мереж.

*Недоліки:* наземні мережі вимагають прокладки спеціалізованої оптоволоконної інфраструктури або розгортання довірених ретрансляторів, кожен з яких є потенційною точкою компрометації; супутникові рішення залежать від погодних умов і часових вікон видимості; технологія не розрахована на мобільні або тактичні застосування; глобальна мережа QKD потребує вирішення проблеми квантових ретрансляторів, яка наразі не має масштабованого рішення.

Квантовий інтернет. Перспективна архітектура глобальної мережі взаємопов'язаних квантових комп'ютерів з ультразахищеними комунікаційними каналами.

*Переваги:* потенційно абсолютно захищений зв'язок між командними пунктами і платформами; можливість розподілених квантових обчислень для вирішення тактичних задач оптимізації.

*Недоліки:* знаходиться на ранніх стадіях досліджень; відсутність масштабованих квантових ретрансляторів є критичним бар'єром; горизонт практичного розгортання – щонайменше 10–15 років; надзвичайно висока вартість розробки і підтримки.

***Напрямок 3. Квантові сенсори***

Квантові сенсори є найбільш близькою до бойового впровадження категорією квантових технологій. Вони використовують надчутливість квантових станів до зовнішніх збурень для вимірювання з точністю, недосяжною для класичних приладів [17].

Квантова навігація (PNT – Positioning, Navigation, and Timing без GPS). Системи позиціонування, навігації та синхронізації часу, що не потребують зовнішніх сигналів (GPS/GNSS – Global Navigation Satellite System) і стійкі до радіоелектронної боротьби. Базуються на квантових акселерометрах (атомна інтерферометрія), квантових гіроскопах, квантових магнетометрах і квантових гравіметрах.

*Переваги:* повна незалежність від зовнішніх сигналів; стійкість до придушення та спуфінгу GPS, що є критичним у сучасних зонах бойових дій; досягнута точність Ironstone Opal (Q-CTRL) у 50 разів вища за традиційні GPS-системи і перевершила інші несупутникові системи (ІНС) у тестових польотах в 11 разів [18]; застосовність для підводних човнів, де GPS недоступний; пасивна робота – без випромінювання сигналів, що забезпечує прихованість.

*Недоліки:* поточні системи ще мають значні габарити та масу, що ускладнює розміщення на малих платформах; висока чутливість до вібрацій і механічних збурень (проблема "розгортання на рухомих платформах"); потребує попереднього завантаження детальних магнітних або гравітаційних карт місцевості; висока вартість і складність в обслуговуванні; необхідність регулярного калібрування.

Квантові радари та системи виявлення. Використання заплутаних фотонів для виявлення малопомітних об'єктів (літаків-невидимок, підводних човнів) і виявлення підземних споруд.

*Переваги:* теоретична здатність виявляти об'єкти зі зниженою ЕПР (ефективна площа розсіювання), недосяжні для класичних систем РЛС; можливість виявлення підводних об'єктів через гравітаційні та магнітні аномалії; розширені можливості ISR (Intelligence, Surveillance, Reconnaissance) для виявлення прихованих сил противника.

*Недоліки:* квантові радари дальньої дії поки що залишаються переважно теоретичною концепцією; практичні дальності виявлення суттєво обмежені втратами заплутаних фотонів у реальному середовищі; складність формування і підтримки заплутаних пар фотонів у польових умовах; чутливість до атмосферних завад.

Квантові атомні годинники та синхронізація. Еталони часу з точністю $10^{-18}$ для задач синхронізації розподілених мереж, точного наведення та розвідки.

*Переваги:* дрейф менше 0,3 наносекунди за 20 днів (зафіксовано у морських випробуваннях Vector Atomic у 2022 р.); можливість заміни рубідієвих еталонів часу на борту GPS-супутників; критична роль у забезпеченні точності систем наведення та зв'язку.

*Недоліки:* обмеження за розміром і енергоспоживанням для мобільного застосування; необхідність вакуумних камер та лазерних систем охолодження; чутливість до магнітних полів і вібрацій.

Узагальнення основних напрямків застосування квантових технологій в обороні і безпеці свідчить, що найближчий горизонт практичного впровадження мають квантові сенсори (5–7 років), а найбільший стратегічний вплив на криптографічну інфраструктуру матимуть квантові обчислення через загрозу існуючим алгоритмам асиметричного шифрування – саме тому перехід на постквантові стандарти набуває невідкладного характеру вже сьогодні.

## Дискусія

Незважаючи на значний теоретичний і практичний потенціал квантових технологій для оборони і безпеки, їх реальне використання стикається з цілою низкою серйозних проблем, з якими фахівці у кожному з напрямків неминуче зіткнуться вже найближчими роками.

***Проблеми використання квантових обчислень***

Найближча і найбільш практично значуща проблема – це невизначеність щодо темпів розвитку криптографічно значимих квантових комп'ютерів (Cryptographically Relevant Quantum Computer, CRQC). Фахівцям з кібербезпеки доводиться проектувати захищені системи без точного розуміння того, коли CRQC стане реальністю. Оцінки варіюються від 5 до 20+ років, що ускладнює планування міграції. При цьому стратегія HNDL (Have Now, Decode Later) вже активна: зловмисники збирають зашифровані дані сьогодні з розрахунку на майбутнє. Це означає, що фахівці, відповідальні за захист інформації з тривалим строком конфіденційності (державна таємниця, медичні дані, фінансові записи), вже перебувають під загрозою, навіть якщо CRQC з'явиться лише через десятиліття.

Перехід на постквантові алгоритми, хоча і технічно здійсненний, є надзвичайно ресурсоємним. Фахівці стикаються з проблемою криптографічної гнучкості: системи потрібно проектувати так, щоб алгоритми можна було замінювати без повного переписування коду –адже один із чотирьох обраних NIST алгоритмів SIDH/SIKE (Supersingular Isogeny Diffie-Hellman/ Supersingular Isogeny Key Encapsulation), вже був зламаний у 2022 році ще до остаточної стандартизації. Це відкриває питання: наскільки надійні нові стандарти і що станеться, якщо один із них виявиться вразливим після масштабного впровадження? Також постає практична проблема збільшення розмірів ключів і підписів, що знижує продуктивність вбудованих систем, IoT-пристроїв і систем з обмеженою пропускною здатністю – типових для тактичного військового рівня.

Окремою проблемою є використання квантових обчислень для криптоаналізу і атак. Фахівці з кібербезпеки і контррозвідки повинні враховувати, що противники, які першими отримають CRQC, зможуть ретроактивно розкрити будь-які перехоплені зашифровані комунікації – включаючи дипломатичні переговори, розвідувальні дані та оперативні накази, що передавались протягом останніх десятиліть.

***Проблеми використання квантового зв'язку (QKD)***

Одна з центральних невирішених проблем – масштабованість QKD-мереж до тактичного і мобільного рівня. Наявні розгортання (JPMorgan Chase, HSBC, китайська QKD-мережа) є стаціонарними і прив'язаними до оптоволоконної інфраструктури. Для польових умов – зв'язок між рухомими штабами, тактичними підрозділами, БПЛА, морськими платформами – це рішення непридатне у поточному вигляді. Квантові ретранслятори, необхідні для подолання обмежень дальності, залишаються предметом фундаментальних досліджень і не мають готових інженерних рішень.

Проблема довірених вузлів у QKD-мережах є нетривіальною з точки зору безпеки: у мережах з ретрансляторами кожен вузол є "довіреним" і може бути скомпрометований фізично або адміністративно. Це означає, що QKD не вирішує проблему безпеки кінцевих вузлів і не усуває необхідності у традиційних засобах фізичного захисту і контролю доступу. Фахівці, що проектують захищені командні мережі, повинні усвідомлювати, що гарантії QKD стосуються виключно каналу – але не системи в цілому.

Ще одна проблема – відсутність єдиних стандартів і сертифікаційних вимог для QKD-обладнання. На відміну від PQC, де NIST провів відкритий міжнародний процес стандартизації, QKD-пристрої різних виробників (ID Quantique, Toshiba, китайські) мають різні характеристики безпеки і несумісні протоколи. Для розгортання у системах національної безпеки це становить серйозну перешкоду.

***Проблеми використання квантових сенсорів***

Попри найбільшу з трьох напрямків готовність до практичного застосування, квантові сенсори стикаються з критичною проблемою розгортання на рухомих платформах. Вони потребують вакуумних камер, точних лазерних систем і захисту від вібрацій – все це суперечить вимогам до габаритно-масових характеристик авіаційних, наземних і водних платформ. Програма DARPA RoQS (Robust Quantum Sensors) спеціально спрямована на подолання цього розриву, але до серійного виробництва ще далеко.

Проблема інтеграції квантових сенсорів у існуючі системи управління і бойових платформ є не менш серйозною, ніж фізична мініатюризація. Квантові навігаційні системи генерують дані у форматі, відмінному від класичних ІНС, і потребують нових алгоритмів злиття даних (sensor fusion). Взаємодія з наявними системами бойового управління (C2), цілевказання і навігації вимагатиме значних доробок програмного забезпечення і переатестації платформ. Фахівці, що відповідають за інтеграцію нових систем, зіткнуться з проблемами сумісності на всіх рівнях: апаратному, програмному і доктринальному.

Проблема картографічного забезпечення є специфічним обмеженням для квантових систем магнітної і гравітаційної навігації (MagNav, GravNav). Їх точність безпосередньо залежить від якості і деталізації відповідних карт аномалій. Актуальні глобальні магнітні і гравітаційні карти з необхідною роздільною здатністю відсутні для більшості театрів бойових дій, особливо в океанічних і полярних районах. Це означає, що ефективне використання квантової навігації вимагає значних попередніх інвестицій у картографування.

***Кадрові та доктринальні проблеми***

Попри технічний характер більшості вищеназваних викликів, ключовою наскрізною проблемою є катастрофічна нестача фахівців, які поєднують глибоке розуміння квантової фізики з практичними знаннями у галузі безпеки, криптографії та військових систем.

Збройні сили і спецслужби більшості країн, включаючи Україну, ще не виробили доктрин, що регламентують застосування квантових технологій, процедури їх сертифікації і обслуговування в бойових умовах, а також правила обробки інформації з урахуванням загроз HNDL. Ця доктринальна прогалина є не менш небезпечною, ніж суто технічні обмеження, адже навіть за наявності готових технологій їх некоректне або несвоєчасне застосування може знецінити очікуваний ефект.

## Висновки

Отже, зважаючи на значну зацікавленість і фінансування квантових технологій з боку як цивільної промисловості, так і урядів, очікується, що ці технології будуть розвиватись і нові квантові застосування стануть доступними протягом найближчих п'яти-десяти років.

Нові досягнення в розробці квантових технологій можуть принести нові можливості для військових. Проте для того щоб військові могли фактично користуватись перевагами нових квантових технологій, важливо, щоб вони активно включились в роботу в цій сфері і скеровували розробку і запровадження військових застосувань квантових технологій. Військові можуть забезпечити значну додану вартість наявним зусиллям промисловості і науки, надавши інфраструктуру для тестування і випробувань (випробувальні центри) і доступ до військових операторів, які будуть кінцевими користувачами. Якомога більш ранні експерименти з цими технологіями не лише допоможуть їхньому подальшому розвитку, але й допоможуть військовим ознайомитись з цими технологіями і їхніми можливостями, що сприятиме майбутньому впровадженню. Більше того, активна участь в квантовій, особливо в кіберсфері. Оцінюючи свої поточні протоколи кібербезпеки, досліджуючи перспективні технології та шукаючи поради експертів, вони можуть краще екосистемі покращує розуміння військовими потенційних ризиків, зв'язаних з квантовими технологіями підготуватися до захисту від майбутніх квантових загроз.

## Список використаних джерел


1. Міхель ван Амеронген Квантові технології в обороні і безпеці. URL: https://www.nato.int/docu/review/uk/articles/2021/06/03/kvantov-tehnolog-v-oboron-bezpets/index.html (дата звернення: 14.01.2026).
2. Данилюк І. А., Лазута Р. Г., Куцаєв В. В., Цимбал І. В. Дослідження перспектив застосування квантових технологій у Збройних Силах України. *Системи і технології зв'язку, інформатизації та кібербезпеки*. 2025. Вип. 7. URL: https://doi.org/10.58254/viti.7.2025.03.28; https://journal.viti.edu.ua/index.php/cicst/article/view/113.
3. Лисецький Ю. М., Боханченко О. С., Сурма А. І. Використання квантових технологій для забезпечення кіберзахисту. *30 років ВА імені Євгенія Березняка: актуальні проблеми розвідки, контррозвідки, правоохоронної діяльності в умовах широкомасштабної збройної агресії рф проти України* : наук. зб. міжвід. наук.-практ. конф. № 54 (м. Київ, 2 квітня 2024 року). Київ, 2024. С. 114–115.
4. The White House. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM-10). May 4, 2022. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ (дата звернення: 20.01.2026).
5. Sahu S. K., Mazumdar K. State-of-the-art analysis of quantum cryptography: applications and future prospects. *Frontiers in Physics.* 2024. Vol. 12. URL: https://doi.org/10.3389/fphy.2024.1456491.
6. Ali S. et al. Next-Generation Quantum Security: The Impact of Quantum Computing on Cybersecurity – Threats, Mitigations, and Solutions. *Computers & Electrical Engineering*. 2025. Vol. 128. Article 110649. URL: https://doi.org/10.1016/j.compeleceng.2025.110649.
7. The Soufan Center. Quantum Computing and the Evolving Cyber Threat Landscape. IntelBrief. November 15, 2024. URL: https://thesoufancenter.org/intelbrief-2024-november-15/ (дата звернення: 22.01.2026).

8. U.S. Government Accountability Office (GAO). Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy. GAO-25-107703. Washington, D.C., November 21, 2024. URL: https://www.gao.gov/products/gao-25-107703 (дата звернення: 18.01.2026).
9. Dervisevic E., Tankovic A., Fazel E., Kompella R., Fazio P., Voznak M., Mehic M. Quantum Key Distribution Networks – Key Management: A Survey. ACM Computing Surveys. 2025. URL: https://doi.org/10.1145/3730575.
10. Quantum Technologies and Cybersecurity: Threats and Defenses. PostQuantum.com. September 24, 2025. URL: https://postquantum.com/quantum-computing/quantum-cybersecurity/ (дата звернення: 22.01.2026).
11. Purohit K., Vyas A. K. Quantum key distribution through quantum machine learning: a research review. *Frontiers in Quantum Science and Technology.* 2025. Vol. 4. Article 1575498. URL: https://doi.org/10.3389/frqst.2025.1575498.
12. SandboxAQ, Defense Innovation Unit advance quantum navigation for GPS-denied operations. GPS World. November 19, 2025. URL: https://www.gpsworld.com/sandboxaq-defense-innovation-unit-advance-quantum-navigation-for-gps-denied-operations/ (дата звернення: 12.01.2026).
13. Burkey M. T. How Quantum Sensing Will Help Solve GPS Denial in Warfare. Fellow Publication. Center for Global Security Research, Lawrence Livermore National Laboratory. June 2025. LLNL-TR-2004820. URL: https://cgsr.llnl.gov/sites/cgsr/files/2025-06/Burkey_QS_final.pdf (дата звернення: 28.01.2026).
14. Sayler K. M. Defense Primer: Quantum Technology. CRS In Focus IF11836. Congressional Research Service. Washington, D.C., November 4, 2024. URL: https://www.congress.gov/crs-product/IF11836 (дата звернення: 15.01.2026).
15. Ekert A. K. Quantum Cryptography Based on Bell's Theorem. *Physical Review Letters*. 1991. Vol. 67. No. 6. P. 661–663. DOI: 10.1103/PhysRevLett.67.661.
16. Shor P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on – IEEE. 1994. P. 124–134.
17. Лисецький Ю. М., Сурма А. І., Данченко О. І. Квантові технології. Нові можливості в кібербезпеці. *Вісник воєнної розвідки.* 2024. № 81. С. 44–47.
18. SandboxAQ, Defense Innovation Unit advance quantum navigation for GPS-denied operations. GPS World. November 19, 2025. URL: https://www.gpsworld.com/sandboxaq-defense-innovation-unit-advance-quantum-navigation-for-gps-denied-operations/ (дата звернення: 12.01.2026).

