УДК 334:338.1:338.2:355/359
JEL Classification: H56; H84; O20

ЗАГРОЗИ РОЗВИТКУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: СУТНІСТЬ І КЛАСИФІКАЦІЯ

©2025 ХАУСТОВА В. Є., ТРУШКІНА Н. В.

УДК 334:338.1:338.2:355/359
JEL Classification: H56; H84; O20

Хаустова В. Є., Трушкіна Н. В.

Загрози розвитку критичної інфраструктури: сутність і класифікація

У статті здійснено комплексне наукове дослідження сутності та класифікації загроз розвитку критичної інфраструктури в умовах трансформації безпекового середовища, зумовленої гібридною війною, цифровізацією і глобальною нестабільністю. Обґрунтовано, що критична інфраструктура є багаторівневою соціо-економіко-технічною системою, від функціонування якої залежать життєздатність держави, сталий розвиток економіки та рівень національної безпеки. Мета статті полягає у теоретичному розкритті природи та структури загроз розвитку критичної інфраструктури, їх систематизації і формуванні науково обґрунтованої класифікації, адаптованої до сучасних безпекових викликів і європейських стандартів резильєнтності. Методологія дослідження ґрунтується на поєднанні системного аналізу, бібліометричного та контент-аналізу, методів класифікації, типологізації, експертного оцінювання, порівняльного аналізу та структурно-логічного узагальнення. Таке поєднання дало змогу глибше виявити взаємозв'язки між типами загроз, чинниками їх ескалації та механізмами впливу на стійкість і керованість інфраструктурних систем. Результати дослідження відображають еволюцію наукових підходів до трактування поняття «загрози розвитку критичної інфраструктури» – від ризик-орієнтованих моделей до інтегрованих концепцій резильєнтності до всіх небезпек (all-hazards resilience). Удосконалено дефініцію цього поняття як сукупності реальних і потенційних чинників природного, техногенного, соціально-економічного, воєнного чи кібернетичного походження, що через уразливості системи можуть порушити її безперервність, цілісність і функціональну керованість. Запропоновано розширену класифікацію загроз, яка охоплює 14 типів – від воєнних, терористичних і кібернетичних до організаційно-кадрових, економічних та екологічних. Розкрито взаємозалежність фізичних, цифрових і когнітивних вимірів загроз та їх каскадний характер. Висновки підтверджують, що сучасне управління критичною інфраструктурою має базуватися на принципах проактивної резильєнтності, інтегрованого ризик-менеджменту та міжсекторальної координації. Серед ключових пріоритетів державної політики безпеки визначено розроблення Національної стратегії розвитку критичної інфраструктури, гармонізованої з вимогами Директив ЄС 2022/2557 (Critical Entities Resilience) і NIS2, створення національної таксономії загроз, а також упровадження стандартів аудиту резильєнтності та системи моніторингу індикаторів стійкості. Практичне значення результатів полягає у можливості використання запропонованих теоретико-методичних положень для удосконалення нормативно-правового регулювання, стратегічного планування та оцінювання ризиків, підвищення рівня кібер-, енергетичної та організаційної стійкості, а також у формуванні наукових засад Національної стратегії резильєнтності критичної інфраструктури України у повоєнний період.

Ключові слова: *критична інфраструктура, об'єкти критичної інфраструктури, розвиток, загрози, ідентифікація, класифікація, систематизація, нормативно-правове регулювання, ризик-менеджмент, національна безпека, кіберзагрози, державна політика безпеки, захист, стійкість, резильєнтність, сталий розвиток.*

DOI: *https://doi.org/10.32983/2222-0712-2025-3-89-104*

Рис.: *1.* ***Табл.****: 6.* ***Бібл.:*** *41.*

Хаустова Вікторія Євгенівна *– доктор економічних наук, професор, директор Науково-дослідного центру індустріальних проблем розвитку НАН України (пров. Інженерний, 1а, 2 пов., Харків, 61166, Україна)*

E-mail: *v.khaust@gmail.com*

ORCID: *https://orcid.org/0000-0002-5895-9287*

Researcher ID: *https://www.webofscience.com/wos/author/record/629132*

Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57216123094*

Трушкіна Наталія Валеріївна *– кандидат економічних наук, старший дослідник, старший науковий співробітник сектора промислової політики та інноваційного розвитку відділу промислової політики та енергетичної безпеки, Науково-дослідний центр індустріальних проблем розвитку НАН України (пров. Інженерний, 1а, 2 пов., Харків, 61166, Україна)*

E-mail: *trushkina@nas.gov.ua*

ORCID: *https://orcid.org/0000-0002-6741-7738*

Researcher ID: *https://www.webofscience.com/wos/author/record/894686*

Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57210808778*

UDC 334:338.1:338.2:355/359
JEL Classification: H56; H84; O20

Khaustova V. Ye., Trushkina N. V. Threats to the Development of Critical Infrastructure: Essence and Classification

The article presents a comprehensive scientific study of the essence and classification of threats to the development of critical infrastructure in the context of the transformation of the security environment, driven by hybrid warfare, digitalization, and global instability. It is substantiated that critical infrastructure is a multi-level socioeconomic and technical system on which the State's viability, sustainable economic development, and national security depend. The aim of the article is to theoretically unveil the nature and structure of threats to the development of critical infrastructure, to systematize them, and to create a scientifically grounded classification adapted to modern security challenges and European resilience standards. The research methodology is based on a combination of systems analysis, bibliometric and content analysis, classification and typology methods, expert evaluation, comparative analysis, and structural-logical generalization. This combination allowed for a deeper identification of the interconnections between threat types, factors of their escalation, and the mechanisms influencing the resilience and controllability of infrastructure systems. The research results reflect the evolution of scientific approaches to interpreting the concept of «critical infrastructure development threats» – from risk-oriented models to integrated all-hazards resilience conceptions. The definition of this concept has been refined as the set of actual and potential factors of natural, technological, socioeconomic, military, or cyber origin, which, through system vulnerabilities, can disrupt its continuity, integrity, and functional controllability. An expanded classification of threats has been proposed, covering 14 types – from military, terrorist, and cyber threats to organizational, personnel, economic, and environmental ones. The interdependence of the physical, digital, and cognitive dimensions of threats and their cascading nature has been revealed. The conclusions confirm that modern management of critical infrastructure should be based on the principles of proactive resilience, integrated risk management, and cross-sectoral coordination. Among the key priorities of State security policy are the development of a National Strategy for Critical Infrastructure Development, aligned with the requirements of EU Directives 2022/2557 (Critical Entities Resilience) and NIS2, the creation of a national threat taxonomy, as well as the implementation of resilience audit standards and a system for monitoring resilience indicators. The practical significance of these results lies in the possibility of using the proposed theoretical and methodological provisions to improve legal and regulatory frameworks, strategic planning, and risk assessment, enhance cyber, energy, and organizational resilience, and establish the scientific foundations of Ukraine's National Critical Infrastructure Resilience Strategy in the post-war period.

