Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2026. № 1. ISSN 2307-2156

DOI: http://doi.org/10.32702/2307-2156.2026.1.11

УДК 351.86:004.056:355/359

М. А. Роговець,

к. т. н., доцент, начальник управління,

Науково-дослідний інститут воєнної розвідки

ORCID ID: https://orcid.org/0000-0002-1587-9017

КОРЕЛЯЦІЯ ДЕРЖАВНОЇ БЕЗПЕКИ ТА НАЦІОНАЛЬНОЇ СТІЙКОСТІ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

M. Rohovets,

PhD in Technical Sciences, Associate Professor, Head of Department at the Defense Intelligence Research Institute

CORRELATION BETWEEN STATE SECURITY AND NATIONAL RESILIENCE UNDER HYBRID THREATS

У статті досліджено взаємозв'язок між державною безпекою та національною стійкістю в умовах гібридних загроз. Обґрунтовано двосторонній характер їхньої кореляції: стійкість зменшує вразливість держави, тоді як ефективна система безпеки гарантує збереження та розвиток ключових елементів стійкості. Запропоновано модель взаємозв'язку, що охоплює інформаційну, інституційну, економічну, кібернетичну та соціогуманітарну сфери, а також систему практичних індикаторів для кількісної оцінки їхнього впливу. Проаналізовано нормативно-правові засади, які формують інтегровану архітектуру безпеки та стійкості,

зокрема Закон України "Про національну безпеку", Доктрину державної безпеки та Доктрину національної стійкості. Результати дослідження підтверджують необхідність комплексного підходу до формування системи протидії гібридним загрозам та окреслюють перспективи подальших наукових розвідок, спрямованих на розробку інтегрованих моделей оцінки, адаптивних сценаріїв реагування та практичних інструментів моніторингу.

The article examines the correlation between state security and national resilience under the conditions of hybrid threats, emphasizing their bidirectional and systemic nature. Resilience reduces the vulnerability of the state to external pressures, while an effective security system ensures the preservation and development of resilience's core elements. The study proposes an integrated model that encompasses five domains – information, institutional, economic, cyber, and socio-humanitarian – each interacting with corresponding spheres of state security. This model is supported by a system of practical indicators designed to provide quantitative assessment of resilience and security effectiveness, including diversification of imports and exports, reserves of critical supplies, levels of media literacy, efficiency of governance, number of repelled cyberattacks, trust in institutions, and social cohesion indices.

The relevance of the research is highlighted by the Russian-Ukrainian war, which represents one of the most explicit examples of hybrid aggression combining military operations with information warfare, economic coercion, cyberattacks, and politico-legal manipulations. Drawing on the works of Hoffman, NATO, RAND Corporation, Chatham House, and leading Ukrainian scholars, the study underscores the necessity of a systemic approach to resilience that integrates institutional reform, strategic communications, enhanced cyber defense, and the strengthening of social unity. The Ukrainian experience demonstrates that hybrid threats exploit internal vulnerabilities such as corruption, social divisions, and dependence of critical infrastructure on external factors, thereby necessitating comprehensive resilience strategies.

The article also analyzes the normative and legal framework of Ukraine, including the Law "On National Security," the Doctrine of State Security, and the Doctrine of National Resilience, which establish the principles of an integrated approach to countering hybrid threats. These documents provide the foundation for

combining military, political, economic, informational, and cyber instruments into a unified architecture of security and resilience.

Methodologically, the research applies scenario analysis, SWOT analysis, matrix models of interdependence, and indicator-based evaluation systems, enabling both qualitative and quantitative assessment of hybrid threats' impact on state functions. The findings confirm that resilience and security form a unified system capable of countering hybrid aggression, where investments in resilience serve as a preventive security strategy and effective security structures guarantee the sustainability of resilience.

The study concludes that further research should focus on developing integrated assessment models, adaptive response scenarios, and monitoring tools that incorporate socio-humanitarian and cultural dimensions. Such approaches will enhance Ukraine's ability to withstand hybrid threats and contribute to the global discourse on resilience and security.

Ключові слова: *державна безпека; національна стійкість; гібридні загрози; інформаційна безпека; нормативно-правові засади; індикатори оцінки.*

Keywords: *state security; national resilience; hybrid threats; information security; normative and legal framework; evaluation indicators*.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Російсько-українська війна є одним із найвиразніших прикладів гібридної агресії, що поєднує воєнні дії з інформаційними, економічними, політико-правовими та кібернетичними інструментами. Як зазначає Ф. Гоффман, гібридна війна – це комбінація регулярних і нерегулярних методів, що створює нові виклики для традиційних систем оборони [1]. Аналітичні центри НАТО [2], RAND Corporation [3] та Chatham House [4] наголошують: ключовим елементом протидії є розвиток національної стійкості, яка забезпечує здатність держави адаптуватися та відновлюватися після криз.