## References

1. Mikhel van Ameronhen (2021). Kvantovi tekhnolohii v oboroni i bezpetsi [Quantum technologies in defense and security]. Retrieved from: https://www.nato.int/docu/review/uk/articles/2021/06/03/kvantov-tehnolog-voboron-bezpets/index.html (accessed 14.01.2026) [in Ukrainian].
2. Danyliuk, I. A., Lazuta, R. H., Kutsaiev, V. V., & Tsymbal, I. V. (2025). Doslidzhennia perspektyv zastosuvannia kvantovykh tekhnolohii u Zbroinykh Sylakh Ukrainy [Research into the prospects of applying quantum technologies in the Armed Forces of Ukraine]. *Systemy i tekhnolohii zviazku, informatyzatsii ta kiberbezpeky*. 7. Retrieved from: https://doi.org/10.58254/viti.7.2025.03.28; https://journal.viti.edu.ua/index.php/cicst/article/view/113 [in Ukrainian].
3. Lysetskyi, Yu. M., Bokhanchenko, O. S., & Surma, A. I. (2024). Vykorystannia kvantovykh tekhnolohii dlia zabezpechennia kiberzakhystu [The use of quantum technologies to ensure cyber defense]. *30 rokiv VA imeni Yevheniia Berezniaka: aktualni problemy rozvidky, kontrrozvidky, pravookhoronnoi diialnosti v umovakh shyrokomasshtabnoi zbroinoi ahresii rf proty Ukrainy*: nauk. zb. mizhvid. nauk.-prakt. konf. 54 (pp. 114–115). Kyiv [in Ukrainian].
4. The White House. (2022). National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM-10). Retrieved from: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ (accessed 20.01.2026).
5. Sahu, S. K., & Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: applications and future prospects. *Frontiers in Physics,* 12. Retrieved from: https://doi.org/10.3389/fphy.2024.1456491.
6. Ali, S. & et al. (2025). Next-Generation Quantum Security: The Impact of Quantum Computing on Cybersecurity – Threats, Mitigations, and Solutions. *Computers & Electrical Engineering*, 128. Article 110649. Retrieved from: https://doi.org/10.1016/j.compeleceng.2025.110649.
7. The Soufan Center. (2024). Quantum Computing and the Evolving Cyber Threat Landscape. IntelBrief. Retrieved from: https://thesoufancenter.org/intelbrief-2024-november-15/ (accessed 22.01.2026).

8. U.S. Government Accountability Office (GAO). (2024). Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy. GAO-25-107703. Washington, D.C. Retrieved from: https://www.gao.gov/products/gao-25-107703 (accessed 18.01.2026).
9. Dervisevic, E., Tankovic, A., Fazel, E., Kompella, R., Fazio, P., Voznak, M., & Mehic, M. (2025). Quantum Key Distribution Networks – Key Management: A Survey. ACM Computing Surveys. Retrieved from: https://doi.org/10.1145/3730575.
10. Quantum Technologies and Cybersecurity: Threats and Defenses. (2025). PostQuantum.com. Retrieved from: https://postquantum.com/quantum-computing/quantum-cybersecurity/ (accessed 22.01.2026).
11. Purohit, K., & Vyas, A. K. (2025). Quantum key distribution through quantum machine learning: a research review. *Frontiers in Quantum Science and Technology*, 4. Article 1575498. Retrieved from: https://doi.org/10.3389/frqst.2025.1575498.
12. SandboxAQ, Defense Innovation Unit advance quantum navigation for GPS-denied operations. (2025). GPS World. Retrieved from: https://www.gpsworld.com/sandboxaq-defense-innovation-unit-advance-quantum-navigation-for-gps-denied-operations/ (accessed 12.01.2026).
13. Burkey, M. T. (2025). How Quantum Sensing Will Help Solve GPS Denial in Warfare. Fellow Publication. Center for Global Security Research, Lawrence Livermore National Laboratory. LLNL-TR-2004820. Retrieved from: https://cgsr.llnl.gov/sites/cgsr/files/2025-06/Burkey_QS_final.pdf (accessed 28.01.2026).
14. Sayler, K. M. (2024). Defense Primer: Quantum Technology. CRS In Focus IF11836. Congressional Research Service. Washington, D.C. Retrieved from: https://www.congress.gov/crs-product/IF11836 (дата звернення: 15.01.2026).
15. Ekert, A. K. (1991). Quantum Cryptography Based on Bell's Theorem. *Physical Review Letters*, 67, 6, 661–663. Retrieved from: https://doi.org/10.1103/PhysRevLett.67.661.
16. Shor, P. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on – IEEE, 124-134.
17. Lysetskyi, Yu. M., Surma, A. I., & Danchenko, O. I. (2024). Kvantovi tekhnolohii. Novi mozhlyvosti v kiberbezpetsi [Quantum technologies. New opportunities in cybersecurity]. *Visnyk voiennoi rozvidky*, 81, 44-47 [in Ukrainian].
18. SandboxAQ, Defense Innovation Unit advance quantum navigation for GPS-denied operations. (2025). GPS World. Retrieved from: https://www.gpsworld.com/sandboxaq-defense-innovation-unit-advance-quantum-navigation-for-gps-denied-operations/ (accessed 12.01.2026).

*Received 05.02.2026 | Accepted 25.02.2026 | Published 30.03.2026*



УДК: 355.865:355.021.2 DOI: 10.63978/3083-6476.2026.1.4.06

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

**Сокоринський Юрій Володимирович**
*доктор юридичних наук, доцент*
*співробітник Служби безпеки України*
*Служба безпеки України*
*Київ, Україна*
*e-mail: usokorinskiy@ukr.net*
*ORCID: 0000-0002-8907-9880*

**Жора Віктор Володимирович**
*військовослужбовець*
*Національна гвардія України*
*ORCID: 0000-0003-2679-3056*

# АНАЛІЗ ДИСПРОПОРЦІЇ МІЖ ДИНАМІКОЮ ГІБРИДНИХ (ДОПОРОГОВИХ) ЗАГРОЗ ТА ЧИННОЮ МОДЕЛЛЮ УПРАВЛІННЯ СЕКТОРОМ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

***Анотація.*** *У статті аналізується системна диспропорція між прискореною еволюцією гібридних (допорогових) загроз та консервативною вертикально-ієрархічною моделлю управління сектором безпеки і оборони України. На основі даних CSIS (2025), ENISA Threat Landscape 2025, RAND "From Policy to Victory" (2025), звіту NATO StratCom COE "The Collage of the Kremlin's Communication Strategy" (2025) та WEF Global Cybersecurity Outlook 2025 автор доводить, що традиційні відомчі «силоси» стали головною вразливістю держави. Агресор діє нелінійно та мережево, експлуатуючи "шви" між компетенціями РНБО, МО, СБУ, Держспецзв'язку та приватними операторами критичної інфраструктури (понад 80 % об'єктів).*

*Чинна нормативна база (Закон "Про національну безпеку" 2018, Стратегія кібербезпеки 2021, Розпорядження Кабінету Міністрів України № 853-р 2025) не передбачає ефективних механізмів горизонтальної координації та оперативного обміну даними в реальному часі. Це призводить до хронічного інституційного лагу, коли розвідувальна інформація не встигає трансформуватися в превентивні дії.*

*Ключовим рішенням пропонується створення Об'єднаного аналітичного центру гібридних загроз (ОАЦГЗ) – компактного хаба (55–65 фахівців), підпорядкованого безпосередньо РНБО. Центр поєднує три блоки: прогнозний моніторинг на базі AI, юридично-атрибуційну оцінку та державно-приватний інтерфейс з Data Sharing Agreements. Реалізація вимагає точкових змін до Закону "Про національну безпеку" та оновлення Стратегії кібербезпеки з елементами Active Defense.*

*Практичне значення роботи полягає в обґрунтуванні переходу від реактивної до предиктивної моделі управління СБО та наданні конкретних рекомендацій щодо пілотного запуску ОАЦГЗ у 2027 році.*

***Ключові слова:*** *гібридні загрози, допорогова агресія, сектор безпеки і оборони, Об'єднаний аналітичний центр гібридних загроз, горизонтальна координація, приватно-державне партнерство, активна оборона, НАТО, стійкість критичної інфраструктури.*

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

**Yurii Sokorynskyi**
*Doctor of Juridical Sciences, Associate Professor*
*Security Service of Ukraine officer*
*Security Service of Ukraine*
*Kyiv, Ukraine*
*e-mail: usokorinskiy@ukr.net*
*ORCID: 0000-0002-8907-9880*

**Viktor Zhora**
*military personnel*
*National Guard of Ukraine*
*Kyiv, Ukraine*
*ORCID: 0000-0003-2679-3056*

# ANALYSIS OF THE DISPROPORTION BETWEEN THE DYNAMICS OF HYBRID (SUB-THRESHOLD) THREATS AND THE CURRENT MODEL OF MANAGEMENT OF UKRAINE'S SECURITY AND DEFENSE SECTOR

***Abstract.*** *The article examines the systemic disproportion between the accelerated evolution of hybrid (sub-threshold) threats and the conservative vertical-hierarchical model of governance of Ukraine's security and defence sector (SDS). Drawing on CSIS data (2025), ENISA Threat Landscape 2025, RAND "From Policy to Victory" (2025), NATO StratCom COE "The Collage of the Kremlin's Communication Strategy" (2025), and WEF Global Cybersecurity Outlook 2025, the authors demonstrate that traditional inter-agency "silos" have become the primary vulnerability of the state. The aggressor operates non-linearly and networked, exploiting the "seams" between the RNBO, MoD, SBU, State Special Communications Service, and private critical infrastructure operators (over 80 % of objects).*

*The existing normative framework (Law on National Security 2018, Cybersecurity Strategy 2021, CMU Order No. 853-r 2025) lacks effective mechanisms for horizontal coordination and real-time data exchange. This results in a chronic institutional lag, whereby intelligence information fails to translate into preventive action.*

*The central proposal is the establishment of a Joint Analytical Centre for Hybrid Threats (JACHT) – a compact hub (55–65 specialists) directly subordinated to the RNBO. The Centre integrates three functional blocks: AI-driven predictive monitoring, legal-attribution assessment, and a public-private interface based on Data Sharing Agreements. Implementation requires targeted amendments to Article 12 of the Law on National Security and updates to the Cybersecurity Strategy incorporating Active Defence elements.*

*The practical value of the study lies in substantiating the transition from a reactive to a predictive SDS governance model and providing concrete recommendations for the pilot launch of JACHT in 2027.*

***Keywords**: hybrid threats, sub-threshold aggression, security and defence sector, Joint Analytical Centre for Hybrid Threats, horizontal coordination, public-private partnership, active defence, NATO, critical infrastructure resilience.*

**JEL Classification:** H56, H12, L86, O32, P43

## Вступ

Еволюція засобів міждержавного протиборства станом на 2026 рік фактично розмила межу між конвенційною війною та миром. Сучасна конфліктність дедалі частіше відбувається в "сірій зоні", де гібридні впливи спрямовані на системну ерозію національної стійкості без формального оголошення війни. Для України, яка стала глобальною лабораторією першої повномасштабної інтегрованої війни, розв'язання цієї проблеми перетворилося на умову виживання.

Особливого експертного занепокоєння додають тенденції, задокументовані у звіті CSIS від 18 березня 2025 року: кількість російських актів саботажу в Європі майже потроїлася між 2023 та 2024 роками (з 12 до 34 атак), демонструючи чотирикратне зростання порівняно з 2022 роком. Основна відповідальність за ці операції лежить на ГРУ (гу гш зс рф), яке через агентурні мережі, безпілотні літальні апарати та "тіньовий флот" для підводних диверсій демонструє спроможність діяти поза класичним полем бою.

На цьому тлі чинна нормативно-правова база України, включно з фундаментом у вигляді Стратегії національної безпеки 2020 року, виявляє ознаки темпорального відставання, оскільки створювалася за умов зовсім іншої швидкості виникнення загроз.

Виникає критичний розрив: агресор діє нелінійно та мережево, тоді як вітчизняна модель управління сектором безпеки і оборони (далі – СБО) залишається заручником вертикальної бюрократії. Навіть враховуючи оновлення стратегії НАТО щодо гібридних загроз у січні 2026 року та запровадження посади Спеціального координатора, Україна ризикує залишити "вікна вразливості" відкритими через відсутність аналогічного горизонтального інтегратора. Як підкреслюється у дослідженні RAND "From policy to victory" (2025), український досвід інтеграції технологій може забезпечити перевагу лише за умови існування єдиної аналітичної платформи, інакше виявлена диспропорція управління лише посилюватиметься.

## Огляд літератури

Наукове розуміння гібридних загроз пройшло довгий шлях. Спочатку вчені описували їх лише як набір тактичних прийомів кібератаки, пропаганду чи саботаж. Сьогодні ми говоримо про щось набагато глибше: "тотальну дифузію", коли агресор розмиває межі між війною і миром, поступово паралізуючи державні інститути.

Данилюк О. точно підмітив цю зміну: сучасні гібридні загрози – це вже не просто зовнішній тиск, а свідома експлуатація слабких місць демократії. Мета не знищити систему одним ударом, а виснажити її зсередини [15].

Український досвід став справжнім "лабораторією" таких конфліктів. Як зазначають у звітах RAND Corporation та в роботі Крапа А., саме Україна показала межі старих оборонних моделей. Традиційні ієрархічні структури, заточені під фізичне стримування, просто не встигають за атаками на когнітивну сферу та цифрову інфраструктуру [16].

Останні дослідження 2025 року тільки підтверджують цю тезу. У звіті НАТО Strategic Communications Centre of Excellence "The Collage of the Kremlin's Communication Strategy" автори детально розбирають, як Кремль поєднує цензуру, синтетичні медіа та пропаганду в єдину комунікаційну машину гібридної війни. Це вже не окремі операції – це цілісна стратегія впливу на свідомість [17].

World Economic Forum у "Global Cybersecurity Outlook 2025" іде ще далі. Звіт показує, як кіберзагрози в "Intelligent Age" переплітаються з дезінформацією. Атаки стають

конвергентними: один удар по інфраструктурі супроводжується інформаційною кампанією, яка підриває довіру суспільства. Традиційні підходи до захисту тут просто не працюють. [18].

Не менш важливий "Parliamentary Handbook on Disinformation, AI and Synthetic Media" від Commonwealth Parliamentary Association та Organization of American States. Автори прямо вказують: штучний інтелект робить фейки майже невловимими. Без швидкої атрибуції та нових законодавчих механізмів держави залишаються вразливими [19].

G7 у своєму аналітичному меморандумі (Policy Brief) "Strategy for Countering Russian Information Operations" (2025) фіксує ще одну тривожну тенденцію: кількість російських операцій FIMI в Європі майже потроїлася за рік [20]. При цьому Москва активно розширює діяльність на Індо-Тихоокеанський регіон, використовуючи локальні проксі-мережі. Це вже не європейська проблема – це глобальна мережа.

Євроатлантичне партнерство також реагує. Десятий прогрес-репорт НАТО-ЄС (2025) показує реальний прогрес: нові структуровані діалоги щодо сталості, кіберзахисту та оборонної промисловості. Але дослідники прямо пишуть: координація ще недостатня, щоб випереджати агресора [21].

Українські дослідники Сальнікова О., Сівоха І., Іващенко А. [22], а також Юськів Б., Карпчук Н. та Пелех О. (2024) [23] підкреслюють, що стратегічні комунікації в гібридній війні – це інструмент рефлексивного управління та випередження. Усі джерела сходяться в одному: ієрархічна модель програє мережевим атакам. Майбутнє – за горизонтальною взаємодією, інтеграцією приватного сектору та швидким обміном даними.