Keywords: *critical infrastructure, critical infrastructure facilities, development, threats, identification, classification, systematization, regulatory framework, risk management, national security, cyber threats, State security policy, protection, endurance, resilience, sustainable development.*

Fig.: *1.* ***Tabl.****: 6.* ***Bibl.****: 41.*

Khaustova Viktoriia Ye. *– Doctor of Sciences (Economics), Professor, Director of the Research Centre for Industrial Problems of Development of NAS of Ukraine (2 floor 1a Inzhenernyi Ln., Kharkiv, 61166, Ukraine)*

E-mail: *v.khaust@gmail.com*

ORCID: *https://orcid.org/0000-0002-5895-9287*

Researcher ID: *https://www.webofscience.com/wos/author/record/629132*

Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57216123094*

Trushkina Nataliia V. *– Candidate of Sciences (Economics), Senior Researcher, Senior Research Fellow of the Sector of Industrial Policy and Innovative Development of the Department of Industrial Policy and Energy Security, Research Centre for Industrial Problems of Development of NAS of Ukraine (2 floor 1a Inzhenernyi Ln., Kharkiv, 61166, Ukraine)*

E-mail: *trushkina@nas.gov.ua*

ORCID: *https://orcid.org/0000-0002-6741-7738*

Researcher ID: *https://www.webofscience.com/wos/author/record/894686*

Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57210808778*

Вступ. У сучасних умовах глобальної нестабільності питання розвитку та безпеки критичної інфраструктури набувають особливого значення. Критично важливі об'єкти все частіше зазнають впливу різнопланових загроз [1], що зумовлюються природними катаклізмами, екологічними та техногенними катастрофами, терористичними актами, кіберінцидентами та військовими конфліктами. Від рівня стійкості та резильєнтності [2] таких систем безпосередньо залежить не лише національна безпека [3; 4], а й функціонування економіки, соціальної сфери та життєзабезпечення населення.

Для України проблема забезпечення стійкості критичної інфраструктури набула виняткового значення у зв'язку з триваючою збройною агресією російської федерації та масштабними безпековими ризиками. Відповідно до Стратегії національної безпеки України (Указ Президента України від 14.09.2020 № 392/2020) [5] одним із ключових напрямів державної політики визначено створення ефективної системи безпеки та стійкості критичної інфраструктури на засадах чіткого розподілу відповідальності між суб'єктами управління і розвитку державно-приватного партнерства. Концепція забезпечення національної системи стійкості (Указ Президента України від 27.09.2021 № 479/2021) [6] передбачає інтегроване управління ризиками та забезпечення захищеності об'єктів критичної інфраструктури як складової загальнонаціональної безпекової архітектури.

Однак, попри наявність стратегічних документів, реальний стан функціонування об'єктів критичної інфраструктури залишається вкрай уразливим. За оцінками Київської школи економіки (KSE) [7], загальна сума прямих задокументованих збитків від руйнувань житлової, промислової та транспортної інфраструктури з початку повномасштабного вторгнення росії сягнула майже 170 млрд дол. США (станом на листопад 2024 р.), що на 8,1 % більше порівняно з квітнем 2024 р. Найбільших втрат за-

знали житловий сектор (60 млрд дол., або 35,3% загального обсягу збитків) та транспортна інфраструктура (38,5 млрд дол., або 22,7%). Значними є також збитки енергетичної галузі (14,6 млрд дол., або 8,6%), промисловості (14,4 млрд дол., або 8,5%) та аграрного сектора (10,3 млрд дол., або 6,1%) [8].

За оцінками Світового банку (RDNA3) [9], у 2024–2034 роках на відбудову інфраструктури України необхідно понад 486 млрд дол., що утричі перевищує обсяг зафіксованих збитків. Найбільше інвестицій потребуватимуть житловий сектор (82,6 млрд дол., або 17% загального обсягу фінансування); транспортна інфраструктура (72,9 млрд дол., або 15%); агропромисловий комплекс (58,3 млрд дол., або 12%); енергетична інфраструктура (48,6 млрд дол., або 10% загального обсягу інвестицій) [10].

В оновленій оцінці RDNA4 [11] загальні потреби у відновленні та реконструкції зросли до 524 млрд дол., що у 2,8 разу перевищує прогнозований номінальний ВВП України на 2024 рік. Найбільш капіталомісткими потребами на відбудову та відновлення залишаються відбудова житла (84 млрд дол., або 16%), транспортна інфраструктура (78 млрд дол., або 15%), енергетика (68 млрд дол., або 13%), промисловість і торгівля (64 млрд дол., або 12%) та агросектор (55 млрд дол., або 10%) [12].

У контексті гібридної війни дедалі більшої ваги набувають кіберзагрози [13], які можуть спричинити наслідки, зіставні або навіть гірші за фізичні атаки. Зловмисні втручання у цифрові системи управління можуть призвести до дестабілізації енергетичних систем, блокування комунікацій, зупинки транспортних і фінансових операцій, витоку стратегічно важливих даних і підриву довіри до державних інституцій.

Попри зростання обізнаності щодо кіберризиків, рівень готовності більшості операторів критичної інфраструктури залишається недостатнім. За результатами дослідження [14], у 2024 році приблизно 70 % українських компаній не інвестували у кібербезпеку, що підвищує вразливість національних інфраструктурних систем. Особливу небезпеку становлять атаки на ланцюги постачання, зокрема на ІТ-компанії, які забезпечують цифрову підтримку операційної діяльності критичних секторів.

Таким чином, забезпечення стійкості критичної інфраструктури постає як стратегічне завдання економічної та національної безпеки України. Розвиток цієї сфери потребує не лише модернізації технічних потужностей і залучення інвестицій, а й формування комплексної системи резильєнтності, здатної протистояти широкому спектру загроз – від природних і техногенних до військових та кібернетичних. Порушення функціонування таких систем спричиняє каскадні ефекти, що відображаються на регіональному, національному та глобальному рівнях.

Тому актуальним завданням є теоретико-методологічне обґрунтування розвитку критичної інфраструктури в умовах зовнішніх загроз і розроблення дієвих механізмів забезпечення її стійкості й адаптивності.

Аналіз останніх досліджень і публікацій. Бібліометричний пошук у базі Scopus за запитом «загроза або загрози» та «критична інфраструктура» (“Threat or threats” and “Critical infrastructure”) показав, що тематика загроз розвитку критичній інфраструктурі залишається однією з найдинамічніших у сфері безпеки та сталого розвитку. За період 1974–2025 рр. ідентифіковано 8306 публікацій, з яких 3145 – наукові статті. Починаючи з 2018 року спостерігається стрімке зростання кількості робіт: якщо у 2018 р. опубліковано 352 статті, то у 2025 р. – вже 1603, що свідчить про формування нового дослідницького піку. Темп щорічного зростання кількості публікацій становить за 2000–2025 рр. 21,2 %. Така динаміка прямо корелює із зростанням гібридних загроз, кібератак, кліматичних ризиків і військових конфліктів, які комплексно впливають на системи життєзабезпечення.