Для України гібридні загрози мають критичне значення, адже агресія спрямована на використання внутрішніх вразливостей – корупції, соціальних

розбіжностей, залежності критичної інфраструктури від зовнішніх чинників. Українські дослідники (Горбулін, Литвиненко [5]; Пирожков та ін. [6]; Погромський [7]) підкреслюють, що війна поєднує військові та невійськові інструменти: дезінформацію, енергетичний шантаж, кібератаки та правові маніпуляції. Це зумовлює потребу у системному підході до стійкості, що включає реформування інституцій, розвиток стратегічних комунікацій та посилення кіберзахисту.

Нормативно-правова база України – Закон «Про національну безпеку» [8], Доктрина державної безпеки [9] та Доктрина національної стійкості [10] – закріплює принципи інтегрованого підходу, який поєднує військові, політичні, економічні та інформаційні інструменти. Водночас бракує систематизації кореляції між рівнем безпеки та показниками стійкості, індикаторів для кількісної оцінки й практичних механізмів інтеграції результатів у стратегічні документи.

Отже, **актуальність проблеми** полягає у необхідності комплексного аналізу взаємозв'язків між безпекою та стійкістю в умовах гібридних загроз і розробці практичних рекомендацій на основі моделей оцінки та адаптивних сценаріїв реагування.

Аналіз останніх досліджень та публікацій. Проблематика гібридних загроз та їхнього впливу на державну безпеку й національну стійкість широко висвітлюється у сучасній літературі. Ф. Гоффман визначає гібридну війну як поєднання регулярних і нерегулярних методів, що створює нові виклики для оборони [1]. Аналітичні центри НАТО [2], RAND Corporation [3] та Chatham House [4] наголошують: ключовим елементом протидії є розвиток національної стійкості, яка забезпечує здатність держави адаптуватися та відновлюватися після криз. У європейських дослідженнях resilience розглядається як стратегічна категорія, що інтегрує економічну, інституційну, інформаційну та соціальну складові й дедалі активніше включається у політику безпеки ЄС та ООН.

Українські науковці (Горбулін, Литвиненко [5]; Пирожков та ін. [6]; Погромський [7]) акцентують на специфіці російсько-української війни, яка поєднує військові та невійськові інструменти агресії: дезінформацію, енергетичний шантаж, кібератаки та правові маніпуляції. Вони підкреслюють необхідність системного підходу до стійкості, що включає реформування інституцій, розвиток стратегічних комунікацій, кіберзахист і формування соціальної єдності.

Важливим джерелом є нормативно-правові акти України: Закон «Про національну безпеку» [8], Доктрина державної безпеки [9] та Доктрина національної стійкості [10], які закріплюють принципи інтегрованого підходу та визначають стратегічні пріоритети.

Методологія досліджень еволюціонувала від описових характеристик до комплексних моделей, що включають сценарний та SWOT-аналіз, матричні моделі й індикаторні системи. Це дозволяє кількісно оцінювати вплив гібридних загроз на ключові сфери функціонування держави. Водночас бракує систематизації кореляції між безпекою та стійкістю, індикаторів для кількісної оцінки й практичних механізмів інтеграції результатів у стратегічні документи.

Формулювання цілей статті (постановка завдання). Метою статті є аналіз взаємозв'язку між державною безпекою та національною стійкістю в умовах гібридних загроз і вироблення практичних рекомендацій для їх інтеграції у стратегічне планування. Завдання полягає у доведенні двостороннього характеру кореляції між безпекою та стійкістю, дослідженні основних сфер прояву гібридних загроз та їхнього впливу на державні інститути, аналізі нормативно-правової бази України як фундаменту інтегрованої системи протидії, а також у розробці моделі взаємозв'язку з практичними індикаторами для кількісної оцінки. Завершальним аспектом є окреслення перспектив подальших досліджень, спрямованих на створення інтегрованих моделей оцінки, адаптивних сценаріїв реагування та інструментів моніторингу.