## Мета та завдання статті

Мета статті – виявити причини структурної невідповідності чинної моделі управління СБО динаміці сучасних гібридних загроз. Завдання полягає в локалізації точок розриву між відомствами та обґрунтуванні створення Об'єднаного аналітичного центру гібридних загроз (ОАЦГЗ) як інструменту переходу від реактивної до предиктивної моделі.

## Методи

Методологія ґрунтується на системному аналізі нормативних актів і компаративістиці організаційних структур СБО України та країн НАТО. Структури розглядаються не як статичні об'єкти, а як динамічні цикли прийняття рішень. Основу становить OSINT-аналіз верифікованих звітів CSIS та ENISA 2024–2025 років. Модель превентивно-реактивних дій (Preventive-Response Options) НАТО (2026) слугує базисом, який, однак, потребує адаптації до українських реалій, де співпраця з приватним сектором досі має декларативний характер.

Окремо враховано аналітику RAND Corporation (2025) щодо еволюції гібридних інструментів у бік підвищення їхньої летальності, що змушує відмовитися від суто описових підходів на користь предиктивного моделювання.

## Результати

Традиційні ієрархічні системи безпеки втрачають ефективність, коли агресор діє нелінійно, одночасно в кількох доменах і з високою швидкістю. Гібридні (допорогові) загрози являють собою синхронізоване поєднання невійськових інструментів від кібероперацій до саботажу з метою системного виснаження суверенітету без переходу до відкритої фази конфлікту. Об'єктом впливу стає не територія, а функціональна спроможність інститутів і стійкість критичної інфраструктури.

Ключові характеристики таких загроз: допороговість, конвергентність і атрибутивна неоднозначність. У 2026 році вони перетворилися на алгоритмізовану агресію. Дані CSIS

(2025) свідчать, що понад 21 % російських підривних операцій у Європі спрямовані на енергетику та логістичні ланцюги.

НАТО реагує на ці виклики через комплексний підхід (Comprehensive Approach), подвоюючи кількість багатонаціональних бойових груп та закладаючи рекордні витрати на оборону до 5 % ВВП до 2035 року. Однак для України ситуація ускладнюється внутрішньою фрагментацією. Розпорядження Кабінету Міністрів України № 853-р від 13 серпня 2025 року визнає наявність нормативних документів, які не мають єдиної візії та належної координації. Така ситуація при реальній відсутності надвідомчого аналітичного хаба створює умови, за яких держава залишається в стані постійної реактивності. Відтак, перебудова моделі управління СБО на основі мережевої синергії розвідки, держорганів та приватного сектору розглядається як спосіб збереження керованості в умовах "тотальної гібридності".

***Технічний аналіз та відомчі обмеження***

Яскравим прикладом стала синхронізована атака на енергосистему Польщі (грудень 2025), де агресор поєднав вразливості FortiGate з вайпером DynoWiper [6], вивівши з ладу понад 30 об'єктів генерації. В українському контексті протидія таким атакам натикається на жорстку відомчу сегментацію. Закон "Про національну безпеку" (2018) чітко розмежовує повноваження, але не передбачає механізмів швидкої взаємодії в "сірій зоні".

Відповідно до Закону "Про національну безпеку України" [7], сектор безпеки має чітку, але надто ізольовану структуру. Повноваження Міністерства оборони, згідно зі Стратегією воєнної безпеки [8], сфокусовані на відсічі збройній агресії, що фактично паралізує залучення військового ресурсу (включно з де-юре відсутніми кіберсилами) до інцидентів у "сірій зоні", які формально не класифікуються як акт війни.

Своєю чергою, Служба безпеки України, виконуючи функції контррозвідки, часто вступає у функціональний конфлікт із Кіберполіцією та Держспецзв'язку. Останній, спираючись на Стратегію кібербезпеки [9], забезпечує захист державних інформаційних ресурсів, проте критична інфраструктура, що перебуває у приватній власності, залишається в зоні «невизначеної відповідальності». Це створює ідеальні умови для агресора: атака на приватного обленерго-провайдера юридично не є атакою на державу, хоча її соціальні наслідки ідентичні.

Рада національної безпеки і оборони України, попри свій статус координаційного органу [2], залишається структурою стратегічного планування. Процес скликання засідань та підготовки Указів Президента України створює часовий лаг, який у 2026 році вимірюється годинами, тоді як автоматизовані атаки розвиваються за мілісекунди. Як зазначають експерти RAND у звіті 2025 року, основні суб'єкти кібербезпеки можуть володіти індикаторами компрометації (IoC) ще до початку атаки, проте складні протоколи передачі таємної інформації цивільним відомствам, таким як Міненерго, блокують можливість превентивного реагування [4].

***Генезис безпекових викликів та еволюція гібридного інструментарію***

Трансформація безпекового середовища навколо України, що набула критичної фази у 2025–2026 роках, не є випадковим сплеском активності, а результатом послідовного генезису доктрини "постійного конфлікту". Витоки нинішнього розриву в управлінні слід шукати в переході від спорадичних дезінформаційних кампаній до системної, алгоритмізованої агресії. Як зазначають дослідники RAND Corporation (2025), сучасна модель гібридної війни рф остаточно оформилася як стратегія "керованого хаосу", де основний акцент зміщено з прямого воєнного зіткнення на дестабілізацію через некінетичні методи [5].

Статистичні дані CSIS підтверджують цей еволюційний злам. Якщо у 2022 році було зафіксовано лише 3 масштабні акти саботажу в Європі, то у 2023-му їхня кількість зросла до 12, а у 2024-му – до 34 [1]. Такий темп (майже трикратне зростання щороку) вказує на

те, що агресор перейшов до етапу “виснаження інфраструктурної стійкості”. Генезис цих викликів демонструє перехід від вузькопрофільних кібератак до конвергентних операцій, де злам цифрового контуру є лише підготовчим етапом для фізичного руйнування об’єктів енергетики чи логістики.

Згідно зі звітом ENISA Threat Landscape 2025, загальна кількість верифікованих інцидентів у Європейському регіоні сягнула 4875, причому 77 % з них становили DDoS-атаки нового покоління, що використовуються як “шумова завіса” для глибшого проникнення в мережі [6].

Для України цей генезис має ще складніший характер. Ми спостерігаємо зрощення кримінальних мереж, проксі-груп та спецслужб рф. НАТО у своїх оновлених оцінках 2026 року визнає, що швидкість, з якою гібридні загрози адаптуються до контрзаходів, перевищує можливості будь-якої закритої ієрархічної системи [3]. Таким чином, генезис викликів випереджає генезис інституцій, створюючи той самий розрив, який ми пропонуємо подолати через мережеву трансформацію СБО.

***Інституційний аналіз сектору безпеки і оборони в контексті гібридного протиборства***

Проведений інституційний аналіз чинної архітектури СБО України вказує на її детермінованість принципами жорсткої вертикалі, що закладалися ще у 2018 році при ухваленні профільного Закону “Про національну безпеку” [7]. Ця модель виходить із презумпції чіткого розподілу ролей: Міноборони – відсіч агресії, СБУ – контррозвідка, МВС – громадський порядок. Проте в умовах 2026 року, коли межі між цими доменами стерті зусиллями агресора, така спеціалізація перетворюється на певну інституційну пастку.

Ключовим вузлом координації залишається Рада національної безпеки і оборони (РНБО). Згідно зі Стратегією національної безпеки 2020 року, саме цей орган має забезпечувати системну єдність [2]. Проте на практиці РНБО функціонує як орган стратегічного координатора, а не оперативного управління. Між ухваленням рішення на рівні РНБО та його імплементацією конкретним відомством утворюється “інституційний лаг”, який є критично неприпустимим при нейтралізації швидких гібридних інцидентів.

Особливого аналізу потребує роль Держспецзв’язку у світлі Стратегії кібербезпеки 2021 року [9]. Попри розширення повноважень, цей інститут залишається обмеженим державним сектором. Як підкреслюють експерти RAND Corporation (2025), сучасна стійкість (resilience) неможлива без інтеграції комерційних технологій та приватних операторів критичної інфраструктури [4]. В українській інституційній моделі приватний сектор досі розглядається не як повноправний суб’єкт СБО, а як об’єкт регулювання або захисту.

Розвідувальна спільнота (ГУР МО, СЗРУ), чия діяльність регулюється Законом “Про розвідку”, володіє найвищим рівнем обізнаності щодо намірів ворога, проте інституційні бар’єри (режим секретності, відсутність спільних дата-платформ) перешкоджають миттєвій передачі цих даних цивільним міністерствам. Як результат, виникає парадоксальна ситуація: держава має інформацію про загрозу, але не має гнучкого механізму її реалізації без задіяння громіздкої бюрократичної машини.

Порівняння з оновленими протоколами НАТО 2026 року свідчить, що успішні системи сьогодні будуються на принципі “горизонтальної довіри”, де обмін даними відбувається в реальному часі без постійної апеляції до вищого керівництва [3]. В Україні ж інституційна культура залишається орієнтованою на “звіт вгору”, що автоматично робить систему реактивною. Отже, інституційна “криза” СБО полягає не у відсутності органів, а в їхній певній закритості, ізольованості та нездатності до мережевої синергії, що прямо підтверджується накопиченням стратегічних документів [10].

***Компаративний аналіз моделей стійкості: досвід країн НАТО та українські реалії***

Усвідомлення глибини управлінського розриву в Україні потребує детального зіставлення з моделями "тотальної оборони» та «всеосяжної безпеки", які де-факто стали стандартом для країн НАТО, що межують із агресором. На відміну від української моделі, де координація часто зводиться до бюрократичного листування, досвід Фінляндії та Естонії демонструє життєздатність горизонтальних екосистем.

*Модель Фінляндії: Комітет безпеки та концепція "Society-Wide Resilience"*

Фінська модель базується на функціонуванні Комітету безпеки (Turvallisuuskomitea), який, попри зовнішню схожість із апаратом РНБО, має принципово іншу операційну природу. Згідно з фінською Стратегією безпеки суспільства (Yhteiskunnan turvallisuusstrategia), безпека не є прерогативою силових відомств, а розподіленою відповідальністю між державними органами, бізнесом та неурядовими організаціями [3; 8].

Ключова відмінність від українських реалій полягає у функціонуванні Національного оперативного центру (НОЦ), який у режимі 24/7 інтегрує дані від цивільних операторів інфраструктури та розвідки. В Україні ж, як зазначалося раніше, дані розвідки (ГУР МО, СЗРУ) часто "застрягають" на рівні вищого політичного керівництва, не потрапляючи до кінцевих розпорядників критичних об'єктів [4]. Фінський досвід доводить: ефективність предиктивного аналізу залежить від довіри, де приватний сектор є не об'єктом контролю, а повноправним учасником обміну розвідданими про загрози.

*Естонський досвід: Центри передового досвіду та цифрова інтегрованість*

Естонія, яка пережила першу масштабну гібридну атаку ще у 2007 році, вибудувала одну з найбільш адаптивних систем кіберзахисту у світі. Особливого значення набуває діяльність Об'єднаного центру передового досвіду з кібероборони НАТО (CCDCOE) у Таллінні. Проте для нашого аналізу важливішим є внутрішній естонський протокол взаємодії в межах Кабінету безпеки.

Згідно зі звітом ENISA 2025, Естонія реалізувала принцип "цифрової безшовності" в управлінні інцидентами [6]. Коли виникає гібридна загроза (наприклад, GPS-спуфінг у Балтійському морі, зафіксований у 2024–2025 рр.), реакція відбувається не через скликання комісій, а через автоматизовану платформу обміну інформацією між Департаментом інформаційних систем (RIA) та силами Кайтселійту (Союзу оборони). В Україні ж аналогічні процеси вимагають узгоджень між Держспецзв'язку, СБУ та профільними міністерствами, що створює той самий "часовий лаг", який агресор успішно експлуатує [10].

*Адаптація протоколів НАТО 2026: від реакції до превенції*

Оновлені протоколи НАТО, ухвалені на початку 2026 року, запроваджують концепцію Preventive-Response Options (PROs), яка передбачає активацію контрзаходів ще до того, як гібридна атака спричинить фізичні руйнування [3]. Це вимагає такого рівня атрибуції загроз, який наразі в Україні технічно розпорошений.

Порівняльний аналіз висвітлює ключову системну помилку української моделі: ми намагаємося регулювати безпеку через збільшення кількості стратегічних документів (понад 330 одиниць [10]), тоді як країни НАТО йдуть шляхом спрощення процедур та створення спільних ситуаційних центрів. Як підкреслюють аналітики RAND у 2025 році, українська система досі функціонує за принципом "потрібно знати" (need to know), що обмежує доступ до інформації, тоді як сучасні виклики вимагають принципу "потрібно поділитися" (need to share) [4].

Звичайно інтеграція західного досвіду в українські реалії не може бути механічним копіюванням. Вона вимагає подолання "культурного розриву" всередині СБО і переходу від закритої відомчої ієрархії до відкритої, але захищеної мережі взаємодії. Це порівняння слугує остаточним аргументом на користь створення Об'єднаного аналітичного центру

гібридних загроз (ОАЦГЗ), який має стати українською відповіддю на мережеві виклики, трансформуючи наш унікальний бойовий досвід у сучасну інституційну форму.

***Синергія між суб'єктами СБО та приватним сектором як чинник стійкості***

Досвід останніх років показує, що забезпечення національної стійкості в умовах тотальної гібридизації конфліктів 2025–2026 років неможливе без радикального переосмислення ролі приватного сектору. Традиційна модель, де держава є монопольним гарантом безпеки, остаточно вичерпала себе, оскільки понад 80 % об'єктів критичної інфраструктури (енергетика, телекомунікації, хмарні сервіси) перебувають поза межами прямого державного управління. Як зазначають аналітики RAND у роботі "From policy to victory" (2025), ключем до переваги є не нарощування власних потужностей держави, а її здатність до швидкої інтеграції з комерційними технологічними гігантами [4].

В українському контексті створення реальної синергії блокується застарілою регуляторною логікою. Відповідно до статті 12 Закону "Про національну безпеку" сектор безпеки і оборони України складається з чотирьох взаємопов'язаних складових: сили безпеки; сили оборони; оборонно-промисловий комплекс; громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки [7]. Чинна Стратегія кібербезпеки 2021 року [9] розглядають приватний сектор переважно як об'єкт для перевірок або надання обов'язкових до виконання вказівок. Проте дані ENISA Threat Landscape 2025 свідчать, що швидкість ідентифікації нових загроз у приватному секторі на 40–60 % вища, ніж у державних структурах, завдяки використанню глобальних масивів даних [6].

Справжня синергія вимагає переходу до моделі Data Sharing Agreements (угод про спільне використання даних), що вже є нормою в оновлених протоколах НАТО 2026 року [3]. Це передбачає створення безпечного інформаційного периметра, де розвідувальні індикатори компрометації (IoC) від ГУР МО чи СБУ автоматично синхронізуються з системами захисту приватних провайдерів без бюрократичних погоджень. Більше того, досвід відсічі кібер-фізичним атакам 2025 року підкреслює необхідність залучення приватних груп швидкого реагування до державних планів кризисного менеджменту.

Однак, як демонструє аналіз Пайє П., створення такої екосистеми в Україні впирається у проблему довіри та відсутність юридичних гарантій захисту комерційної таємниці при взаємодії з силовиками [4]. Без внесення змін до законодавства, які б легалізували статус приватних технологічних компаній як суб'єктів забезпечення безпеки з відповідним рівнем доступу до даних, синергія залишатиметься на рівні декларативного волонтерства. У 2026 році такий розрив є не просто організаційним дефектом, а прямою загрозою національній стійкості, оскільки ворог атакує найбільш вразливу, тобто найменш інтегровану ланку системи. Для подолання цієї диспропорції необхідно впроваджувати механізми горизонтальної координації, де держава виступає не як контролер, а як модератор спільних зусиль [10].