Як свідчить аналіз, на ранніх етапах (до 2010 р.) наукові розвідки мали переважно описовий характер – акцентувались на класифікації загроз і підходах до ідентифікації критично важливих об’єктів. Однією з базових праць стала робота H. Luiijf, A. Nieuwenhuijs [15], де розроблено розширювану таксономію загроз для критичної інфраструктури в межах проєкту VITA, що заклала основу європейської системи категоризації ризиків.

Починаючи з 2015–2019 рр. фокус досліджень зміститься у бік кібербезпеки. Публікації Z. Chen et al. [16] і H. Kure, S. Islam [17] доводять необхідність розвитку систем моніторингу загроз на базі хмарних обчислень і інтеграції кіберрозвідки у процеси управління ризиками. Водночас зростає кількість робіт, присвячених людському фактору (I. Ghafir et al. [18]), що підкреслює важливість соціо-технічного підходу до безпеки критичної інфраструктури. Період 2020–2025 рр. характеризується міждисциплінарністю та розвитком концепції резильєнтності. Статті E. Wells et al. [19] та A. Jovanović et al. [20] демонструють перехід до моделювання резильєнтності критичної інфраструктури за умов каскадних загроз, включаючи пандемії, кліматичні події та військові дії. Новим трендом є розроблення індексів оцінювання резильєнтності (CIRIX), а також використання мережевих методів і сценарного аналізу для прогнозування наслідків екстремальних загроз.

Аналіз наукових праць провідних зарубіжних вчених (Z. Chen et al. [16]; A. Djenna et al. [21]; K. Geppert, J. Konieczny [22]; I. Ghafir et al. [18]; A. Jovanović et al. [20]; H. Kure & S. Islam [17]; H. Luiijf & A. Nieuwenhuijs [15]; S. Mehdiyev & M. Hashimov [23]; E. Wells [19]) показує, що ядро досліджень формують такі ключові слова: «критична інфраструктура», «загроза», «кіберзагроза», «кібербезпека», «оцінка ризиків», «стійкість», «резильєнтність», «Інтернет речей (IoT)», «кібератаки», «ризик-менеджмент» тощо (*табл. 1*). Це свідчить про злиття технічної, інформаційної та управлінської парадигм у дослідженнях безпеки.

Слід зазначити, що підвищену увагу науковців і фахівців-практиків приділено кіберфізичним системам (CPS), SCADA-мережам, розумним енергетичним системам (Smart Grid), а також штучному інтелекту, машинному та глибокому навчанню, що використовуються для моніторингу та прогнозування загроз. Дослідження A. Djenna et al. [21] підкреслюють ризики IoT-інфраструктур, тоді як S. Mehdiyev & M. Hashimov [23] демонструють галузевий приклад у нафтогазовому секторі, зосереджений на вразливості виробничих систем до кібератак.

Таблиця 1

Ключові слова, які зустрічаються у наукових публікаціях, що входять до міжнародної наукометричної бази даних Scopus

Ключове слово	Джерело								
	Z. Chen et al.	A. Djenna et al.	K. Geppert et al.	I. Ghafir et al.	A. Jovanović et al.	H. Kure et al.	H. Luiijf et al.	S. Mehdiyev et al.	E. Wells et al.
Критична інфраструктура	+	+	+	+	+	+	+	+	+
Системи критичної інфраструктури	+								
Захист							+		
Безпека	+		+	+					
Ризик							+		
Загроза			+	+			+	+	+
Небезпека									+
Вразливість								+	
Тероризм							+		
Кіберзагрози				+				+	
Кібератака		+						+	
Людський фактор				+			+		
Таксономія							+		
Виявлення загроз	+								
Моніторинг мережі	+								
Хмарні обчислення	+								
Інтернет речей		+							
Екстремальні загрози					+				
Резильєнтність					+				+
Показники резильєнтності					+				
Каскадування									+
Кібербезпека		+		+		+		+	
Розвідка кіберзагроз						+			
Контроль безпеки						+			
Ризик-менеджмент						+			
Міська агломерація			+						

Джерело: складено авторами на основі джерел [15–23]

На сучасному етапі відбувається зміщення від реагування на інциденти до проактивного управління загрозами, підкріпленого штучним інтелектом, аналітикою великих даних і прогнозними моделями. Зростає роль індикаторів резильєнтності, які дозволяють оцінювати вразливість регіональних систем (наприклад, у роботі A. Jovanović et al. [20]). Крім того, актуальним стає врахування екологічних і кліматичних факторів, що розширює поняття загрози до інтегрованого підходу, який враховує всі небезпеки (“all-hazards approach”).

Отже, у сучасних дослідженнях фокус зміщується від класифікацій загроз до моделей резильєнтності, що враховують взаємозалежність соціальних, економічних і технічних підсистем. Як свідчить аналіз літературних джерел, наукові роботи охоплюють теми ризик-менеджменту, кіберзахисту, енергетичної та цифрової безпеки, управління кризами, сталого відновлення інфраструктури у воєнних і поствоєнних умовах.

На підставі результатів бібліометричного аналізу побудовано мережеву карту взаємозв’язку між ключовими словами «загроза або загрози», «критична інфраструктура», «розвиток критичної інфраструктури» (*рис. 1*).

Візуалізація демонструє п’ять основних тематичних кластерів досліджень, які відображають еволюцію наукових підходів до проблеми загроз розвитку критичної інфраструктури. Карта демонструє високу взаємозалежність