***Виклад основного матеріалу дослідження*. Теоретико-методологічні засади.** Теоретичне підґрунтя дослідження базується на інтеграції трьох ключових категорій – державної безпеки, національної стійкості та гібридних загроз. Державна безпека охоплює не лише військову складову, а й захист інформаційного простору, критичної інфраструктури, економічної стабільності та інституційної спроможності. Національна стійкість визначається як здатність держави та суспільства виявляти ризики, адаптуватися до них і відновлюватися після криз [10]. Гібридні загрози розглядаються як поєднання військових і невійськових інструментів впливу, спрямованих на дестабілізацію держави без масштабного вторгнення, що підтверджується у працях Ф. Гоффмана [1], а також у дослідженнях НАТО, RAND Corporation та Chatham House [2–4].

Методологічна основа спирається на системний та міждисциплінарний підхід із використанням сценарного аналізу, SWOT-аналізу, матричних моделей та індикаторних систем. Це дозволяє оцінити потенційні наслідки гібридних загроз, визначити сильні й слабкі сторони системи та кількісно виміряти рівень стійкості через показники економічної диверсифікації, медіаграмотності, інституційної спроможності та кіберзахисту. Застосування цих методів відповідає вимогам Закону України “Про національну безпеку” [8] і Доктрини державної безпеки [9], що наголошують на інтегрованому плануванні та доказовій політиці.

Сфери прояву гібридних загроз. Гібридні загрози мають багатовимірний характер і поєднують військові та невійськові інструменти. В інформаційній сфері ключовими є дезінформація, пропаганда та використання технологій “big data” і “deepfake”. Кібернетична сфера охоплює атаки на державні реєстри, фінансові системи та критичну інфраструктуру, зокрема через “кіберпроксі”. В економічній площині проявляються енергетичний шантаж, санкційний тиск і корупційні схеми. Військова та нерегулярна сфера включає проксі-сили, приватні військові компанії (ПВК) та диверсії, що створюють “сірі зони” конфлікту. Політико-правова сфера реалізується через

маніпуляції договорами, міжнародний тиск та “lawfare”. Соціогуманітарна сфера використовує культурні, мовні й релігійні відмінності для провокування внутрішніх конфліктів.

Ці сфери взаємопов’язані та взаємопідсилюють одна одну: інформаційні атаки супроводжуються кібероперaціями, економічний тиск поєднується з політичними маніпуляціями, а нерегулярні військові дії прикривають інші форми агресії. Така багатовимірність вимагає комплексного підходу, що поєднує розвиток державної безпеки та національної стійкості (табл. 1).

Таблиця 1. Огляд сфер прояву гібридних загроз

Сфера загрози	Основні інструменти	Наслідки для держави
Інформаційно-психологічна	Дезінформація, пропаганда, “deepfake”, соцмережі	Підрив довіри до влади, делегітимація інститутів, розкол суспільства
Кібернетична	DDoS-атаки, злам баз даних, кіберпроксі	Порушення роботи критичної інфраструктури, витік даних, економічні збитки
Економічна	Енергетичний шантаж, торговельні обмеження, корупція	Залежність від зовнішніх ринків, фінансова нестабільність, зростання вразливості
Військова/ нерегулярна	Проксі-сили, ПВК, диверсії, “сірі зони”	Дестабілізація прикордонних територій, зниження обороноздатності
Політико-правова	“Lawfare”, маніпуляції договорами, підтримка рухів	Делегітимація державних рішень, міжнародний тиск
Соціогуманітарна	Культурні, мовні та релігійні відмінності	Провокування внутрішніх конфліктів, посилення соціальної напруги

Кореляція державної безпеки та національної стійкості. Взаємозалежність між державною безпекою та національною стійкістю має двосторонній характер і визначає здатність держави протидіяти гібридним загрозам. Стійкість знижує вразливість суспільства та інститутів: економічна диверсифікація мінімізує ризики шантажу, соціальна єдність нейтралізує

дезінформацію, інституційна спроможність блокує корупційні та правові маніпуляції. Таким чином, стійке суспільство та ефективні інститути формують “імунітет” держави до зовнішнього тиску.

Водночас державна безпека гарантує стійкість: діяльність силових структур, правоохоронних органів і системи кіберзахисту забезпечує охорону критичної інфраструктури, правопорядок та захист інформаційного простору. Ефективна безпекова система не лише нейтралізує загрози, а й сприяє розвитку економічної, інституційної та інформаційної стійкості.