Подолання цього розриву неможлива без експертної ревізії нормативно-правового поля, яке станом на 2026 рік залишається занадто консервативним. Автори пропонують розглянути можливість внесення змін до ключових законів для офіційного закріплення мережевої моделі управління в законодавстві.

1. Зміни до Закону "Про розвідку" [10]:

Критичним є перегляд механізмів передачі розвідувальної інформації. Наразі цей Закон (ст. 1) обмежує коло споживачів розвідінформації передусім вищими посадовими особами держави. Для ефективності ОАЦГЗ необхідно легалізувати передачу деперсоніфікованих технічних даних (threat intelligence) безпосередньо технічним підрозділам суб'єктів критичної інфраструктури. Це дозволить реалізувати концепцію "розвідки для захисту", а не лише для інформування "визначених Президентом України інших складових сектору безпеки і оборони України".

2. Реформа Стратегії кібербезпеки України [9]:

Потрібен перехід від “захисту периметра” до моделі Активної оборони (Active Defense). Це передбачає внесення правок, що дозволяють визначеним суб’єктам СБО проводити превентивні операції з нейтралізації інфраструктури агресора (С2-серверів) за межами національного сегменту мережі. Як зазначається у рекомендаціях RAND Corporation (2025), пасивний захист у 2026 році є апріорі програшним [4].

3. Впровадження інституту “Цифрового офіцера зв’язку” на стратегічних приватних компаніях:

Законодавче закріплення присутності представників Служби безпеки України та Держспецзв’язку у визначених стратегічних приватних компаніях. Це не контроль, а створення прямого каналу зв’язку, що відповідає практиці Фінляндії та Естонії. Звичайно впровадження інституту “Цифрового офіцера зв’язку” вимагає чіткого визначення критеріїв, за якими такі компанії обираються. Необхідно встановити, зокрема, критерії стратегічної значущості для національної безпеки, належність до критичних секторів інфраструктури (енергетика, транспорт, телекомунікації тощо), масштаб їхнього впливу на оборонно-промисловий комплекс тощо. Також доцільно встановити механізм періодичного перегляду переліку таких компаній з урахуванням змін у ризиковому ландшафті та стратегічних пріоритетах держави.

Ця правова трансформація має супроводжуватися скасуванням або суттєвим спрощенням застарілих відомчих інструкцій, які не повною мірою відповідають характеру сучасних гібридних (допорогових) загроз.

***Пропонована архітектура моделі управління: перехід до мережецентричності***

Для подолання виявленої структурної диспропорції між динамікою гібридних загроз і чинною вертикальною моделлю управління сектором безпеки і оборони України пропонується здійснити фундаментальну трансформацію. Центральним елементом трансформації може стати Об’єднаний аналітичний центр гібридних загроз (ОАЦГЗ) – компактний високошвидкісний хаб, підпорядкований безпосередньо РНБО. Штатна чисельність на етапі пілоту – 55-65 фахівців.

Структура центру включає три блоки:

– Групу прогнозного моніторингу (AI-аналіз відкритих джерел, розвідданих і логів приватних операторів);

– Групу юридично-атрибуційної оцінки (підготовка доказової бази);

– Інтерфейс державно-приватної взаємодії (автоматизований обмін IoC через Data Sharing Agreements).

Пілотний запуск рекомендується здійснити на початку 2027 року на обмеженій групі об’єктів (енергетика, зв’язок, транспорт).

Результати пілоту протягом року дозволять прийняти обґрунтоване рішення щодо масштабування моделі.

Повномасштабна реалізація цієї архітектури вимагатиме внесення відповідних змін до Закону “Про національну безпеку України” [7], Закону “Про Державну службу спеціального зв’язку та захисту інформації”. Крім того, Стратегія кібербезпеки має бути доповнена протоколами Active Defense (активної оборони), які б дозволяли визначеним суб’єктам СБО нейтралізувати загрози в зародку, а не лише фіксувати збитки [9].

## Висновки

Проведений аналіз підтверджує існування фундаментального розриву між швидкістю еволюції гібридних (допорогових) загроз і консервативною вертикальною моделлю управління сектором безпеки і оборони України. Ця диспропорція закладена в чинному законодавстві та проявляється в хронічній затримці між отриманням розвідданих і оперативними діями.

На думку авторів статті, косметична модернізація існуючих органів уже недостатня. Структурним рішенням є створення Об'єднаного аналітичного центру гібридних загроз як оперативного інтегратора. Його пілотний запуск у 2027 році на обмеженій групі об'єктів дозволить перевірити ефективність моделі в реальних умовах.

Автори не претендують на істину в останній інстанції. Запропоновані положення мають характер попередньої наукової гіпотези. Деякі висновки можуть сприйматися як загальні, що пояснюється обмеженим доступом до закритої інформації. Окремі твердження потребують подальшої верифікації та критичного обговорення.

Водночас автори вважають, що порушені проблеми управління сектором безпеки і оборони в умовах гібридних (допрогових) загроз є надто важливими, щоб залишатися лише предметом внутрішньовідомчих дискусій. Стаття спрямована на ініціювання відкритого наукового діалогу та внесок у спільний пошук ефективних інституційних рішень. Автори з повагою ставляться до будь-яких конструктивних зауважень і критики з боку наукової спільноти та читачів і розглядають їх як необхідний етап удосконалення запропонованих ідей.

## Список використаних джерел


1. Center for Strategic and International Studies (CSIS). Russian Sabotage Operations in Europe: Data Analysis and Strategic Implications. CSIS Special Report. March 18, 2025.
2. ENISA Threat Landscape 2025: From Cyber Espionage to Physical Sabotage. *European Union Agency for Cybersecurity (ENISA).* URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.
3. Countering Hybrid Threats: Updated Protocols on Horizontal Coordination and Resilience. *North Atlantic Treaty Organization (NATO).* 2026. URL: https://www.nato.int/cps/en/natohq/topics_156338.htm.
4. Paillé P. others. From Policy to Victory: Recommendations to Ukraine for Harnessing Defence Technology. *RAND Europe.* 2025.
5. Microsoft Digital Defense Report 2024: The Evolution of Hybrid Conflicts. *Microsoft.* Microsoft Security Response Center. 2024.
6. Google Cloud / Mandiant. APT44: 2024 Retrospective. A Close Look at Sandworm's Evolving Cyber-Physical Tactics. 2024.
7. Wang H., Zakheim B. China's Lessons from the Russia-Ukraine War: Perceived New Strategic Opportunities and an Emerging Model of Hybrid Warfare. RAND Corporation, 2025.
8. The Finnish Security and Defence Committee. The Strategy for Society's Resilience: Comprehensive Security Model. Helsinki, Ministry of Defence, 2024.
9. Про національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19.
10. Про розвідку : Закон України від 17 вересня 2020 року № 912-IX. URL: https://zakon.rada.gov.ua/laws/show/912-20.
11. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року : Указ Президента України № 392/2020 "Про Стратегію національної безпеки України".
12. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року : Указ Президента України № 121/2021 "Про Стратегію воєнної безпеки України".
13. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року : Указ Президента України № 447/2021 "Про Стратегію кібербезпеки України".
14. Про затвердження плану заходів щодо синхронізації стратегічного планування у сфері національної безпеки : Розпорядження Кабінету Міністрів України від 15 серпня 2025 року № 853-р.
15. Danylyuk O. Total Diffusion: The New Reality of Hybrid Aggression against Democratic Institutions. London: Royal United Services Institute (RUSI), 2024.
16. Lysenko S., Marukhovskyi O., Krap A., Illiuschenko S., Pochapska O. The Analysis of World Information Warfare and Information Security in the Context of the Russian-Ukrainian War. *Studies in Media and Communication.* 2023. № 11 (7). P. 150–158. URL: https://redfame.com/journal/index.php/smc/article/view/6414; https://doi.org/10.11114/smc.v11i7.6414.
17. NATO Strategic Communications Centre of Excellence. The Collage of the Kremlin's Communication Strategy. Riga: NATO StratCom COE, 2025.
18. World Economic Forum. Global Cybersecurity Outlook 2025 (In collaboration with Accenture). Geneva: WEF, 2025.

19. Commonwealth Parliamentary Association & Organization of American States. Parliamentary Handbook on Disinformation, AI and Synthetic Media. London/Washington, D.C., 2023.
20. Swanström N., Logan T. J. G7 Strategy for Countering Russian Information Operations in the Indo-Pacific Region: A Framework for Enhanced Multilateral Coordination and Response. *Institute for Security & Development Policy*. 2025. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.isdp.eu/wp-content/uploads/2025/06/Policy-Brief-FIMI.pdf.
21. European Union & North Atlantic Treaty Organization. Tenth progress report on the implementation of the common set of proposals (June 2024 – May 2025). Brussels. 2025.
22. Юськів Б., Карпчук Н., Пелех О. Зміни стратегічних комунікацій України в час російсько-української війни (2022–2024 рр.). *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2024. № 3 (20). С. 99-112. URL: https://doi.org/10.29038/2524-2679-2024-03-99-112.
23. Сальнікова О., Сівоха І., Іващенко А. Стратегічні комунікації в сучасних війнах гібридного типу. *Social Development & Security*. 2019. № 9 (5). С. 133–142. URL: http://doi.org/10.33445/sds.2019.9.5.9.

## References

1. Center for Strategic and International Studies (CSIS). (2025). Russian Sabotage Operations in Europe: Data Analysis and Strategic Implications. CSIS Special Report. March 18, 2025.
2. European Union Agency for Cybersecurity (ENISA). (2025). ENISA Threat Landscape 2025: From Cyber Espionage to Physical Sabotage. Retrieved from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.
3. North Atlantic Treaty Organization (NATO). (2026). Countering Hybrid Threats: Updated Protocols on Horizontal Coordination and Resilience. Retrieved from: https://www.nato.int/cps/en/natohq/topics_156338.htm.
4. Paillé, P., & others. (2025). From Policy to Victory: Recommendations to Ukraine for Harnessing Defence Technology. RAND Europe.
5. Microsoft. (2024). Microsoft Digital Defense Report 2024: The Evolution of Hybrid Conflicts. Microsoft Security Response Center.
6. Google Cloud / Mandiant. (2024). APT44: 2024 Retrospective. A Close Look at Sandworm's Evolving Cyber-Physical Tactics.
7. Wang, H., & Zakheim, B. (2025). China's Lessons from the Russia-Ukraine War: Perceived New Strategic Opportunities and an Emerging Model of Hybrid Warfare. RAND Corporation.
8. The Finnish Security and Defence Committee. (2024). The Strategy for Society's Resilience: Comprehensive Security Model. Helsinki, Ministry of Defence.
9. Zakon Ukrainy. (2018). Pro natsionalnu bezpeku Ukrainy [On national security of Ukraine] (No. 2469-VIII). Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19 [in Ukrainian].
10. Zakon Ukrainy. (2020). Pro rozvidku [On intelligence] (No. 912-IX). Retrieved from: https://zakon.rada.gov.ua/laws/show/912-20 [in Ukrainian].
11. President of Ukraine. (2020). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku "Pro Stratehiiu natsionalnoi bezpeky Ukrainy" [On the decision of the National Security and Defense Council of Ukraine of September 14, 2020 "On the National Security Strategy of Ukraine"] (Decree No. 392/2020) [in Ukrainian].
12. President of Ukraine. (2021). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 25 bereznia 2021 roku "Pro Stratehiiu voiennoi bezpeky Ukrainy" [On the decision of the National Security and Defense Council of Ukraine of March 25, 2021 "On the Military Security Strategy of Ukraine"] (Decree No. 121/2021) [in Ukrainian].
13. President of Ukraine. (2021). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy" [On the decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine"] (Decree No. 447/2021) [in Ukrainian].
14. Kabinet Ministriv Ukrainy. (2025). Pro zatverdzhennia planu zakhodiv shchodo synkhronizatsii stratehichnoho planuvannia u sferi natsionalnoi bezpeky [On approval of the action plan for the synchronization of strategic planning in the field of national security] (Order No. 853-r) [in Ukrainian].
15. Danylyuk, O. (2024). Total Diffusion: The New Reality of Hybrid Aggression against Democratic Institutions. London: Royal United Services Institute (RUSI).
16. Lysenko, S., Marukhovskyi, O., Krap, A., Illiuschenko, S., & Pochapska, O. (2023). The Analysis of World Information Warfare and Information Security in the Context of the Russian-Ukrainian War. *Studies in Media and Communication,* 11 (7), 150–158. Retrieved from: https://redfame.com/journal/index.php/smc/article/view/6414; https://doi.org/10.11114/smc.v11i7.6414.

17. NATO Strategic Communications Centre of Excellence. (2025). The Collage of the Kremlin's Communication Strategy. Riga: NATO StratCom COE.
18. World Economic Forum. (2025). Global Cybersecurity Outlook 2025 (In collaboration with Accenture). Geneva: WEF.
19. Commonwealth Parliamentary Association & Organization of American States. (2023). Parliamentary Handbook on Disinformation, AI and Synthetic Media. London/Washington, D.C.
20. Swanström, N., & Logan, T. J. (2025). G7 Strategy for Countering Russian Information Operations in the Indo-Pacific Region: A Framework for Enhanced Multilateral Coordination and Response. *Institute for Security & Development Policy*. Retrieved from: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.isdp.eu/wp-content/uploads/2025/06/Policy-Brief-FIMI.pdf.
21. European Union & North Atlantic Treaty Organization. (2025). Tenth progress report on the implementation of the common set of proposals (June 2024 – May 2025). Brussels.
22. Yuskiv, B., Karpchuk, N., & Pelekh, O. (2024). Zminy stratehichnykh komunikatsii Ukrainy v chas rosiisko-ukrainskoi viiny (2022–2024 rr.) [Changes in Ukraine's strategic communications during the Russian-Ukrainian war (2022–2024)]. *Mizhnarodni vidnosyny, suspilni komunikatsii ta rehionalni studii*, 3 (20), 99-112. Retrieved from: https://doi.org/10.29038/2524-2679-2024-03-99-112 [in Ukrainian].
23. Salnikova, O., Sivokha, I., & Ivashchenko, A. (2019). Stratehichni komunikatsii v suchasnykh viinakh hibrydnoho typu [Strategic Communications in Modern Hybrid Wars]. *Social Development & Security*, 9 (5), 133–142. Retrieved from: http://doi.org/10.33445/sds.2019.9.5.9 [in Ukrainian].