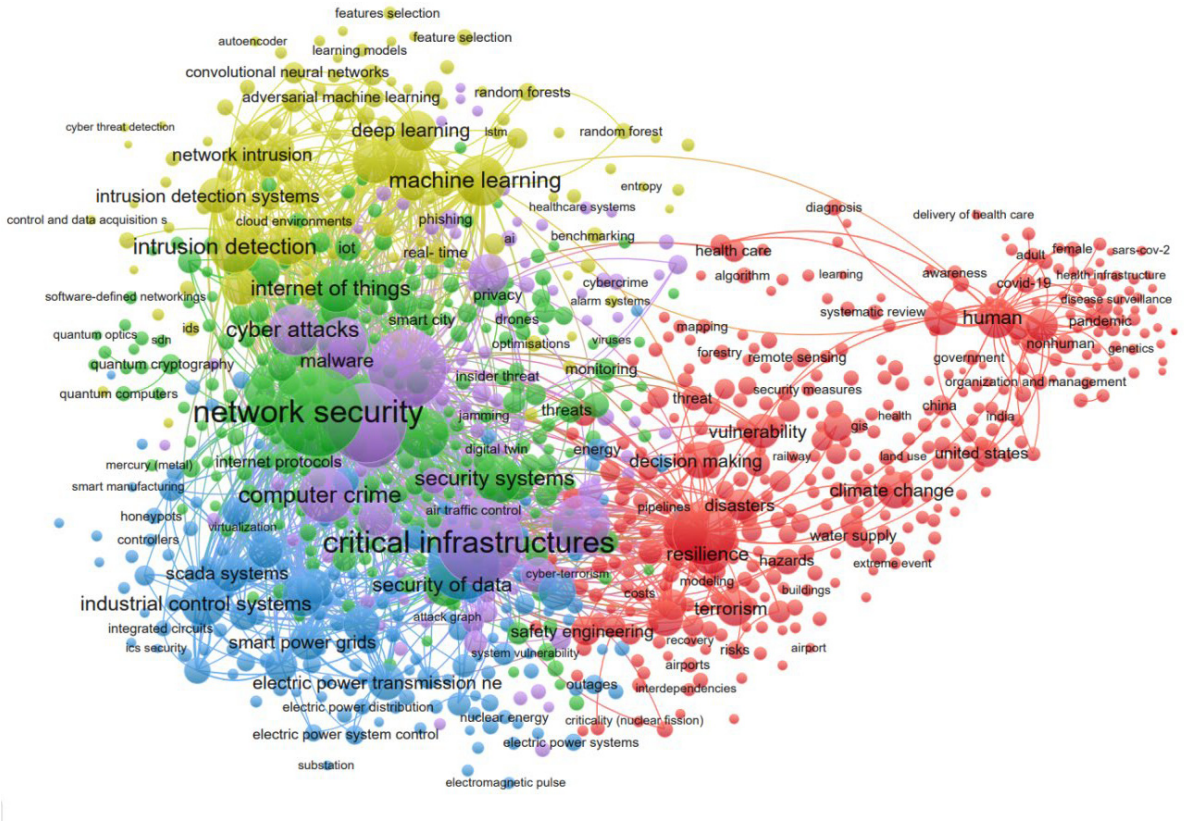

Рис. 1. Мережева карта ключових слів за темою «Загрози розвитку критичної інфраструктури»

Джерело: побудовано авторами за даними бази Scopus (1974–2025 рр.) із використанням програмного забезпечення VOSviewer

між технічними, управлінськими та соціальними аспектами безпеки, що засвідчує формування комплексної міждисциплінарної парадигми «резильєнтні та безпечні інфраструктурні системи».

Як видно з *рис. 1*, кластер 1 (синій) – це технічна безпека енергетичних і промислових систем. Тематика охоплює проблеми фізичної безпеки, управління технологічними процесами та надійності енергетичних, транспортних і виробничих систем. Дослідження зосереджено на захисті промислових мереж, моделюванні відмов і резильєнтності енергосистем, що особливо актуально у контексті декарбонізації та переходу до Smart Grid-архітектури.

Кластер 2 (фіолетовий) – кібербезпека та захист мереж. Основна увага приділяється виявленню вторгнень, моніторингу мережевого трафіку та створенню систем реагування на кіберінциденти. Визначальними є публікації, які поєднують розвідку кіберзагроз (CTI) із управлінням ризиками (CSRM) (H. Kure & S. Islam [17]), а також застосування хмарних технологій для моніторингу (Z. Chen et al. [16]). У кластері 3 (зелений) – штучний інтелект і машинне навчання – дослідження спрямовано на використання інтелектуальних алгоритмів для виявлення аномалій, ідентифікації вторгнень, оптимізації ризик-аналізу. Напрацювання у цьому кластері забезпечують технічну основу для автоматизованого реагування на загрози в режимі реального часу, що робить його динамічним сегментом досліджень 2020-х років.

Ключовим аспектом у кластері 4 (червоний) – це людський фактор, соціальні й кліматичні загрози. Цей кластер репрезентує зсув від технократичних до соціо-екологічних підходів, де розглядаються поведінкові, управлінські та організаційні аспекти безпеки, а також вплив пандемій, кліматичних екстремумів і терористичних актів на функціонування критичної інфраструктури. Значну кількість робіт пов'язано із моделюванням каскадних загроз (A. Jovanović et al. [20]; E. Wells [19]).

Кластер 5 (жовтий) включає публікації, які присвячено застосуванню аналітичних моделей та інноваційних технологій. Цей сегмент досліджень фокусується на моделюванні ризиків, оцінюванні резильєнтності систем, захисті персональних даних і впровадженні цифрових інновацій у контексті управління безпекою критичної інфраструктури.

Таким чином, еволюційна динаміка наукових підходів у зарубіжних джерелах засвідчує поступовий перехід від класифікацій загроз, характерних для 2000-х років, до інтегрованих моделей резильєнтності, що формуються у 2020-х роках. У межах цих моделей критична інфраструктура розглядається як складна соціо-економіко-технічна система, що вкрай вразлива до дії мультифакторних ризиків.

У науковому дискурсі (Д. Бобро [24], О. Герасименко [25], О. Єрменчук [26-27], С. Іванюта та ін. [28; 29], А. Магомедов [30], Д. Мельник [31], Р. Мурасов, Я. Мельник [32], А. Невольніченко та ін. [33], А. Помаза-Пономаренко [34], М. Чеховська, О. Лісовська [35]) щодо загроз і захисту кри-

тичної інфраструктури України простежується чітка еволюція від концептуально-методологічних підходів і правових засад до прикладних моделей оцінювання ризиків і формування проактивних механізмів резильєнтності. Ранні праці українських науковців окреслили ризик-орієнтовану рамку та необхідність системного державного підходу до критичної інфраструктури. У той час як сучасні дослідження, які зумовлені повномасштабною російською збройною агресією, деталізують класифікації загроз, інструменти оцінювання та інтеграцію каскадних ефектів і відновлення.

Наприклад, у праці Д. Бобро [24] сформульовано логіку ризик-менеджменту критичної інфраструктури як добутку частоти реалізації загрози, вразливості та нормованих наслідків, з виокремленням «зони неприйнятного ризику» і пріоритезації об'єктів за критичністю наслідків (підхід all-hazards, акцент на комбінованих загрозах і каскадних ефектах). Автор пропонує чіткий поділ об'єктів за групами захисту/відновлення, що фактично операціоналізує принцип 80/20 для державної політики у ресурсно обмежених умовах [24]. Подібний системно-ризиковий підхід відтворюється в аналітичній записці С. Іванюти [28], де обґрунтовано потребу моніторингу реалізації стратегії національної безпеки через призму загроз критичній інфраструктурі та підсилення координаційних механізмів [28]. Монографічне видання вченого О. Єрменчука розширює основу, пропонуючи науково-методичні засади формування національної системи захисту критичної інфраструктури (терміни, інституційні ролі, принципи побудови системи та інтеграцію безпеки й стійкості) [27].