Кореляційні зв’язки (табл. 2) можуть бути прямими й оберненими: зростання стійкості підвищує ефективність безпеки, тоді як її зниження збільшує вразливість. Найбільш критичними є інформаційна та інституційна сфери. Для кількісної оцінки взаємозв’язку застосовуються індикатори економічної, інформаційної, інституційної та кіберстійкості – диверсифікація імпорту й експорту, резерви критичних запасів, рівень медіаграмотності, ефективність управління, кількість відбитих кібератак та довіра до інституцій.

Таблиця 2. Кореляція державної безпеки та національної стійкості

Елемент національної стійкості	Відповідна сфера державної безпеки	Взаємозв’язок / ефект взаємодії
Економічна диверсифікація	Економічна безпека	Зменшує ризики зовнішнього шантажу та фінансової дестабілізації
Соціальна єдність	Інформаційна безпека	Знижує ефективність дезінформації та психологічного впливу
Інституційна спроможність	Внутрішня безпека	Унеможливлює використання корупції як інструменту гібридної агресії
Медіаграмотність населення	Стратегічні комунікації	Підвищує стійкість до маніпуляцій, сприяє формуванню критичного мислення
Кіберстійкість	Кібербезпека	Забезпечує захист цифрової інфраструктури, знижує ризики кіберзагроз

Досвід російсько-української війни доводить, що мобілізаційна спроможність суспільства, волонтерські рухи, інформаційна стійкість та міжнародна підтримка є ключовими чинниками державної безпеки. Ефективна діяльність силових структур і системи оборони забезпечує соціальну єдність та розвиток інституційної стійкості.

Кореляція безпеки та стійкості є визначальним чинником протидії гібридним загрозам. Інвестиції у стійкість виступають превентивною стратегією, що гарантує стабільність і здатність держави протистояти зовнішньому втручанню. Індикаторний підхід дозволяє оцінити взаємозв'язок, визначити критичні ризики та інтегрувати результати у стратегічні документи, формуючи комплексну систему захисту й розвитку держави.

Модель взаємозв'язку державної безпеки та національної стійкості. Запропонована модель ґрунтується на інтегрованому підході, що розглядає державну безпеку та національну стійкість як взаємопов'язані елементи системи протидії гібридним загрозам. Її концепція передбачає двосторонню взаємодію: стійкість знижує вразливість держави, а ефективна безпекова система забезпечує розвиток ключових елементів стійкості.

Модель охоплює п'ять сфер: економічну, інформаційну, інституційну, кібернетичну та соціогуманітарну. Економічна диверсифікація мінімізує ризики шантажу, соціальна єдність протидіє дезінформації, інституційна спроможність блокує корупцію, медіаграмотність підвищує критичне мислення, а кіберстійкість захищає цифрову інфраструктуру (табл. 3). Відповідні напрями державної безпеки створюють умови для їхнього розвитку.

Для кількісної оцінки застосовується індикаторний підхід: диверсифікація імпорту й експорту, резерви критичних запасів, рівень медіаграмотності, ефективність управління, кількість відбитих кібератак, довіра до інституцій та соціальна згуртованість. Практична значущість моделі підтверджується досвідом війни, де мобілізаційна спроможність суспільства,

волонтерські рухи та міжнародна підтримка зберегли безпеку, а діяльність силових структур забезпечила єдність і розвиток інституцій.

Таблиця 3. Модель взаємозв'язку державної безпеки та національної стійкості

Сфера безпеки	Елемент стійкості	Ефект взаємодії
Інформаційна безпека	Інформаційна стійкість (медіаграмотність, критичне мислення)	Зменшує ефективність дезінформації, забезпечує легітимність державних інститутів
Внутрішня безпека	Інституційна стійкість (верховенство права, антикорупційні механізми)	Ліквідує внутрішні вразливості, підвищує довіру суспільства до влади
Кібербезпека	Кіберстійкість (захист цифрової інфраструктури)	Забезпечує функціонування критичних систем, підтримує обороноздатність та управління
Економічна безпека	Економічна стійкість (диверсифікація, стратегічні резерви)	Знижує ризики зовнішнього шантажу, стабілізує фінансову систему
Соціогуманітарна безпека	Соціальна стійкість (єдність, культурна інтеграція)	Мінімізує можливості використання внутрішніх протиріч для дестабілізації

Таким чином, інвестиції у стійкість виступають превентивною стратегією безпеки, а ефективна система безпеки гарантує її збереження. Застосування моделі у стратегічному плануванні дозволяє формувати інтегровані сценарії реагування та створювати інструменти моніторингу для довготривалої стабільності держави

Запропонована модель показує, що кожна сфера державної безпеки має відповідний елемент національної стійкості, який підсилює її ефективність у протидії гібридним загрозам. Інформаційна безпека залежить від медіаграмотності суспільства, внутрішня – від інституційної спроможності та боротьби з корупцією, кібербезпека – від захисту цифрової інфраструктури,

економічна – від диверсифікації та стратегічних резервів, соціогуманітарна – від єдності й культурної інтеграції.