*Received 06.03.2026 | Accepted 19.03.2026 | Published 30.03.2026*



338.2:338.45:330.3(477) DOI: 10.63978/3083-6476.2026.1.4.07

**Скуріневська Леся Валентинівна**
*доктор економічних наук,*
*старший науковий дослідник*
*заступник начальника*
*навчально-наукового центру*
*оборонного менеджменту*
*Національний університет*
*оборони України*
*Київ, Україна*
*e-mail: olesya201405@gmail.com*
*ORCID: 0000-0003-4536-9170*

# СТРУКТУРНІ ДЕФЕКТИ ІНСТИТУЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СТРАТЕГІЧНОГО ФОРСАЙТУ ТА ЕКОНОМІЧНА НЕСТІЙКІСТЬ ЕНЕРГЕТИЧНОЇ СИСТЕМИ УКРАЇНИ В УМОВАХ ПОВНОМАСШТАБНОЇ ВІЙНИ

***Анотація.*** *В статті проведено дослідження того, як інституційна неспроможність стратегічного форсайту трансформуватися в обов'язкові економічні рішення посилює структурну вразливість енергетичного сектору України під час війни. Більшість загроз, які сьогодні реалізуються у формі масованих атак на генерацію та передачу, були чітко прогнозованими ще з 2022 року. Однак вони так і не стали підставою для перебудови архітектури системи в напрямі економічної стійкості.*

*Метою роботи є виявлення глибинного розриву між рівнем прогнозованості ризиків і реальною якістю управлінських реакцій, а також обґрунтування моделі, яка дозволила б зробити форсайт не аналітичним супроводом, а обов'язковим елементом економічної політики держави. Особлива увага приділяється монопольній структурі ринку та її впливу на макроекономічну стабільність.*

*У роботі показано, що домінування реактивної логіки, відсутність інституційного закріплення форсайту та збереження централізованої архітектури перетворили енергетичну систему на критичний фактор економічної вразливості. Рекомендації спрямовані на інтеграцію сценарного планування в бюджетний процес, просторове розміщення об'єктів і антимонопольну політику як складову національної безпеки. Результати можуть стати підставою для коригування державної політики в сфері економічної та енергетичної безпеки, а також для проєктів післявоєнної відбудови критичної інфраструктури.*

***Ключові слова:*** *енерегтична безпека, економічна безпека, загрози національній безпеці, стратегічний форсайт, управління ризиками*

**Lesya Skurenivska**
*Doctor of Economics*
*Senior Researcher*
*Deputy Head of the Defense Management*
*Training and Research Center*
*National Defense University of Ukraine*
*Kyiv, Ukraine*
*e-mail: olesya201405@gmail.com*
*ORCID: 0000-0003-4536-9170*

# STRUCTURAL DEFECTS OF INSTITUTIONAL SUPPORT OF STRATEGIC FORESIGHT AND ECONOMIC INSTABILITY OF UKRAINE'S ENERGY SYSTEM IN THE CONDITIONS OF FULL-SCALE WAR

***Abstract.*** *The article studies how the institutional failure of strategic foresight to transform into binding economic decisions increases the structural vulnerability of Ukraine's energy sector during the war. Most of the threats that are currently being implemented in the form of massive attacks on generation and transmission were clearly predicted as early as 2022. However, they have not become the basis for restructuring the system architecture in the direction of economic sustainability.*

*The aim of the work is to identify a deep gap between the level of risk predictability and the real quality of management responses, as well as to substantiate a model that would make foresight not an analytical support, but a mandatory element of the state's economic policy. Particular attention is paid to the monopoly structure of the market and its impact on macroeconomic stability.*

*The paper shows that the dominance of reactive logic, the lack of institutional consolidation of foresight, and the preservation of a centralized architecture have turned the energy system into a critical factor of economic vulnerability. The recommendations are aimed at integrating scenario planning into the budget process, spatial location of facilities, and antitrust policy as a component of national security.*

*The results may serve as a basis for adjusting state policy in the field of economic and energy security, as well as for projects for the post-war reconstruction of critical infrastructure.*

***Keywords:*** *energy security, economic security, threats to national security, strategic foresight, risk management.*

**JEL Classification:** Q48, H11, O21, H56

## Вступ

Повномасштабне вторгнення російської федерації змусило по-новому поглянути на природу сучасних загроз національній безпеці. Енергетичний сектор опинився не просто об'єктом руйнувань, а головним полем гібридної війни, де удари по інфраструктурі прямо підривають економічну спроможність держави. Масштабні атаки на генерацію, передачу та розподіл електроенергії виявили не стільки технічні недоліки, скільки системну неспроможність управлінських інститутів працювати на випередження.

З жовтня 2025 року країна втратила 8,5 ГВт потужностей, а імпорт електроенергії з Європи сягнув рекордних 1,9 ГВт. Ці цифри – не просто статистика руйнувань. Вони є прямим наслідком того, що прогнози, які роками готувалися в аналітичних центрах, так і не були перекладені мовою обов'язкових економічних рішень.

Стратегічний форсайт, який теоретично мав би слугувати інструментом випереджального управління ризиками, на практиці залишився радше академічним вправою. Це змушує поставити питання: чи не є така ситуація проявом глибшої інституційної кризи, коли наявність знань не супроводжується політичною волею та регуляторними механізмами їх реалізації?

Саме тому сьогодні особливо гостро постає потреба переосмислити роль форсайту не як допоміжного аналітичного інструменту, а як обов'язкового елемента системи забезпечення економічної безпеки держави в умовах воєнних загроз.

## Огляд літератури

Література з питань стратегічного форсайту та енергетичної безпеки значною мірою зосереджена на технічних і геополітичних аспектах. OECD та UNDP розглядають форсайт переважно як інструмент управління невизначеністю, проте рідко акцентують на механізмах його обов'язкової інтеграції в бюджетний процес. IEA та RAND Corporation

підкреслюють економічну доцільність превентивних інвестицій, однак часто залишають поза увагою інституційні причини їх відсутності.

Роботи Рябець Н. М. та Тимків І. В. [20] суттєво розширюють розуміння проблеми, акцентуючи на монополізації критичних мінералів як деструктивному чиннику глобального енергетичного переходу. Автори слушно зазначають, що перехід від паливоємної до мінералоємної моделі створює нові ризики, особливо коли контроль над ланцюгами постачання зосереджений у руках обмеженої кількості акторів.

Дослідження Лісового А.В. та співавторів [21] надає детальну емпіричну картину втрат українського енергетичного сектору: окупація Запорізької АЕС, руйнування ТЕС, падіння видобутку вуглеводнів, втрата значної частини ВДЕ. Автори обґрунтовано пов'язують ці втрати з необхідністю децентралізації та розвитку відновлюваних джерел як основи відновлення економічного потенціалу.

Разом ці джерела дозволяють стверджувати, що наукова дискусія поступово переходить від опису загроз до пошуку інституційних рішень. Водночас залишається недостатньо вивченим саме механізм трансформації форсайту в обов'язкові економічні рішення в умовах війни.

Важливим концептуальним і емпіричним підґрунтям цього дослідження стала колективна робота вітчизняних науковців Клята Ю., Гурковського В., Войтка О. [22] опублікована в журналі Social Development and Security (Т. 16. № 1. С. 20–33).

У статті "Недоліки стратегічного форсайту та вразливість енергетичної безпеки України в умовах війни: проблеми прогнозування та стійкості" автори здійснюють детальний аналіз причин системного розриву між рівнем прогнозованості енергетичних загроз і реальною якістю управлінських рішень. Виконане безпосередньо в умовах повномасштабної війни, це дослідження є одним із найбільш ґрунтовних вітчизняних напрацювань останнього періоду, де проблема інституційної неспроможності форсайту трансформуватися в обов'язкові економічні та інфраструктурні рішення розглядається через призму забезпечення макроекономічної стабільності та енергетичної стійкості держави. Висновки авторів щодо механізмів інституційної інерції, монопольних обмежень і короткозорості прогнозування лягли в основу концептуальної рамки поточного аналізу.

## Постановка проблеми

Енергетична криза в Україні виявилася не стільки наслідком браку генерації, скільки відсутністю заздалегідь підготовленої децентралізованої та стійкої моделі енергозабезпечення, яка б відповідала вимогам економічної безпеки. Навіть за значних бюджетних видатків захист об'єктів здійснювався фрагментарно, а підготовка до блекаутів залишалася переважно реактивною.

Центральним парадоксом є те, що атаки на енергетичну інфраструктуру не були несподіваними. Вони логічно випливали з характеру війни на виснаження і були описані в десятках міжнародних і національних документів. Проте стратегічний форсайт так і не став обов'язковою підставою для зміни архітектури системи, просторового розміщення об'єктів чи принципів резервування.

Інституційна інерція та монополізована структура ринку додатково ускладнили ситуацію. Навіть технічно можливі рішення – локальна генерація, підземне розміщення підстанцій, розвиток розподілених мереж – залишалися заблокованими на рівні регуляторних і політичних бар'єрів.

## Мета та завдання статті

Мета статті полягає не лише в констатації фактів, а в поясненні причин інституційного провалу та обґрунтуванні моделі, яка могла б забезпечити реальну трансформацію форсайт-сценаріїв у обов'язкові економічні рішення.

## Методи

Методологія дослідження поєднує інституційно-аналітичний підхід з елементами сценарного аналізу та аналізу державної політики в сфері економічної безпеки. Енергетична інфраструктура розглядається тут не як технічний комплекс, а як результат конкретних управлінських виборів, регуляторних обмежень і розподілу відповідальності між інституціями.

Сценарний аналіз дозволив зіставити прогнози міжнародних організацій з реальними подіями 2022–2025 років. Особливо показовим є те, що удари по підстанціях 750 кВ повністю відповідали сценаріям, які фігурували в документах ще до початку широкомасштабного вторгнення.

Інституційний аналіз допоміг виявити механізми блокування превентивних рішень, зокрема взаємодію центральних органів, регулятора та монопольних суб'єктів ринку. Порівняльний метод дав змогу зіставити українську практику з підходами країн, які стикалися з подібними загрозами.

Окремо варто зазначити, що методологія враховує не лише технічні, а й економічні наслідки інституційних дефектів, оскільки втрати енергетичної стійкості безпосередньо трансформуються в макроекономічні шоки.

## Результати

***Енергетична безпека України станом на квітень 2026 року: системна криза та контури нової моделі стійкості***

Енергетична безпека України продовжує визначати не лише щоденне функціонування економіки й життєдіяльності населення, а й загальну здатність держави протистояти війні. Зима 2025–2026 років стала найважчою за весь період повномасштабного вторгнення: рекордні морози до –26 °C, масовані атаки на генерацію та передачу призвели до оголошення енергетичної надзвичайної ситуації (14 січня 2026). За оцінками Міненерго та міжнародних партнерів, загальні втрати генеруючих потужностей сягнули 70–80 % від довоєнного рівня (з 38 ГВт до близько 14 ГВт доступної потужності). Це змусило країну імпортувати рекордні обсяги електроенергії з Європи – у лютому 2026 року імпорт перевищив 1,26 млн МВт·год, а в березні знизився на 25 % через потепління та часткове відновлення генерації.

Проте проблема не обмежується фізичними руйнуваннями. Як показують останні аналізи (зокрема колективна робота вітчизняних дослідників у Social Development and Security, 2026), ключовим фактором вразливості залишається інституційна неспроможність стратегічного форсайту перетворюватися на обов'язкові економічні рішення. Прогнози атак на енергосистему були відомі ще з 2022 року, проте централізована архітектура, монопольна структура ринку та домінування реактивної логіки управління зберегли систему в стані критичної залежності від вузлових об'єктів. Навіть значні бюджетні кошти та міжнародна допомога (ЄС надав 447 аварійних генераторів на 3,7 млн євро лише в січні 2026) часто використовувалися для латання наслідків, а не для превентивної перебудови.

У відповідь на це уряд активно формує нову архітектуру енергетичної безпеки. Пріоритети 2026 року – захист критичних вузлів, створення стратегічних резервів обладнання та розбудова щонайменше 1,5 ГВт розподіленої генерації (децентралізовані джерела, переважно ВДЕ з накопичувачами). Цей підхід відповідає рекомендаціям IEA та практикам країн, які стикалися з подібними загрозами: менші, розпорошені об'єкти важче уразити, швидше відновити та легше інтегрувати в мережу. Паралельно Верховна Рада розглядає законопроєкти про спрощення дозволів для стратегічних інфраструктурних проєктів за стандартами ЄС (TEN-E), а уряд імплементує європейські норми безпеки постачання газу (оновлення Закону "Про ринок природного газу").

Довгостроково енергетична безпека України все більше пов'язується з економічною трансформацією. План відновлення передбачає розширення інтерконекторів з ENTSO-E до 6 ГВт, нарощування ядерної генерації (нові блоки на Хмельницькій АЕС), розвиток 30+ ГВт ВДЕ та водневої інфраструктури. Це не просто технічне відновлення, а стратегічний перехід від паливоємної централізованої моделі до децентралізованої, електрифікованої та низьковуглецевої системи. Водночас залишаються серйозні ризики: залежність від імпорту обладнання та критичних матеріалів, дефіцит маневрових потужностей, інституційна інерція та недостатня антимонопольна політика.

Загалом ситуація на початку квітня 2026 року виглядає двоїсто. З одного боку – очевидний прогрес: синхронізація з європейською мережею, зростання ролі розподіленої генерації, активна міжнародна підтримка (ЄС, США, EBRD). З іншого енергосистема досі працює на межі, а системні інституційні дефекти, описані ще в довоєнних і ранньовоєнних дослідженнях, продовжують обмежувати стійкість. Енергетична безпека України сьогодні – це вже не лише питання "чи вистачить світла взимку", а фундаментальна умова економічного відновлення, обороноздатності та європейської інтеграції. Подальший розвиток залежатиме від того, наскільки швидко вдасться перейти від реактивного "латання" до системної превентивної трансформації, де стратегічний форсайт стане не декларацією, а обов'язковим елементом державного управління.

***Форсайт як інструмент забезпечення економічної та енергетичної безпеки в умовах війни***

Сучасне розуміння форсайту виходить далеко за межі традиційного прогнозування. Це не екстраполяція тенденцій, а системне конструювання альтернативних сценаріїв розвитку з чітким визначенням управлінських дій, необхідних для мінімізації економічних втрат. У воєнних умовах така логіка набуває особливого значення.

Документи OECD та рекомендації NATO Energy Security Centre of Excellence підкреслюють, що форсайт має бути інтегрований у бюджетне планування та регулювання критичної інфраструктури. На практиці ж в Україні він часто залишається на рівні аналітичних звітів, що не мають нормативної сили.

Особливість воєнного форсайту полягає в тому, що загрози носять не абстрактний, а цілеспрямований характер. Атаки на енергетичну інфраструктуру є інструментом підриву не лише фізичної, а й економічної стійкості держави. Саме тому форсайт повинен виконувати три функції одночасно: аналітичну, нормативно-обмежувальну та інституційну.

На наш погляд, без закріплення останньої функції в нормативних актах (зокрема через оновлення Закону України "Про критичну інфраструктуру" та Енергетичної стратегії України) форсайт так і залишатиметься декларативним інструментом.

Розрив між стратегічним форсайтом і економічно обґрунтованими управлінськими рішеннями в Україні

Розрив між прогнозами та діями є не випадковістю, а системним явищем. Реактивна логіка управління домінує над превентивною, а підготовчі заходи відкладаються до моменту, коли криза вже настала. Міжнародні звіти та матеріали The New York Times і Reuters 2026 року чітко фіксують цей патерн.

Збереження централізованої архітектури системи не можна пояснити лише технічною інерцією. Це свідомий інституційний вибір, який концентрує економічні ризики в кількох вузлових точках. Монополізація ринку, як слушно зазначають автори Central European Journal of International and Security Studies, обмежує адаптивність і виключає альтернативні сценарії з політичного порядку денного.

Рябець Н. М. і Тимків І. В. [20] доповнюють цю картину, показуючи, як монополізація критичних ресурсів посилює вразливість усього енергетичного переходу. Лісовий А. В. та співавтори [21] наводять конкретні цифри втрат потужностей, які підтверджують, що централізація стала одним із головних чинників економічної нестійкості.

Такий розрив має не лише технічний, а насамперед економічний вимір: він безпосередньо впливає на макроекономічну стабільність, бюджетні видатки та інвестиційний клімат.

***Логічна модель "форсайт → економічно обґрунтовані управлінські рішення → стійка інфраструктура"***

Центральною проблемою залишається саме відсутність механізму, який би змушував форсайт впливати на реальні рішення. Запропонована логічна модель дозволяє простежити причинно-наслідкові зв'язки між аналітичними оцінками, управлінськими діями та кінцевим станом інфраструктури.

Для наочного зіставлення фактичного стану справ і нормативної моделі в дослідженні використана порівняльна таблиця "Було / Має бути". Вона виконує не описову, а діагностичну функцію, демонструючи розбіжність між реактивною практикою, що склалася в Україні, та тією моделлю управління, яка випливає з рекомендацій OECD, IEA, World Bank та сучасних досліджень енергетичної безпеки як wicked problem.