Значна частина наукових робіт синтезує законодавчі вимоги та стратегічні документи, фіксуючи прогалини у визначенні дефініцій «загроза об'єкту критичної інфраструктури» та відсутність уніфікованого переліку загроз на рівні актів прямої дії. Останні огляди підкреслюють потребу гармонізації з європейськими підходами до резильєнтності критичних суб'єктів і системного врахування гібридних впливів [26; 35]. Порівняльні висновки підтверджують, що без формалізації єдиної таксономії загроз і критеріїв віднесення до критичної інфраструктури неможливо забезпечити узгоджене планування й нагляд.

Як показує теоретичний аналіз, у вітчизняних публікаціях для інтеграції багатофакторних невизначеностей у війні та кіберпросторі (коли історична частота подій не є інформативною) використовуються експертно-оцінні підходи (Delphi/шкальні методики, FAIR-логіка). Так, низкою авторів показано, що агреговані експертні оцінки досягають задовільної надійності, особливо при багатоетапній процедурі [24; 32]. Моделювання системної динаміки застосовується для картування причинно-наслідкових петель, затримок і «накопичувачів» ризику на об'єктах критичної інфраструктури та суміжних системах. Це дозволяє тестувати сценарії надзвичайних ситуацій і втручань без ризику для об'єктів реальної інфраструктури [33].

Крім цього, варто зазначити, що поряд із класичною тріадою (природні, техногенні, зловмисні дії) у воєнних умовах акцент зміщується до комбінованих сценаріїв, що синхронізують ракетно-дронові удари, кібератаки, диверсії, інформаційно-психологічні впливи і деструкції ланцюгів постачання. Узагальнені результати експертного оцінювання виділяють пріоритетні загрози: ракетно-дронові атаки, кібератаки, аварії суміжних об'єктів, технічна зношеність і перевантаження, дефіцити електроживлення/паливних резервів, кадрові втрати, слабке стратегічне планування та координація [25; 30; 31; 32]. Низка праць структурує загрози за сферами (воєнна, інформаційна, політична, економічна, науково-технологічна, екологічна), що полегшує міжвідомче планування й матричне закріплення відповідальності [26; 31; 36].

Останні напрацювання наголошують на переході від реактивного управління безпекою до проактивної резильєнтності – завчасного виявлення слабких місць, регулярного оцінювання загроз, шифрування залежностей, сек'юритизації ланцюгів постачання, координації держави та приватних операторів, підготовки сценарних планів відновлення (альтернативні маршрути, резервування, модульність систем) [27; 35]. Такий підхід підсилює здатність критичної інфраструктури не лише витримати вплив, а й швидко відновити критичні функції за умов триваючої агресії.

Однак на цей момент невирішеними залишилися питання, які потребують подальших напрацювань. До них можна віднести: відсутність єдиної національної таксономії загроз із прив'язкою до вимірюваних індикаторів стійкості/відновлення (включно з кіберфізичними перетинами та ланцюгами постачання); обмежена кількісна верифікація експертних оцінок в умовах воєнної невизначеності; недостатнє моделювання міжсекторних каскадів та ефектів «доміно» (енергетика – транспорт – цифрова інфраструктура); брак стандартизованих метрик резильєнтності (час відновлення, глибина втрати функцій, еластичність до шоків) у форматі, придатному для порівняння між операторами й регіонами; обмежена інтеграція проактивних сценаріїв (випереджувальне ремонтування, «security-by-design», кібер-stress-tests, чорні/сірі лебеді) у типові програми забезпечення безпеки.

Таким чином, сучасний масив публікацій демонструє зрілу еволюцію від номінативного опису загроз до конструкції ризик-орієнтованої, проактивної та резильєнтної моделі захисту критичної інфраструктури України. Методологічні рішення (Delphi/FAIR-логіка, системна динаміка) дозволяють працювати з невизначеністю, проте потребують стандартизації шкал. Правові та організаційні рамки вимагають подальшого наповнення уніфікованою таксономією загроз, які мають вимірюватися індикаторами резильєнтності й міжвідомчими процедурами координації, особливо з урахуванням гібридних сценаріїв і каскадних ефектів.

З огляду на зазначене, **мета цієї статті** полягає у теоретичному обґрунтуванні сутності загроз розвитку критичної інфраструктури та формуванні їх науково обґрунтованої класифікації з урахуванням сучасних безпекових викликів, що постають перед Україною в умовах воєнної агресії та глобальної нестабільності.

Для досягнення поставленої мети використано комплекс взаємопов'язаних методів наукового дослідження, серед яких: метод системного аналізу, бібліометричного аналізу, контент-аналізу, експертного опитування, класифікації та типологізації, структурно-логічного узагальнення.

Сукупне застосування зазначених методів дозволило забезпечити комплексне бачення сутності загроз критичній інфраструктурі та обґрунтувати напрями підвищення її резильєнтності в умовах сучасних гібридних викликів.

Викладення основного матеріалу дослідження. Аналіз чинної законодавчої та нормативно-правової бази (Закон України від 16.11.2021 р. № 1882-IX «Про критичну інфраструктуру» (із змінами, у редакції від 21.09.2024 р.) [37]; Стратегія національної безпеки України, затверджена Указом Президента України від 14.09.2020 р. № 392/2020 (із змінами, у редакції від 07.01.2025 р.) [5]; Стратегія енергетичної безпеки, схвалена Розпорядженням Кабінету Міністрів України від 04.08.2021 р. № 907-р [38]; Стратегія економічної безпеки України, затверджена Указом Президента України від 11.08.2021 р. № 347/2021 [39]; Постанова Кабінету Міністрів України від 01.04.2025 р. № 367 «Про затвердження вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності» [40]) свідчить, що вона створює основу захисту критичної інфраструктури, однак не формує повноцінного механізму її розвитку, адаптації та резильєнтності. До ключових загроз розвитку критичної інфраструктури відносяться такі, як погіршення технічного стану, відсутність інвестицій, кібер- і фізичні ризики, законодавча фрагментарність, тимчасова окупація частини території України.

Так, у Законі України від 16.11.2021 р. № 1882-IX «Про критичну інфраструктуру» (із змінами, у редакції від 21.09.2024 р.) [37] наведено поняття «кризова ситуація», «інцидент безпеки критичної інфраструктури», «несанкціоноване втручання». Під кризовою ситуацією розглядається порушення або загроза порушення штатного режиму функціонування критичної інфраструктури чи окремого її об'єкта, реагування на яке потребує залучення додаткових сил і ресурсів [37]. Поняття «інцидент безпеки критичної інфраструктури» визначається як подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактору) та/або таких, що мають ознаки несанкціонованого втручання у функціонування об'єкта критичної інфраструктури, які становлять загрозу його безпеці, системі управління технологічними процесами об'єкта критичної інфраструктури, створюють ймовірність порушення штатного режиму функціонування такого об'єкта (у тому числі зриву та/або блокування роботи, та/або несанкціонованого управління його ресурсами), ставлять під загрозу його захищеність [37].

Під терміном «несанкціоноване втручання» у законодавчому документі розуміються незаконні дії, що створили загрозу безпечному функціонуванню об'єкта критичної інфраструктури та призвели до одного або декількох з таких наслідків: порушили його безперервність і стійкість; створили реальні чи потенційні загрози для населення, суспільства, соціально-економічного стану, національної безпеки і оборони України [37].