Таким чином, державна безпека та національна стійкість формують єдину інтегровану систему, що забезпечує захист від зовнішніх впливів і створює умови для довготривалої стабільності та розвитку держави й суспільства

Практичні індикатори оцінки. Ефективність моделі взаємозв'язку державної безпеки та національної стійкості вимірюється системою практичних індикаторів, що охоплюють економічну, інформаційну, інституційну, кібернетичну та соціогуманітарну сфери. Індикаторний підхід дозволяє кількісно оцінювати рівень стійкості, визначати критичні ризики та інтегрувати результати у стратегічні документи.

Економічні показники відображають диверсифікацію ринків, стратегічні резерви та фінансову стабільність. Інформаційні – рівень медіаграмотності, ефективність комунікацій і захищеність від дезінформації. Інституційні – якість управління, рівень корупції та верховенство права. Кібернетичні – здатність цифрової інфраструктури витримувати атаки, ефективність систем попередження та міжнародної кооперації. Соціогуманітарні – соціальна згуртованість, культурна інтеграція та громадянська активність.

Матриця ризиків (табл. 4) показує, що найбільш критичними залишаються інституційна та кібернетична сфери, тоді як інформаційна та соціогуманітарна стійкість визначають здатність суспільства протидіяти маніпуляціям, а економічна – гарантує незалежність від зовнішнього тиску.

Таким чином, індикаторний підхід формує доказову базу для державної політики, забезпечує системний моніторинг, своєчасне реагування та довготривалу стабільність розвитку держави й суспільства

Таблиця 4. Матриця ризиків: індикатор – рівень впливу – стратегічні заходи

Індикатор	Потенційний рівень впливу	Стратегічні заходи реагування
Індекс диверсифікації імпорту/експорту	Високий ризик при монополізації постачання	Розширення торговельних партнерств, створення стратегічних резервів
Резерви критичних запасів	Середній ризик при недостатніх обсягах	Формування державних резервів, розвиток внутрішнього виробництва
Індекс медіаграмотності населення	Високий ризик при низькому рівні	Освітні програми, стратегічні комунікації, підтримка незалежних медіа
Рівень соціальної довіри	Високий ризик при падінні довіри	Прозорість влади, залучення громадян до прийняття рішень, антикорупційні заходи
Індекс ефективності державного управління	Високий ризик при низькій ефективності	Реформа управління, цифровізація процесів, підвищення професійної компетентності
Рівень корупції	Критичний ризик при високих показниках	Антикорупційні інститути, міжнародний моніторинг, посилення верховенства права
Кількість успішно відбитих кібератак	Високий ризик при низькій здатності до захисту	Інвестиції у кіберзахист, створення центрів реагування на інциденти
Рівень захищеності критичних систем	Критичний ризик при слабкій інфраструктурі	Модернізація цифрових систем, резервні канали управління та зв’язку
Рівень соціальної єдності	Високий ризик при внутрішніх конфліктах	Програми інтеграції, підтримка культурного діалогу, розвиток громадянського суспільства

Нормативно-правові засади. Нормативно-правова база України формує стратегічні засади інтегрованої системи державної безпеки та національної стійкості. Закон “Про національну безпеку” [8] визначає принципи комплексного планування та інтеграції військових і невійськових інструментів. Доктрина державної безпеки [9] окреслює пріоритети протидії гібридним загрозам, тероризму та кібератакам, а Доктрина національної

стійкості [10] формулює засади розвитку економічної диверсифікації, соціальної єдності, інституційної ефективності та кіберзахисту.

Ці документи створюють нормативну основу для практичної реалізації політики безпеки, забезпечують легітимність рішень, координацію між державними інститутами та громадянським суспільством, а також визначають рамки міжнародної співпраці. Українська нормативна база поступово адаптується до стандартів НАТО та ЄС, що сприяє гармонізації політики та посиленню здатності протидіяти гібридним загрозам.