Таблиця 1

Порівняльна характеристика трансляції стратегічного форсайту в економічно обґрунтовані управлінські та інфраструктурні рішення

| Аналітичиний вимір | Було (де-факто) | Має бути (нормативна модель) |
|---|---|---|
| Роль форсайту | Дорадчий характер, не обов'язковий | Інституційний як обов'язковий елемент управління |
| Зв'язок з бюджетом | Відсутній прямий зв'язок | Форсайт-сценарії інтегровані в бюджетне планування |
| Архітектура енергосистеми | Висока централізація, залежить від вузлових об'єктів | Децентралізована система з локальними мережами та резервуванням |
| Просторове розміщення | Переважно надземна інфраструктура | Пріоритет підземному розміщенню критичних елементів |
| Реакція на загрози | Реактивна: дії після атак | Превентивна: підготовка до найгірших сценаріїв |
| Структура ринку | Домінування монопольних операторів | Диверсифікація та антимонопольні механізми |
| Захист населення та економіки | Перекладання відповідальності на населення і бізнес | Централізована муніципальна політика стійкості |

Модель враховує не лише технічні аспекти, а й економічні: інтеграцію форсайту в бюджетне планування, антимонопольні механізми та пріоритет підземного розміщення об'єктів. Саме такий комплексний підхід відповідає сучасним уявленням про whole-of-systems approach у енергетичній безпеці.

Хоча деякі автори вважають, що технічні рішення можуть вирішити проблему самі по собі, емпіричні дані українського кейсу свідчать про протилежне: без інституційних змін будь-які інвестиції залишатимуться малоефективними.

***Інституційний провал стратегічного форсайту: сутність, причини та наслідки***

Інституційний провал стратегічного форсайту в Україні не є простою технічною недоробкою чи браком аналітичних даних. Це системне явище, коли наявні прогнози загроз не трансформуються в обов'язкові управлінські рішення, а залишаються на рівні дорадчих рекомендацій. Саме такий розрив, як показує колективна робота Клят Ю., Гурковського В.,

Войтка О. та співавторів (2026), став однією з головних причин, чому енергетична система країни опинилася в стані критичної вразливості під час повномасштабної війни. Прогнози масованих атак на вузлові елементи передачі електроенергії, зокрема підстанції 750 кВ, фігурували в міжнародних і національних документах ще з 2022 року, проте не були перекладені на мову конкретних регуляторних вимог, бюджетних пріоритетів чи змін у просторовому плануванні.

Причини цього провалу лежать значно глибше за відсутність політичної волі.

По-перше, це хронічна інституційна інерція: державні органи продовжували діяти в рамках довоєнної логіки, де енергетична безпека сприймалася переважно як питання технічної надійності, а не економічної стійкості.

По-друге, монопольна структура ринку – домінування кількох великих операторів у генерації та передачі – створила додаткові бар'єри для впровадження альтернативних рішень. Локальна генерація, підземне розміщення об'єктів, розвиток розподілених мереж – усі ці технічні можливості залишалися заблокованими через регуляторні та економічні інтереси, які не співпадали з вимогами національної безпеки.

Відсутність нормативного закріплення форсайту як обов'язкового елемента державного управління зробила його фактично необов'язковим. Навіть коли прогнози були точними, вони не мали юридичної сили, яка б змушувала міністерства, регулятора чи місцевої влади діяти превентивно.

Наслідки такого провалу стали очевидними вже в перші місяці широкомасштабного вторгнення і досягли піку взимку 2025–2026 років. Рекордні втрати потужностей (близько 70–80 % від довоєнного рівня), масовий імпорт електроенергії та оголошення енергетичної надзвичайної ситуації – це не просто статистика руйнувань. Це матеріалізований результат того, що знання про загрози не перетворилося на дію. Як слушно зазначають Лісовий А. В. та співавтори (2025), навіть значні бюджетні асигнування та міжнародна допомога часто витрачалися на ліквідацію наслідків, а не на зниження вразливості системи. У підсумку енергетична безпека перетворилася на критичний фактор економічної нестабільності: зростання імпортних витрат, інфляційний тиск, зупинка промисловості та соціальна напруга.

Таким чином, інституційний провал стратегічного форсайту виявився не окремим недоліком, а системним дефектом моделі державного управління. Він показав, що без радикальної зміни підходів – від інституціоналізації форсайту як обов'язкового елемента політики до демонополізації ринку та переходу до децентралізованої архітектури – жодні інвестиції в відновлення не гарантуватимуть довгострокової стійкості. Саме тому подолання цього провалу сьогодні є не технічним, а принципово управлінським завданням, від вирішення якого залежить не лише енергетична безпека, а й загальна економічна спроможність держави в умовах війни.

## Висновки

Проведене дослідження переконливо показує, що енергетична криза, яка досягла піку взимку 2025–2026 років, є не стільки наслідком інтенсивності російських атак, скільки результатом глибокого інституційного провалу. Прогнози масованих ударів по генерації та системі передачі були відомі ще з 2022 року, проте стратегічний форсайт так і не став обов'язковим елементом економічної політики держави. Саме цей розрив між рівнем прогнозованості ризиків і якістю управлінських рішень, як детально продемонстрували Клят Ю., Гурковський В. та співавтори (2026), перетворив енергетичну систему на один із найуразливіших компонентів національної безпеки.

Емпіричні дані, зібрані Лісовим А. В. та ін. (2025), доповнені аналізом монополізації критичних ресурсів у роботі Рябець Н. М. і Тимків І. В. (2024), підтверджують: збереження централізованої архітектури та домінування реактивної логіки управління не дозволили використати наявні знання для превентивної перебудови сектору. Рекордні втрати

потужностей, масовий імпорт електроенергії та оголошення енергетичної надзвичайної ситуації стали логічним наслідком інституційної інерції, а не браку технічних можливостей чи фінансових ресурсів.

Отже, енергетична безпека України сьогодні не може розглядатися окремо від економічної. Вона є питанням якості державного управління, здатності інститутів трансформувати аналітичні оцінки в обов'язкові регуляторні та бюджетні рішення. Без радикальної зміни підходів інституціоналізації стратегічного форсайту, демонополізації ринку та переходу до децентралізованої моделі, навіть значні інвестиції в відновлення інфраструктури даватимуть лише тимчасовий ефект.

У довгостроковій перспективі подолання цього інституційного розриву стає ключовою умовою не лише стабілізації енергосистеми, а й відновлення економічного потенціалу держави загалом. Лише коли стратегічний форсайт перестане бути декларативним інструментом і набуде нормативної сили, Україна зможе перейти від крихкої, централізованої моделі до стійкої, адаптивної енергетичної системи, яка відповідатиме вимогам сучасної війни та європейської інтеграції.

## Список використаних джерел


1. BBC News Україна. Удари РФ по енергетиці України: наслідки для цивільного населення. 2024. URL: https://www.bbc.com/ukrainian/articles/cq6v82gy094o (дата звернення: 10.01.2026).
2. RAND Corporation. Russia's Attacks on Ukraine's Energy Infrastructure. URL: https://www.rand.org/ (дата звернення: 12.01.2026).
3. World Bank. Resilient Infrastructure for Sustainable Development. Washington, DC : World Bank, 2021.
4. NATO Energy Security Centre of Excellence. Energy Infrastructure Protection and Resilience. Vilnius : NATO ENSEC COE, 2022.
5. Organisation for Economic Co-operation and Development (OECD). Strategic Foresight for Better Policies. Paris : OECD Publishing, 2019.
6. United Nations Development Programme (UNDP). Foresight Manual. New York : UNDP, 2018.
7. Miles I., Saritas O., Sokolov A. Foresight for Science, Technology and Innovation. Cheltenham : Edward Elgar Publishing, 2016.
8. European Commission. Energy Market Design and Competition Policy. Brussels, 2020.
9. Міністерство енергетики України. Стан енергетичної системи в умовах воєнного стану. URL: https://www.mev.gov.ua (дата звернення: 10.01.2026).
10. European Investment Bank. Underground Infrastructure and Urban Resilience. Luxembourg : EIB, 2021.
11. International Energy Agency. Energy Security and Resilience. Paris : IEA, 2022.
12. Лебедина О. Patriot не для дронів: захист критичної інфраструктури України. *ZN.UA*. URL: https://zn.ua/ukr/POLITICS/patriot-ne-dlja-droniv-zelenskij-rozkritikuvav-zakhist-kritichnikh-objektiv.html (дата звернення: 11.01.2026).
13. International Energy Agency. Energy Security and Resilience. URL: https://www.iea.org/topics/energy-security (дата звернення: 12.01.2026).
14. The New York Times. Russian Strike Leaves Ukrainian City Struggling to Restore Heat. URL: https://www.nytimes.com/2026/01/08/world/europe/ukraine-dnipro-power-russia-strike-heat.html (дата звернення: 15.01.2026).
15. Reuters. Russian drone attack forces power cuts in Ukraine's Kryvyi Rih, military says. URL: https://www.reuters.com/world/russian-drone-attack-forces-power-cuts-ukraines-kryvyi-rih-military-says-2026-01-14/ (дата звернення: 15.01.2026).
16. Novikau A. Energy Security in Security Studies: A Systematic Review of Twenty Years of Literature. *Central European Journal of International and Security Studies*. 2023. Vol. 17., Iss P. 34-64. URL: https://doi.org/10.51870/PDDC2102.
17. Brown M., et al. Energy Security as a Wicked Problem: A Foresight Approach to Developing a Grand Strategy for Resilience. *The Solutions Journal*. February 22, 2016. URL: https://thesolutionsjournal.com/energy-security-as-a-wicked-problem-a-foresight-approach-to-developing-a-grand-strategy-for-resilience/#:~:text=Energy%20Security%20as%20a%20%22Wicked%20Problem%22%E2%80%94A%20Foresight,to%20Developing%20a%20Grand%20Strategy%20for%20Resilience.
18. Center for Strategic and International Studies. Risk and Foresight Group. Washington, DC : CSIS.
19. International Energy Agency. Summit on the Future of Energy Security: Background Paper. Paris : IEA, 2023.

20. Рябець Н. М., Тимків І. В. Глобальна енергетична безпека: концепт, фактори та шляхи забезпечення. *Економіка та суспільство.* 2024. Вип. 61. URL: https://doi.org/10.32782/2524-0072/2024-61-120.
21. Лісовий А. В., Андрух О. В. Енергетична безпека України: виклики війни та перспективи відновлення економічного потенціалу. *Український економічний часопис.* 2025. Вип. 8. С. 40-43. URL: https://doi.org/10.32782/2786-8273/2025-8-7.
22. Клят Ю., Гурковський В., Войтко О. Недоліки стратегічного форсайту та вразливість енергетичної безпеки України в умовах війни: проблеми прогнозування та стійкості. *Social Development and Security*. 2026. Т. 16. № 1. С. 20–33. URL: https://doi.org/10.33445/sds.2026.16.1.2; https://paperssds.eu/index.php/JSPSDS/article/view/1045 (дата звернення: 04.03.2026).

## References

1. BBC News Ukraina. (2024). Udary RF po enerhetytsi Ukrainy: naslidky dlia tsyvilnoho naselennia [Russian attacks on Ukraine's energy sector: consequences for the civilian population]. Retrieved from: https://www.bbc.com/ukrainian/articles/cq6v82gy094o (accessed 10.01.2026) [in Ukrainian].
2. RAND Corporation. Russia's Attacks on Ukraine's Energy Infrastructure. Retrieved from: https://www.rand.org/ (accessed 12.01.2026).
3. World Bank. (2021). Resilient Infrastructure for Sustainable Development. Washington, DC: World Bank.
4. NATO Energy Security Centre of Excellence. (2022). Energy Infrastructure Protection and Resilience. Vilnius: NATO ENSEC COE.
5. Organisation for Economic Co-operation and Development (OECD). (2019). Strategic Foresight for Better Policies. Paris: OECD Publishing.
6. United Nations Development Programme (UNDP). (2018). Foresight Manual. New York : UNDP.
7. Miles, I., Saritas, O., & Sokolov, A. (2016). Foresight for Science, Technology and Innovation. Cheltenham : Edward Elgar Publishing.
8. European Commission. (2020). Energy Market Design and Competition Policy. Brussels.
9. Ministerstvo enerhetyky Ukrainy. Stan enerhetychnoi systemy v umovakh voiennoho stanu [State of the Energy System under Martial Law]. Retrieved from: https://www.mev.gov.ua (accessed 10.01.2026) [in Ukrainian].
10. European Investment Bank. (2021). Underground Infrastructure and Urban Resilience. Luxembourg: EIB.
11. International Energy Agency. (2022). Energy Security and Resilience. Paris: IEA.
12. Lebedyna, O. (2025). Patriot ne dlia droniv: zakhyst krytychnoi infrastruktury Ukrainy [Patriot is not for drones: protecting Ukraine's critical infrastructure]. *ZN.UA.* Retrieved from: https://zn.ua/ukr/POLITICS/patriot-ne-dlja-droniv-zelenskij-rozkritikuvav-zakhist-kritichnikh-objektiv.html (дата звернення: 11.01.2026) [in Ukrainian].
13. International Energy Agency. (2025). Energy Security and Resilience. Retrieved from: https://www.iea.org/topics/energy-security (accessed 12.01.2026).
14. The New York Times. (2026). Russian Strike Leaves Ukrainian City Struggling to Restore Heat. Retrieved from: https://www.nytimes.com/2026/01/08/world/europe/ukraine-dnipro-power-russia-strike-heat.html (accessed 15.01.2026).
15. Reuters. (2026). Russian drone attack forces power cuts in Ukraine's Kryvyi Rih, military says. URL: https://www.reuters.com/world/russian-drone-attack-forces-power-cuts-ukraines-kryvyi-rih-military-says-2026-01-14/ (accessed 15.01.2026).
16. Novikau, A. (2023). Energy Security in Security Studies: A Systematic Review of Twenty Years of Literature. *Central European Journal of International and Security Studies*, 17, 3, 34-64. Retrieved from: https://doi.org/10.51870/PDDC2102.
17. Brown M., et al. (2016.). Energy Security as a Wicked Problem: A Foresight Approach to Developing a Grand Strategy for Resilience. *The Solutions Journal*. Retrieved from: https://thesolutionsjournal.com/energy-security-as-a-wicked-problem-a-foresight-approach-to-developing-a-grand-strategy-for-resilience/#:~:text=Energy%20Security%20as%20a%20%22Wicked%20Problem%22%E2%80%94A%20Foresight,to%20Developing%20a%20Grand%20Strategy%20for%20Resilience.
18. Center for Strategic and International Studies. Risk and Foresight Group. Washington, DC : CSIS.
19. International Energy Agency. (2023). Summit on the Future of Energy Security: Background Paper. Paris: IEA.
20. Riabets, N. M., & Tymkiv, I. V. (2024). Hlobalna enerhetychna bezpeka: kontsept, faktory ta shliakhy zabezpechennia [Global energy security: concept, factors and ways of ensuring it]. *Ekonomika ta suspilstvo*, 61. Retrieved from: https://doi.org/10.32782/2524-0072/2024-61-120 [in Ukrainian].

21. Lisovyi, A. V., & Andrukh, O. V. (2025). Enerhetychna bezpeka Ukrainy: vyklyky viiny ta perspektyvy vidnovlennia ekonomichnoho potentsialu [Energy security of Ukraine: challenges of war and prospects for restoring economic potential]. *Ukrainskyi ekonomichnyi chasopys*, 8, 40-43. Retrieved from: https://doi.org/10.32782/2786-8273/2025-8-7 [in Ukrainian].
22. Kliat, Yu., Hurkovskyi, V., & Voitko, O. (2026). Nedoliky stratehichnoho forsaitu ta vrazlyvist enerhetychnoi bezpeky Ukrainy v umovakh viiny: problemy prohnozuvannia ta stiikosti [Shortcomings of strategic foresight and vulnerability of Ukraine's energy security in war conditions: problems of forecasting and sustainability]. *Social Development and Security*, 16, 1, 20–33. Retrieved from: https://doi.org/10.33445/sds.2026.16.1.2; https://paperssds.eu/index.php/JSPSDS/article/view/1045 (дата звернення: 04.03.2026) [in Ukrainian].