Як зазначено у Постанові Кабінету Міністрів України від 01.04.2025 р. № 367 «Про затвердження вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності» [39], ризик безпеки на об'єктах критичної інфраструктури – це можливість виникнення інциденту безпеки критичної інфраструктури/порушення стану захищеності критичної інфраструктури, що становить загрозу для забезпечення функціональності, безперервності роботи, відновлюваності, цілісності та стійкості об'єктів критичної інфраструктури. До основних ризиків безпеки віднесено: матеріальні ризики, ризики кібербезпеки та захисту інформації, ризики людського фактору, ризики порушення взаємозв'язків, ризики, пов'язані з процесами [39].

У Стратегії енергетичної безпеки, що схвалена Розпорядженням Кабінету Міністрів України від 04.08.2021 р. № 907-р [38], вживаються такі терміни, як «загрози енергетичній безпеці», «ризики у сфері енергетичної безпеки», «кризова ситуація в енергетиці» тощо. Серед загроз енергетичній безпеці варто вказати ті, які негативно впливають на розвиток критичної (енергетичної) інфраструктури, а саме: кіберзагрози/кіберінциденти щодо об'єктів критичної інфраструктури енергетичного сектора; зростання зношеності основних фондів об'єктів енергетичної інфраструктури; загрози фізичній безпеці об'єктів енергетичної інфраструктури; триваюча збройна агресія росії проти України, яка перешкоджає сталій роботі енергетичних активів суб'єктів господарювання енергетичних ринків [38].

Як відмічено у Стратегії економічної безпеки України, затвердженою Указом Президента України від 11.08.2021 р. № 347/2021 [39], основними викликами та загрозами у сфері виробничої безпеки є незадовільний технічний стан і рівень захисту об'єктів критичної інфраструктури; недостатність інвестицій в її оновлення та розвиток; потенційна загроза несанкціонованих втручань фізичного і кіберхарактеру в її функціонування тощо. Про ці ж загрози йдеться і в Стратегії національної безпеки України, затвердженою Указом Президента України від 14.09.2020 р. № 392/2020 (із змінами) [39].

Узагальнюючи результати аналізу законодавчих і нормативно-правових документів, слід зазначити, що чинні акти формують базову національну систему захисту критичної інфраструктури в Україні (*табл. 2*).

Однак, як видно з *табл. 2*, структура нормативно-правових документів залишається фрагментованою та орієнтованою переважно на реагування на загрози, а не на їх попередження або забезпечення резильєнтності. Відсутність єдиного стратегічного документа, який би визначав довгострокові пріоритети розвитку критичної інфраструктури, створює ризик неузгодженості між секторами та обмежує ефективність державної політики. Необхідним є перехід до моделі проактивного управління резильєнтністю з урахуванням вимог директив ЄС (зокрема, 2022/2557 та NIS2), тобто зміщення акценту з «реактивного захисту» ("reactive protection") на «проактивну резильєнтність і сталий розвиток» "proactive resilience and sustainable development" – із чіткою інтеграцією економічних, енергетичних та безпекових політик. Це, своєю чергою, дозволить забезпечити сталий розвиток, інтеграцію у європейський простір і зміцнення національної безпеки України.

Тепер проаналізуємо трактування поняття «загрози критичній інфраструктурі» або «загрози розвитку критичної інфраструктури», які наведено у наукових працях українських вчених (*табл. 3*).

Таблиця 2

Аналіз нормативно-правової бази стосовно визначення загроз розвитку критичної інфраструктури

Назва документа	Ключові положення	Виявлені недоліки	Рекомендації щодо вдосконалення
Закон України «Про критичну інфраструктуру» [36]	Визначає базові поняття, структуру національної системи захисту критичної інфраструктури, процедури ідентифікації, категоризації, створення паспортів безпеки та проєктних загроз	Фокус на захисті, а не розвитку; відсутність фінансових стимулів; фрагментарність ризикового підходу; слабка інтеграція кібер- та фізичної безпеки	Доповнити положеннями щодо сталого розвитку, модернізації та фінансування критичної інфраструктури; запровадити ризик-орієнтовану модель управління відповідно до директиви ЄС 2022/2557
Стратегія національної безпеки України [5]	Визначає основні напрями національної безпеки, підкреслює погіршення технічного стану критичної інфраструктури, кіберзагрози, брак інвестицій	Відсутність механізмів усунення загроз; немає індикаторів ризиків і моніторингу резильєнтності	Розробити операційні плани дій; запровадити систему оцінки ризиків та регулярного звітування про стан критичної інфраструктури
Стратегія економічної безпеки України на період до 2025 року [38]	Аналізує деіндустріалізацію, втрату промислового потенціалу, низьку ресурсоефективність, технічну деградацію об'єктів критичної інфраструктури	Не визначено фінансових механізмів модернізації; відсутні індикатори резильєнтного розвитку	Створити систему фінансових стимулів та механізми державно-приватного партнерства для модернізації критичної інфраструктури
Стратегія енергетичної безпеки України [37]	Визначає енергетичну систему як сектор критичної інфраструктури, акцентує на загрозах енергобезпеці (кібератаки, дефіцит резервів, технічні ризики)	Не передбачено системи ризик-менеджменту; відсутня інтеграція з енергоринками ЄС; бракує положень щодо захисту енергетичних даних	Гармонізувати із Законом про КІ; розробити єдину систему управління ризиками; врахувати вимоги ENTSO-E та директиви NIS2

Джерело: складено авторами на основі документів [5; 37–39]

На думку Д. Мельника [31], загрозами критичній інфраструктурі є чинники, що спроможні реально чи потенційно завдати шкоди безперервності її роботи, функціональності, цілісності й стійкості або призвести до руйнування. Тобто автор пропонує розглядати загрози як сукупність впливів (реальних і потенційних), що порушують сталість функціонування об'єктів критичної інфраструктури [31].

О. Герасименко [25] трактує загрозу як будь-який вплив (природного, техногенного аби зловмисного походження), який може порушити безпеку, стійкість або функціонування систем, важливих для держави.

Д. Бобро [24] під загрозою критичній інфраструктурі розуміє потенційну подію або дію, яка реалізується через вразливість об'єкта і спричиняє втрати для людини, суспільства, бізнесу, держави.

Р. Мурасов та Я. Мельник [32] описують «загрозу критичній інфраструктурі» як об'єкт оцінки, що характеризується ймовірністю виникнення та руйнівними наслідками. З їх точки зору, у методологічному аспекті загроза може розглядатися як подія з певною ймовірністю реалізації та рівнем деструктивного впливу, що може бути кількісно оцінена [32]. С. Іванюта [28] під загрозою розуміє сукупність факторів ризику, що мають бути системно виявлені, оцінені та керовані на державному рівні.