Взаємодія зазначених актів із суміжними документами у сфері оборони, кіберзахисту та інформаційної політики формує цілісну архітектуру безпеки. Вона забезпечує інтеграцію різних інструментів, системний моніторинг і довготривалу стабільність, створюючи правову основу для стійкого розвитку держави й суспільства.

Висновки та перспективи подальших розвідок у даному напрямі. Аналіз показав, що державна безпека та національна стійкість утворюють взаємопов'язану систему, де кожен елемент підсилює інший. Висока стійкість зменшує вразливість до гібридних загроз, а ефективна безпекова система забезпечує розвиток ключових складових стійкості. Запропоновані моделі та індикатори дозволяють кількісно оцінювати взаємозв'язок, визначати критичні ризики та інтегрувати результати у стратегічне планування.

Нормативно-правова база – Закон України "Про національну безпеку", Доктрина державної безпеки та Доктрина національної стійкості – формує фундамент комплексної системи протидії сучасним викликам, інтегруючи військові, політичні, економічні, інформаційні та кібернетичні інструменти.

Перспективи досліджень полягають у створенні інтегрованих моделей оцінки з багатовимірними індикаторами, розробці адаптивних сценаріїв реагування та поглибленні взаємодії з міжнародними ініціативами. Комплексний підхід має стати основою для практичних інструментів моніторингу, прогнозування та стратегічного управління у сфері протидії гібридним загрозам.

Література

1. Hoffman F. Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies, 2007. 98 p.

2. NATO. Resilience and Hybrid Threats: Strategic Concept Papers. Brussels: NATO Publications, 2024. 76 p.

3. RAND Corporation. Countering Hybrid Threats: Lessons for National Security. Santa Monica, CA: RAND Corporation, 2020. 142 p.

4. Chatham House. Resilience in the Age of Hybrid Conflict. London: Chatham House Reports, 2021. 64 p.

5. Горбулін В., Литвиненко О. Гібридна війна: сутність та особливості. Київ: НІСД, 2019. 312 с.

6. Пирожков С. та ін. Національна стійкість України: виклики та перспективи. Київ: Інститут стратегічних досліджень, 2022. 224 с.

7. Погромський О. Інституційна спроможність та державна безпека в умовах гібридних загроз. Київ: Академія державного управління, 2025. 198 с.

8. Закон України «Про національну безпеку України». Відомості Верховної Ради України. 2018. № 31.

9. Доктрина державної безпеки України. Київ: Офіційне видання, 2020. 48 с.

10. Доктрина національної стійкості України. Київ: Офіційне видання, 2021. 52 с.

References

1. Hoffman, F. (2007), Conflict in the 21st century: The rise of hybrid wars, Potomac Institute for Policy Studies, USA.

2. NATO. (2024), Resilience and hybrid threats: Strategic concept papers, NATO Publications, Brussels.

3. RAND Corporation. (2020), Countering hybrid threats: Lessons for national security, : RAND Corporatio,n Santa Monica, USA.

4. Chatham House. (2021), Resilience in the age of hybrid conflict, Chatham House Reports, London, UK.

5. Horbulin, V., & Lytvynenko, O. (2019), *Hibrydna vijna: sutnist' ta osoblyvosti* [Hybrid war: Essence and features], National Institute for Strategic Studies, Kyiv, Ukraine.

6 Pyrozhkov, S., et al. (2022), *Natsional'na stijkist' Ukrainy: vyklyky ta perspektyvy* [National resilience of Ukraine: Challenges and prospects], Institute for Strategic Studies, Kyiv, Ukraine.

7 Pohromskyi, O. (2025), *Instytutsijna spromozhnist' ta derzhavna bezpeka v umovakh hibrydnykh zahroz* [Institutional capacity and state security under hybrid threats], Academy of Public Administration, Kyiv, Ukraine.

8. Verkhovna Rada of Ukraine. (2018), Law of Ukraine “On National Security of Ukraine”, Official Bulletin of the Verkhovna Rada of Ukraine, vol. 31.

9. Cabinet of Ministers of Ukraine. (2020), *Doktryna derzhavnoi bezpeky Ukrainy* [Doctrine of State Security of Ukraine], Official Publication, Kyiv, Ukraine.

10. Cabinet of Ministers of Ukraine. (2021), *Doktryna natsional'noi stijkosti Ukrainy* [Doctrine of National Resilience of Ukraine], Official Publication, Kyiv, Ukraine.

Стаття надійшла до редакції 14.12.2025 р.