*Received 22.01.2026 | Accepted 10.02.2026 | Published 30.03.2026*


УДК 339.923:338.1(470):355.01 DOI: 10.63978/3083-6476.2026.1.4.08

**Слюсаренко Марина Олександрівна**
*кандидат технічних наук,*
*старший дослідник*
*старший науковий співробітник*
*Центральний науково-дослідний інститут*
*Збройних сил України*
*Київ, Україна*
*e-mail: slusarenko@gmail.com*
*ORCID: 0000-0003-4165-3908*

**Фурманов Костянтин Віталійович**
*кандидат військових наук*
*старший науковий співробітник*
*начальник управління – заступник начальника центру*
*Центральний науково-дослідний інститут*
*Збройних сил України*
*Київ, Україна*
*e-mail: k.furmanov16@gmail.com*
*ORCID: 0000-0002-0049-8959*

# АНАЛІЗ ВПЛИВУ МІЖНАРОДНОЇ САНКЦІЙНОЇ ПОЛІТИКИ НА СТАН ЕКОНОМІКИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

***Анотація.*** *Актуальність дослідження обумовлена необхідністю оцінювання впливу міжнародної санкційної політики на економіку російської федерації в умовах повномасштабної російсько-української війни. Після початку агресії проти України у 2022 році проти рф було запроваджено масштабні санкції, які охопили фінансову систему, енергетичний сектор, зовнішню торгівлю, технологічний трансфер та активи політичної й економічної еліти. Це зумовлює потребу комплексного аналізу їхнього впливу на економічний потенціал держави та її здатність продовжувати війну.*

*Метою статті є аналіз впливу міжнародних санкцій на стан економіки російської федерації. У дослідженні застосовано системний та структурно-функціональний підходи, а також методи порівняльного аналізу, статистичного узагальнення й аналізу динаміки макроекономічних показників.*

*За результатами дослідження встановлено, що санкції мають комплексний характер і впливають на ключові сектори російської економіки. Фінансові обмеження призвели до замороження значної частини міжнародних резервів, ускладнення міжнародних розрахунків та скорочення іноземних інвестицій. Енергетичні санкції спричинили зниження доходів від експорту нафти й газу, необхідність переорієнтації експорту на азійські ринки та зростання логістичних витрат. Обмеження на постачання високотехнологічної продукції призводять до дефіциту комплектуючих і технологічної деградації окремих галузей промисловості. Водночас у структурі російського бюджету зростає частка військових витрат, що супроводжується збільшенням бюджетного дефіциту та використанням резервних фондів.*

*Зроблено висновок, що у короткостроковій перспективі російська федерація зберігає можливість фінансувати війну за рахунок доходів від експорту енергоносіїв, використання резервів та посилення внутрішнього фіскального тиску. Проте у середньо- та довгостроковій перспективі санкції істотно обмежують економічний потенціал рф, посилюють структурні дисбаланси та знижують її можливості щодо ведення тривалої війни.*

*Перспективи подальших досліджень пов'язані з аналізом соціально-економічних наслідків санкцій для різних регіонів і соціальних груп населення російської федерації, а також їх впливу на внутрішньополітичну стабільність держави.*

***Ключові слова:*** *міжнародні санкції, економіка російської федерації, фінансування війни, енергетичний сектор, фінансова система, бюджетна політика, технологічна деградація, військово-промисловий комплекс, соціально-економічні наслідки.*

**Maryna Sliusarenko**
*Candidate of Technical Sciences,*
*Senior Research Scientist*
*Senior Research*
*Central Research Institute*
*of the Armed Forces of Ukraine*
*Kyiv, Ukraine*
*e-mail: slusarenko@gmail.com*
*ORCID: 0000-0003-4165-3908*

**Kostiantyn Furmanov**
*Candidate of Military Sciences,*
*Senior Researcher*
*Head of Directorate,*
*The Central Research Institute*
*of the Armed Forces of Ukraine*
*Kyiv, Ukraine*
*e-mail: k.furmanov16@gmail.com*
*ORCID: 0000-0002-0049-8959*

# ANALYSIS OF THE IMPACT OF INTERNATIONAL SANCTIONS POLICY ON THE STATE OF THE RUSSIAN FEDERATION'S ECONOMY

***Abstract.*** *The relevance of the study is the unprecedented scale and complexity of international sanctions imposed on the russian federation after the start of its full-scale aggression against Ukraine, as well as the need for an objective assessment of their real impact on the economy of the aggressor state and its ability to continue the war in the medium and long term.*

*In this regard, the article is aimed at providing a comprehensive analysis of the economic consequences of sanctions for russian federation and determining their impact on the financial, energy, industrial, and budgetary capacities of the country to finance military operations.*

*The leading approach to the study of this problem is a systemic and structural-functional analysis, which makes it possible to comprehensively examine the impact of sanctions on key sectors of the russian economy, along with the use of comparative analysis, statistical generalization, and time-series analysis of macroeconomic indicators.*

*The article presents a classification of the main groups of sanctions, reveals their impact on the financial system, energy sector, industry, and budgetary policy of the russian federation, identifies trends toward technological degradation and increased dependence of the economy on military production, and substantiates the limitations of Russia's ability to finance the war in the medium and long term.*

*The materials of the article are of practical value for specialists in the fields of economic security, public administration, and defense planning and may be used in the development of sanctions policy, assessment of the economic resilience of the aggressor state, and elaboration of international pressure measures aimed at weakening its military potential.*

***Keywords:*** *international sanctions; economy of the russian federation; war financing; energy sector; financial system; fiscal policy; technological degradation; military-industrial complex; socio-economic consequences.*

**JEL Classification:** F51, P27, Q43, E62, F38

## Вступ

Міжнародні санкції, запроваджені проти російської федерації після початку повномасштабної агресії проти України у 2022 році, стали безпрецедентними за масштабом і комплексністю. Вони охопили фінансову систему, енергетичний сектор, промисловість, експортно-імпортні операції, транспорт, технологічний трансфер та персональні активи політичної й економічної еліти. Метою санкцій було суттєве обмеження ресурсної бази рф, зниження її економічного потенціалу та, як наслідок, зменшення спроможності вести тривалу війну.

Актуальність теми зумовлена необхідністю оцінювання реального впливу санкцій на російську економіку та військові можливості держави-агресора. Попри офіційну риторику російської влади про "стійкість" економіки, незалежні експертні оцінки свідчать про глибокі структурні деформації, зростання залежності від військового виробництва та технологічну деградацію.

## Огляд літератури

Західні санкції та економічна ізоляція росії негативно впливають на російську економіку. За перебігом подій уважно слідкують багато фахівців. Автор у [1] аналізує критичний стан економіки рф, виділяючи три основних фактори: рецесію, інфляцію й бюджетну кризу. Як економічні санкції впливають на авторитарні режими на прикладі рф досліджується у [2]. Про вплив санкцій на фінансову стабільність ідеться у офіційному макроекономічному звіті про економіку рф [3]. Дострокову стагнацію економіки через санкції та війну оцінює світовий банк [4]. Джерело [5] порівнює економіку рф до і після санкцій: падіння продуктивності, втрата технологій обмеження експорту та імпорту. Фахівці у [6] аналізують як санкції ЄС впливають на російський експорт, як зменшуються доходи від енергоносіїв, розглядають проблеми з обходом санкцій і необхідністю контролю.

Дослідники у [7] розглядають вплив санкцій на здатність рф фінансувати війну. Серед вітчизняних спеціалістів, які досліджують вплив санкцій на економіку рф, це [8]–[10]. Однак у цих працях не розкрито комплексного впливу міжнародних санкцій на економіку російської федерації та її здатність продовжувати війну.

## Мета та завдання статті

Мета статті – проаналізувати вплив міжнародних санкцій на стан економіки російської федерації.

## Методи

Провідним підходом для дослідження цієї проблеми є системний і структурно-функціональний аналіз, що дозволяє комплексно розглянути вплив санкцій на ключові сектори економіки рф, а також застосування методів порівняльного аналізу, статистичного узагальнення та аналізу динамічних рядів макроекономічних показників.

## Результати

Санкції проти росії мають комплексний характер, їх можна поділити на кілька основних груп, табл. 1.

Таблиця 1

Основні групи санкцій, які застосовуються проти рф

| Групи санкцій | Стислий зміст |
|---|---|
| Фінансові | Відключення окремих банків від системи SWIFT, заморожування валютних резервів Центрального банку рф за кордоном, обмеження доступу до міжнародних ринків капіталу |
| Торговельні | Заборона або обмеження експорту високотехнологічної продукції (мікроелектроніка, авіаційні компоненти, обладнання подвійного призначення) |
| Енергетичні | Ембарго або обмеження на імпорт нафти, нафтопродуктів і газу з рф у країни ЄС та інші держави |
| Персональні | Блокування активів та обмеження пересування для представників політичної, військової й економічної еліти рф |
| Технологічні | Обмеження доступу до сучасних технологій у сфері IT, машинобудування, авіа- та суднобудування |

Джерело: авторська розробка

Комплексність цих заходів спрямована не лише на скорочення поточних доходів держави, а й на підрив її довгострокового економічного розвитку. Розглянемо, як впливають санкції на фінансову систему рф.

1. *Фінансова система* стала однією з перших сфер, що зазнали удару. Замороження значної частини золотовалютних резервів Центрального банку рф позбавило уряд можливості повноцінно стабілізувати курс національної валюти та фінансувати бюджетні дефіцити за рахунок зовнішніх ресурсів.

Відключення низки банків від SWIFT (Society for Worldwide Interbank Financial) ускладнило міжнародні розрахунки та призвело до зростання транзакційних витрат. Російські банки були змушені переорієнтовуватися на внутрішній ринок і на альтернативні платіжні системи (китайська CIPS, внутрішня система “Мир”), які не можуть повноцінно замінити глобальну фінансову інфраструктуру. Крім того, санкції спричинили відтік капіталу та скорочення прямих іноземних інвестицій. Західні компанії масово залишили російський ринок або призупинили діяльність, що негативно позначилося на зайнятості та доходах населення.

Санкції, введені ЄС та його партнерами проти фінансової системи росії, обмежують можливості рф фінансувати війну. 300 млрд євро резервів російського центрального банку заблоковано в ЄС (дві третини), в інших країнах G7 та Австралії. 70 % активів російської банківської системи підпадають під санкції. Заморожено близько 20 млрд євро активів понад 1500 осіб та організацій, на яких накладено санкції.

Оскільки ключова ставка є фундаментальним елементом фінансової системи держави та основним інструментом її грошово-кредитної політики розглянемо, як змінювалася динаміка ключової ставки рф, рис. 1.

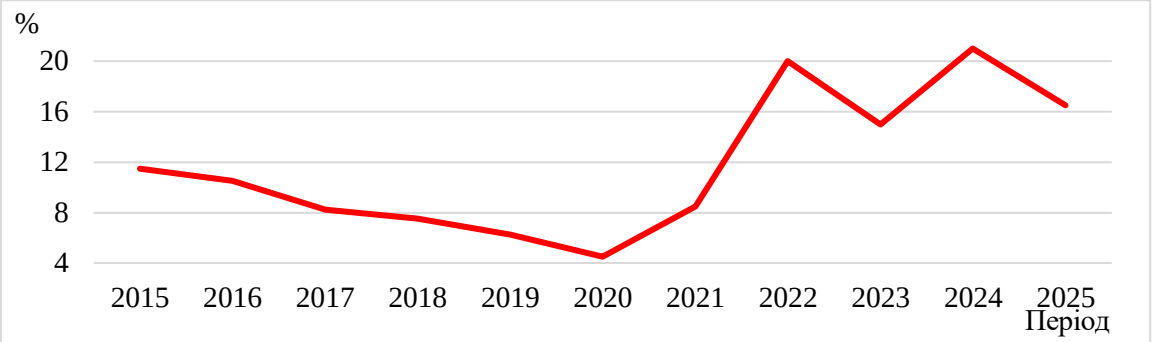


Рис. 1. Динаміка змінення ключової ставки рф протягом 2015–2025 р.р.
*Джерело: розроблено авторами за даними [11]*

Як видно, з 2022 року відбуваються різкі коливання під час початку повномасштабної війни в Україні; у 2023–2024 р.р. – потужний тренд на підвищення, ставка зросла до 21 % у жовтні 2024 р. у відповідь на високі темпи інфляції; 2025 р. 16 % та 2026 – 15,5 %, незначне зниження.

2. *Енергетичний сектор* традиційно є основою російського бюджету. До запровадження санкцій понад третина бюджетних доходів формувалася за рахунок експорту нафти і газу. Ембарго ЄС на російську нафту та нафтопродукти, а також обмеження на імпорт газу змусили рф переорієнтовувати експорт на країни Азії, передусім Китай та Індію. Однак така переорієнтація супроводжується значними втратами:

– продаж нафти здійснюється зі значними знижками;
– зростають логістичні витрати через більші відстані транспортування;
– інфраструктура не повністю адаптована до нових маршрутів.

У результаті доходи від енергетичного експорту зменшуються, що безпосередньо впливає на наповнення бюджету та, відповідно, на фінансування військових витрат.

У квітні 2025 року доходи росії від експорту нафти впали до 13,2 млрд доларів – це другий найнижчий рівень з моменту введення енергетичних санкцій. Середня ціна бареля російської нафти другий місяць поспіль залишалася нижче 60 доларів, що пов’язано з тенденціями на світовому ринку та рішеннями країн ОПЕК+. Якщо така ситуація триватиме, зовнішні рахунки росії можуть зазнати значного тиску. У січні-квітні 2025 року доходи бюджету від нафти і газу зменшилися на 10% порівняно з аналогічним періодом 2024 року. Динаміку нафтогазових доходів рф та їх частку у загальних доходах бюджету наведено на рис. 2.

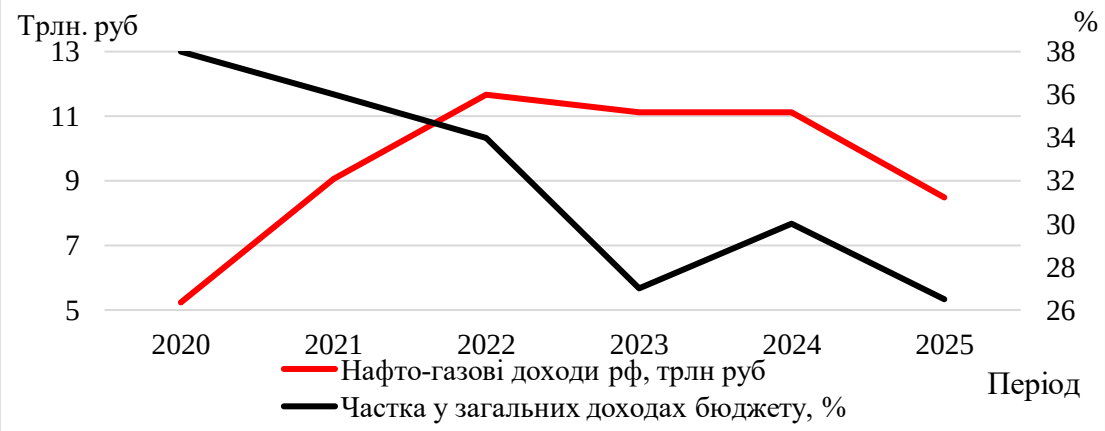


Рис. 2. Динаміка змінення нафтогазових доходів рф та їх частки у загальних доходах бюджету
*Джерело: розроблено авторами за даними [12]*

Як видно спостерігається різке падіння частки у 2023 році та подальше зниження у 2025 році як в абсолютних доходах, так і у відсотковій частці бюджету.