О. Єрменчук [27] у своїй монографії «Наукові та методичні засади формування системи захисту критичної інфраструктури в Україні» розглядає загрози у контексті взаємодії державного управління, інфраструктурних об'єктів і суспільства, наголошуючи, що загрози критичній інфраструктурі є наслідком як цілеспрямованих дій, так і недостатньої взаємопов'язаності систем. Загрози є елементами середовища, що дестабілізують механізм функціонування національної інфраструктури [27].

Як свідчить аналіз, більшість авторів розглядають загрозу як множину чинників або подій, що через уразливості системи спричиняють порушення критичних функцій. Д. Мельник [31] надає найчіткішу функціональну дефініцію з зазначенням на безперервність, цілісність, стійкість. Д. Бобро [24] вписує загрозу в тріаду «загроза – вразливість – наслідок», що відповідає міжнародній ризик-логіці. М. Чеховська та О. Лісовська [35] фіксують відсутність кодифікованої дефініції в праві, що ускладнює єдині стандарти.

Отже, у сучасних працях домінує функціонально-резильєнтний підхід: загроза – це те, що підриває критичні функції інфраструктури (безперервність, цілісність, стійкість). Операціоналізація загроз переходить від якісних переліків до кількісних моделей (експертні методи, системна динаміка, ідентифікатори загроз і кумулятивні ефекти). Залишається правова прогалина – відсутність уніфікованої дефініції та переліку на рівні актів прямої дії; це гальмує стандартизацію оцінювання.

У *табл. 4* наведено класифікації загроз розвитку критичної інфраструктури, які зустрічаються у науковій літературі.

Матеріал охоплює еволюцію від базових ризик-орієнтованих підходів до інтегрованих системно-резиль-

Таблиця 3

Наукові підходи до трактування поняття «загрози критичній інфраструктурі»

Представники	Сутність	Ключові аспекти
Д. Мельник [31]	«Загрозами критичній інфраструктурі є чинники, що реально чи потенційно шкодять безперервності, функціональності, цілісності й стійкості або призводять до руйнування»	Функціональна спрямованість загрози; акцент на безперервності та стійкості
О. Герасименко [25]	Визначено сутність терміна; запропоновано класифікацію проявів загроз: фізичні напади, кібератаки, економічні диверсії, терористичні дії, атаки з використанням кліматичної зброї	Всеохопна таксономія за походженням/способом реалізації
Д. Бобро [24]	Загроза як елемент «моделі ризику»: поєднання загроз, вразливостей і нормованих наслідків для людини, суспільства, бізнесу, держави	Ризик-орієнтований підхід; пріоритезація за неприйнятним ризиком
Р. Мурасов Я. Мельник [32]	Загроза – об'єкт експертного оцінювання з ймовірністю реалізації та кумулятивними деструктивними наслідками; введено ідентифікатори загроз	Кількісно-якісна операціоналізація (Delphi/експертні методи)
С. Іванюта [28]	Наголос на необхідності комплексної методології оцінки загроз і ризиків та координації державних інституцій	Інституційно-нормативна рамка; методологія оцінювання
М.Чеховська О. Лісовська [35]	Констатується відсутність у законодавстві визначення термінів «загроза об'єкту критичної інфраструктури» та «загроза критичній інфраструктурі», а також єдиного переліку загроз	Виявлена правова лакуна, тобто прогалина у законодавстві; потреба уніфікації термінів
О. Єрменчук [27]	Системний погляд: загрози як наслідок цілеспрямованих дій і слабкої взаємопов'язаності систем національної інфраструктури	Системно-інституційний фрейм; взаємозалежності
А. Магомедов [30]	Систематизація ризиків/загроз, що призводять до деградації або руйнування систем; підкреслено технічні, організаційні, соціальні, воєнні чинники	Практична інвентаризація ризиків і наслідків

Джерело: складено авторами на основі [24; 25; 27; 28; 30–32; 35]

єнтних моделей. Джерела проаналізовано за роком, типом класифікації, основними категоріями та ключовими особливостями.

Проведений теоретичний аналіз засвідчує, що підходи до класифікації загроз еволюціонували від секторальних і ризик-орієнтованих моделей до інтегрованих систем, орієнтованих на резильєнтність і функціональну стійкість. Загальною тенденцією є конвергенція класифікацій у напрямі «рамки усіх небезпек», що охоплює природні, техногенні, воєнні, соціально-економічні та кіберзагрози. Після 2022 р. суттєво зростає увага до гібридних загроз, кібератак і ланцюгових ефектів. Водночас відсутня уніфікована національна таксономія, що ускладнює міжгалузеву порівняльність оцінок.

З огляду на вищевказане, для уніфікації пропонується:

- затвердити національну таксономію загроз;
- гармонізувати національні підходи з вимогами директив ЄС (Critical Entities Resilience, NIS2);
- ввести обов'язкові індикатори резильєнтності (час/глибина втрати функцій);
- стандартизувати підхід до пріоритезації (зона неприйнятного ризику, CAPEX/OPEX баланс);
- інституціоналізувати регулярні «stress-tests» каскадні сценарії;
- запропонувати уніфіковане визначення, яке має узгоджувати наукові та прикладні підходи й бути придатним для імплементації у нормативні документи та методики оцінювання.

На підставі теоретичного узагальнення вживаних трактувань поняття «загрози критичній інфраструктурі» автори цієї роботи пропонують використовувати термін «загрози розвитку критичної інфраструктури», розглядаючи його з таких позицій, як:

1) реальні або потенційні чинники природного, техногенного, соціально-економічного чи воєнного походження, які здатні через використання вразливостей об'єктів порушити безперервність їх функціонування, знизити рівень їхньої цілісності, керованості, резильєнтності та спричинити шкоду безпеці людини, суспільства й держави;
2) сукупність екзогенних та ендогенних факторів, що гальмують модернізацію, відновлення, цифровізацію або інтеграцію об'єктів критичної інфраструктури в систему національної безпеки.