3. *Промисловість і технологічна деградація*. Санкції проти високотехнологічного експорту призвели до дефіциту комплектуючих у багатьох галузях: авіабудуванні, автомобілебудуванні, електроніці, приладобудуванні. Російська промисловість значною мірою залежала від імпортних компонентів, особливо у сфері мікроелектроніки. В умовах обмеженого доступу до західних технологій рф намагається замінити імпорт за рахунок внутрішнього виробництва або постачання з третіх країн. Проте така "імпортозаміна" часто означає зниження якості продукції, технологічне відставання та зростання собівартості. Особливо гостро проблема проявляється у військово-промисловому комплексі, де сучасні системи озброєння потребують високотехнологічних компонентів. Дефіцит таких елементів знижує темпи виробництва та модернізації озброєння.

4. *Бюджетна політика* та зростання військових витрат. Після початку повномасштабної війни структура російського бюджету зазнала суттєвих змін. Значно зросла частка витрат на оборону та безпеку. У квітні 2025 р. росія була змушена провести перегляд федерального бюджету – раніше, ніж будь-коли в новітній історії. Це призвело до скорочення фінансування соціальних програм, освіти, охорони здоров'я та інфраструктурних проєктів. Для покриття дефіциту бюджету уряд рф використовував Фонд національного добробуту (ФНД) та внутрішні запозичення. Проте ці ресурси не є безмежними й на сьогодні ФНД практично вичерпано. В умовах зменшення експортних доходів і стагнації економіки фінансування війни дедалі більше здійснюється за рахунок внутрішніх резервів і прихованої інфляції. На рис. 3 показано як змінювався ФНД протягом 2022–2025 р.р.

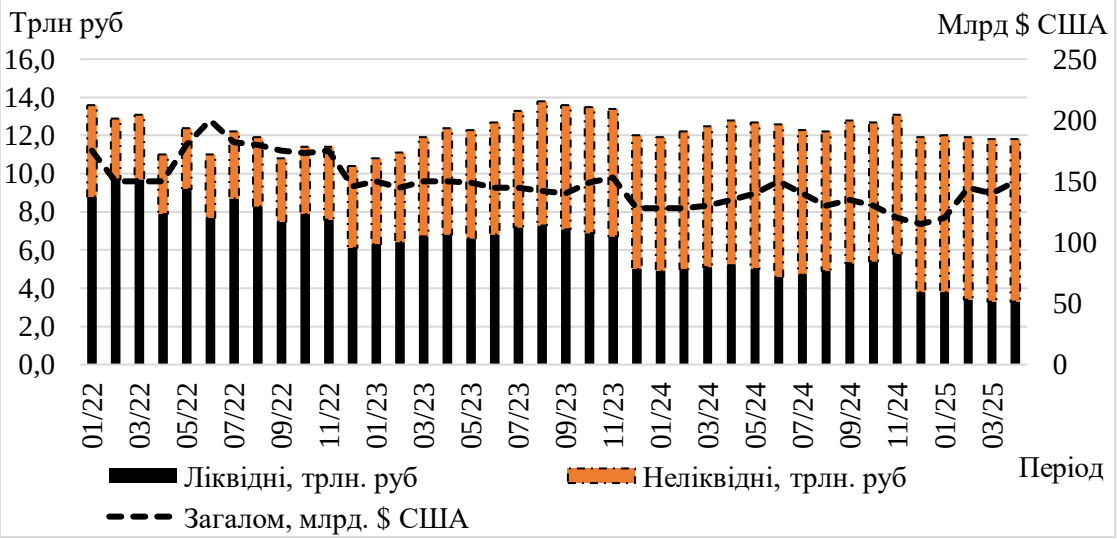


Рис. 3. Змінення активів ФНД, у млрд руб. та млрд. $ США
*Джерело: розроблено авторами за даними [13]*

За роки війни росія втратила понад дві третини ліквідних коштів ФНД. Через високий дефіцит бюджету у січні 2026 р. (понад 22 млрд. дол.) запасів майже не залишилося. Основні ліквідні активи складаються із китайських юанів та золота.

5. *Соціально-економічні наслідки санкцій.* Санкції та війна призвели до зниження рівня життя населення. Реальні доходи громадян скорочуються через інфляцію та зростання цін на імпортні товари. Водночас офіційна статистика часто не відображає реальних масштабів проблем через адміністративний контроль і зміну методик підрахунку. Ринок праці зазнав структурних змін: зростає зайнятість у військовому секторі та суміжних

галузях, тоді як цивільні сектори (послуги, малий бізнес, торгівля) скорочуються. Це формує деформовану економічну модель, орієнтовану на війну.

6. *Здатність рф фінансувати війну* в короткостроковій перспективі. У короткостроковій перспективі Росія зберігає можливість фінансувати війну завдяки:

– наявності залишкових резервів;

– доходам від експорту енергоносіїв;

– посиленню податкового тиску на бізнес і населення;

– використанню емісійних механізмів.

Однак така модель є нестійкою, оскільки базується на вичерпанні ресурсів і посиленні внутрішніх економічних дисбалансів.

7. *Середньо- та довгострокові обмеження.* У середньо- та довгостроковій перспективі вплив санкцій стає більш відчутним. Основними обмеженнями є:

– технологічне відставання;

– скорочення інвестицій;

– деградація людського капіталу через еміграцію фахівців та їх мобілізацію;

– зростання залежності від обмеженого кола торговельних партнерів.

Ці фактори знижують потенціал економічного зростання та ускладнюють відновлення економіки після війни.

8. *Політичний вимір санкцій.* Санкції мають не лише економічний, а й політичний ефект. Вони підривають легітимність російської влади в очах частини населення, обмежують можливості для зовнішньополітичного маневру та посилюють залежність від авторитарних режимів-партнерів.

Разом з тим, російська пропаганда використовує санкції для мобілізації населення та формування образу “обложеної фортеці”, що частково нівелює внутрішній протестний потенціал.

9. Порівняльний аналіз із попередніми санкційними режимами.

Історичний досвід санкцій проти Ірану, Північної Кореї та Венесуели свідчить, що довготривалі обмеження здатні суттєво підірвати економіку, але не завжди призводять до швидкої зміни політичного курсу. Аналогічна ситуація спостерігається і щодо рф: санкції поступово знижують економічну базу війни, але не гарантують її негайного припинення.

## Дискусія

Отримані результати свідчать, що міжнародна санкційна політика має комплексний та поступово кумулятивний вплив на економіку російської федерації. На відміну від короткострокових очікувань швидкого економічного колапсу, фактичний вплив санкцій проявляється у формі довготривалого структурного послаблення економічного потенціалу держави. Найбільш відчутні наслідки спостерігаються у фінансовій системі, енергетичному секторі та високотехнологічній промисловості. Замороження значної частини міжнародних резервів, обмеження доступу до світових фінансових ринків і відключення частини банків від міжнародних платіжних систем суттєво ускладнили міжнародні фінансові операції та знизили інвестиційну привабливість російської економіки. Водночас переорієнтація експорту енергоносіїв на альтернативні ринки супроводжується зниженням прибутковості та зростанням логістичних витрат, що поступово зменшує доходну базу державного бюджету.

Отримані результати загалом узгоджуються з висновками попередніх досліджень. Зокрема, у роботі [1] зазначається, що санкції сприяють формуванню так званої “економічної тріади” проблем російської економіки – рецесії, інфляції та бюджетного дефіциту. Подібні висновки містяться і в дослідженні [2], які доводять, що санкції не обов’язково призводять до негайної економічної дестабілізації, однак поступово знижують економічний потенціал авторитарних режимів і обмежують їхню здатність фінансувати

довготривалі військові конфлікти. Звіти міжнародних організацій також підтверджують тенденції структурної деградації російської економіки. Зокрема, аналітичні матеріали МВФ та Світового банку [3; 4] вказують на зниження довгострокових темпів економічного зростання, скорочення інвестицій і посилення технологічної залежності від обмеженого кола партнерів.

Разом з тим результати проведеного дослідження уточнюють попередні оцінки, акцентуючи увагу на трансформації структури російської економіки у бік її мілітаризації. Зростання частки оборонних витрат у державному бюджеті, скорочення фінансування соціальних програм та використання резервних фондів свідчать про формування моделі «воєнної економіки», яка дозволяє підтримувати військові дії у короткостроковій перспективі, але водночас поглиблює структурні дисбаланси у довгостроковому періоді.

Водночас дослідження має певні обмеження. По-перше, значна частина офіційної статистичної інформації російської федерації після 2022 року є обмеженою або частково закритою, що ускладнює точну оцінку реального стану економіки. По-друге, деякі економічні показники можуть бути викривлені через адміністративне регулювання, зміну методик розрахунку або політичні фактори. По-третє, результати дослідження базуються переважно на макроекономічних показниках і не повністю враховують регіональні відмінності та галузеві особливості розвитку економіки. Крім того, складність санкційної політики та наявність механізмів обходу обмежень через треті країни можуть частково знижувати реальний ефект санкцій, що також потребує подальшого вивчення.

Таким чином, результати дослідження підтверджують висновки попередніх наукових праць щодо поступового послаблення економічного потенціалу російської федерації під впливом санкцій, водночас підкреслюючи довгостроковий характер цих процесів та їхній структурний вплив на економічну систему держави.

## Висновки

Аналіз впливу міжнародної санкційної політики свідчить, що вона має комплексний і багатовимірний вплив на економіку російської федерації. Санкції призводять до скорочення фінансових ресурсів, до технологічної деградації промисловості, до зростання бюджетних дисбалансів і погіршення соціально-економічної ситуації. У короткостроковій перспективі рф зберігає здатність фінансувати війну, використовуючи накопичені резерви та доходи від експорту енергоносіїв. Проте в середньо- та довгостроковій перспективі санкції істотно обмежують її можливості щодо ведення тривалої війни.

Отже, міжнародні санкції є важливим інструментом стримування агресора, який не дає миттєвого результату, але поступово підточує економічні основи війни. Їх ефективність значною мірою залежить від збереження єдності міжнародної спільноти, посилення контролю за обходом обмежень та поєднання економічного тиску з політичною та військовою підтримкою України.

Предметом подальшого дослідження може бути вивчення соціально-економічних наслідків санкцій для різних груп населення та регіонів російської федерації, а також їх впливу на стійкість внутрішньополітичної системи.

## Список використаних джерел

1. Милов В. Russian Economy's "Unholy Trinity". *Free russia Foundation.* 2022. 2–10. URL: https://thinktank.4freerussia.org/ru/reports/russian-economy-sanctions-august-2024/.
2. Guriev S., Itskhoki O. Sanctions and economic statecraft: Theory and evidence from russia. *Journal of Economic Perspectives.* 2022. № 36 (4). P. 1-26. URL: https://doi.org/10.1257/jep.36.4.3
3. International Monetary Fund. Russian federation: Staff report for the 2023 Article IV consultation. *IMF,* 2023. URL: https://www.elibrary.imf.org.
4. World Bank. Russia economic update: Navigating sanctions and isolation. *World Bank Group.* 2023. URL: https://www.worldbank.org.

5. OECD. The impact of international sanctions on russia's economy. *OECD Publishing*, 2023. URL: https://www.consilium.europa.eu.
6. European Commission. EU sanctions against russia: Economic impact and enforcement. *Publications Office of the European Union*, 2024. URL: https://www.europarl.europa.eu.
7. U.S. Department of the Treasury. Sanctions on russia: Implications for energy markets and military capacity. *Office of Foreign Assets Control (OFAC)*, 2024. URL: https://macmap.org.
8. HICD (Національний інститут стратегічних досліджень). Вплив санкцій на економіку російської федерації. Київ: NISS, 2022. URL: niss.gov.ua.
9. Мальський В. І. Вплив санкційної політики на економічну стабільність: аналіз суспільно-політичних наслідків. *Політичне життя*. 2025. № 1. С. 188-192. URL:jpl.donnu.edu.ua.
10. Орел О., Яцківська А., Власенко О. Економічні санкції ЄС проти росії та ефективність їх застосування. *Society and Security*. 2023. № 1 (1). С. 166-174. URL: sas.ztu.edu.ua.
11. Bank of Russia. Історія ключової ставки. 2025. URL: https://www.cbr.ru/hd_base/keyrate.
12. Ministry of Finance of the russian federation. Federal budget execution reports. *Minfin RF*, 2024. URL: https://www.themoscowtimes.com.
13. Ministry of Finance, KFE Institute. URL: https://mof.gov.ua.

## References

1. Mylov, B. (2022). Russian Economy's "Unholy Trinity". *Free russia Foundation*, 2-10. Retrieved from: https://thinktank.4freerussia.org/ru/reports/russian-economy-sanctions-august-2024/ [in Ukrainian].
2. Guriev, S., & Itskhoki, O. (2022). Sanctions and economic statecraft: Theory and evidence from russia. *Journal of Economic Perspectives*, 36 (4), 1-26. Retrieved from: https://itskhoki.com.
3. International Monetary Fund. (2023). Russian Federation: Staff report for the 2023 Article IV consultation. *IMF*. Retrieved from: https://www.elibrary.imf.org.
4. World Bank. (2023). Russia economic update: Navigating sanctions and isolation. *World Bank Group*. Retrieved from: https://www.worldbank.org.
5. OECD. (2023). The impact of international sanctions on russia's economy. *OECD Publishing*. Retrieved from: https://www.consilium.europa.eu.
6. European Commission. (2024). EU sanctions against russia: Economic impact and enforcement. *Publications Office of the European Union*. Retrieved from: https://www.europarl.europa.eu.
7. U.S. Department of the Treasury. (2024). Sanctions on russia: Implications for energy markets and military capacity. *Office of Foreign Assets Control (OFAC)*. Retrieved from: https://macmap.org.
8. NISD (Natsionalnyi instytut stratehichnykh doslidzhen). Vplyv sanktsii na ekonomiku rosiiskoi federatsii/ NISD (National Institute for Strategic Studies). (2022). The impact of sanctions on the economy of the russian federation. Kyiv: NISS. Retrieved from: https://niss.gov.ua [in Ukrainian].
9. Malsky, V. I. (2025). Vplyv sanktsiinoi polityky na ekonomichnu stabilnist: analiz suspilno-politychnykh naslidkiv. Politychne zhyttia [The impact of sanctions policy on economic stability: analysis of socio-political consequences]. *Political Life*, 1, 188–192. Retrieved from: https://jpl.donnu.edu.ua [in Ukrainian].
10. Orel, O., Orel, O., Yatskevych, A., & Vlasenko, O. (2023). Ekonomichni sanktsii YeS proty rosii ta efektyvnist yikh zastosuvannia [EU economic sanctions against Russia and the effectiveness of their application]. *Society and Security*, 1 (1), 166-174. Retrieved from: https://sas.ztu.edu.ua [in Ukrainian].
11. Bank of russia (2025). Key rate history. Retrieved from: https://www.cbr.ru/hd_base/keyrate [in Ukrainian].
12. Ministry of Finance of the russian federation. (2024). Federal budget execution reports. *Minfin rf*. Retrieved from: https://www.themoscowtimes.com.
13. Ministry of Finance, KFE Institute. Retrieved from: https://mof.gov.ua.

НАУКОВЕ ВИДАННЯ

# MILITARY STRATEGY AND TECHNOLOGY

**НАУКОВО-ПРАКТИЧНИЙ ЖУРНАЛ**

**№ 1 (4) / 2026**



Відповідальний за випуск *І.В. Івженко*

*Ідентифікатор медіа R40-05944 згідно з рішенням Національної ради України з питань телебачення і радіомовлення від 10.04.2025 № 804*

**Засновник і видавець:** Громадська організація "Центр воєнної стратегії і технологій"
**Адреса:** вул. Саксаганського, буд.41, місто Київ, 01033, Україна
**Телефон:** +38 (067) 42-61-105
**E-mail редколегії:** technical.sciences2025@gmail.com