Отже, під загрозами розвитку критичної інфраструктури слід розуміти сукупність факторів і умов, що здатні спричинити дестабілізацію функціонування інфраструктурних систем, порушення безперервності надання послуг, втрату керованості або пошкодження об'єктів. Вони можуть мати природне, техногенне, соціальне, політичне або кібернетичне походження та характеризуються високим потенціалом каскадних ефектів – коли вихід

Таблиця 4

Класифікації загроз розвитку критичної інфраструктури, які запропоновано українськими дослідниками у 2015–2025 роках

Науковці	Тип класифікації	Основні категорії	Особливість
Д. Бобро [24]	Ризик-орієнтована	Природні, техногенні, антропогенні; локальні, регіональні, національні; допустимі, граничні, неприйнятні	Введено поняття «зони неприйнятного ризику», застосовано матрицю «ймовірність × наслідок»
С. Іванюта [28]	Управлінсько-інституційна	Державні, галузеві, регіональні; зовнішні/внутрішні; прямі/опосередковані	Системний підхід до управління загрозами в межах національної стратегії безпеки
О. Герасименко [25]	Змішана (за джерелом і способом дії)	Фізичні, кібернетичні, економічні, терористичні, кліматичні	Розроблено класифікацію all-hazards, адаптовану до умов війни
О. Єрменчук [27]	Системна	Природні, техногенні, соціально-економічні, політичні, воєнні, інформаційні	Враховано каскадний характер загроз і міжсекторні залежності
Р. Мурасов Я. Мельник [32]	Кількісно-оцінна	Ймовірність, рівень руйнівних наслідків, тривалість впливу, відновлюваність	Запроваджено ідентифікатори загроз і шкали критичності
Д. Мельник [31]	Функціональна	Порушення безперервності, деградація цілісності, втрата керованості, зниження стійкості	Зосереджено на впливі загроз на критичні функції систем
А. Магомедов [30]	Прикладна	Технічні, організаційні, соціальні, воєнні, природні	Практична орієнтація на інженерно-організаційне управління ризиками
М. Чеховська О. Лісовська [35]	Нормативно-оглядова	Зовнішні (воєнні, терористичні, кібератаки), внутрішні (організаційні, кадрові, технічні)	Виявлено відсутність державної класифікації загроз, рекомендовано її створення

Джерело: складено авторами на основі [24; 25, 27; 28; 30–32; 35]

з ладу одного критично важливого елемента призводить до дестабілізації суміжних стратегічних секторів національної економіки.

У науковій літературі та міжнародних документах (EU Directive 2022/2557, OECD Guidelines on Critical Infrastructure Resilience, NATO Resilience Framework) поняття загрози тісно пов'язується з категоріями ризику, небезпеки, вразливості та резильєнтності. Таким чином, виявлення та класифікація загроз є необхідною передумовою для побудови ефективної системи управління ризиками у сфері критичної інфраструктури.

На основі виконаного теоретичного аналізу та синтезу наукових підходів запропоновано класифікаційні ознаки систематизації загроз розвитку критичної інфраструктури (*табл. 5*).

Запропонована систематизація дозволяє здійснювати багатовимірну ідентифікацію загроз, враховуючи їхню природу, масштаб, сферу дії та механізм впливу. Особливе місце серед них посідають гібридні загрози, які поєднують елементи кібернетичних, інформаційних, економічних і військових атак, спрямованих на підрив стійкості держави в цілому. Вони характеризуються прихованим характером, важкістю ідентифікації джерела походження та швидким поширенням наслідків через інтегрованість сучасних систем.

Виходячи з вищенаведеного авторами побудовано узагальнену класифікацію загроз розвитку критичної інфраструктури в Україні (*табл. 6*).

Як видно з *табл. 6*, класифікація охоплює 14 основних типів загроз, які можуть бути згруповані за природою походження: 1) антропогенні (1-7, 12–13) – пов'язані з людською діяльністю, управлінськими помилками, політичними або економічними факторами; 2) природні (8-11, 14) – викликані природними або кліматичними процесами. Система загроз має гібридний характер: дедалі частіше поєднуються фізичні, кібернетичні, інформаційні та соціальні компоненти.

Для України особливо актуальні воєнні, кібернетичні, енергетичні, кліматичні та медико-біологічні загрози, що підтверджується поточними ризиками у сфері енергетики, безпеки постачання й стійкості державного управління [41].

Рекомендується розглядати цю класифікацію як відправну точку для секторальної деталізації або ідентифікації об'єктів критичної інфраструктури (енергетика, транспорт, інформаційно-комунікаційні технології, водні ресурси, охорона здоров'я тощо) та формування інтегрального профілю ризиків.

Висновки. Сучасні тенденції управління загрозами розвитку критичної інфраструктури характеризуються високою динамічністю, міжсекторальною взаємозалежністю та зростанням складності ризиків. В умовах триваючої воєнної агресії проти України спектр загроз значно розширився, охоплюючи одночасно фізичну, цифрову та когнітивну сфери. Серед найсуттєвіших варто виокремити:

Таблиця 5

Систематизація загроз розвитку критичної інфраструктури за класифікаційними ознаками

Класифікаційна ознака	Вид загроз	Характеристика впливу
За походженням	Природні; техногенні; антропогенні; соціально-політичні; кібернетичні	Зумовлені стихійними лихами, аваріями, людським фактором, соціальними конфліктами або кібератаками
За масштабом впливу	Локальні; регіональні; національні; транскордонні	Визначають просторовий рівень поширення наслідків
За тривалістю дії	Короткострокові; довгострокові; латентні	Характеризують часовий горизонт прояву небезпеки
За сферою прояву	Енергетичні; транспортні; фінансові; комунікаційні; інформаційні; оборонні; медичні; продовольчі	Визначають сектор, на який спрямовано деструктивний вплив
За способом реалізації	Прямі (фізичні); непрямі (інформаційні, економічні, психологічні)	Визначають механізм завдання шкоди
За джерелом виникнення	Внутрішні; зовнішні; комбіновані	Залежно від локалізації ініціатора або причини загрози

Джерело: запропоновано авторами.

Таблиця 6

Узагальнена класифікація загроз розвитку критичної інфраструктури в Україні

Тип загрози	Підвиди (групи)	Приклади проявів / форми впливу	Джерела виникнення або характер
1	2	3	4
Воєнного характеру	застосування зброї масового ураження; ракетні, авіаційні, артилерійські удари; дії безпілотників; проникнення диверсійних груп	руйнування енергетичних, транспортних, комунікаційних об'єктів; ураження персоналу; блокування управління	бойові дії, гібридна війна, воєнна агресія
Терористичні / диверсійні	підриви, підпали, захоплення, диверсії	знищення критичних об'єктів, загибель людей, створення паніки	радикальні угруповання, спецслужби противника
Кібернетичні	порушення цілісності, конфіденційності, доступності інформації; атаки на системи управління; відсутність резервних каналів	кібератаки на SCADA, DDoS, вірусні ураження, збої зв'язку	державні та кримінальні хакерські структури
Інформаційно-психологічні	дезінформація, маніпуляції, витік даних, інформаційний тиск	паніка, підрив довіри, дестабілізація управління	інформаційні операції, соціальні мережі, медіа
Соціальні	захоплення об'єктів, страйки, заворушення, саботаж, поширення панічних настроїв	порушення виробничого процесу, зрив постачання, блокування персоналу	соціально-політична нестабільність
Техногенні	аварії, пожежі, вибухи, викиди небезпечних речовин, гідродинамічні аварії, руйнування споруд	пошкодження систем енергопостачання, транспорту, зв'язку	зношення обладнання, недотримання безпеки, людський фактор
Організаційно-кадрові	помилки персоналу, низька кваліфікація, порушення інструкцій, слабкий контроль	технічні збої, аварії, помилки в управлінні	людський фактор, управлінська неефективність
Природні (геофізичні)	землетруси, зсуви, обвали, осідання, карстові провали, підтоплення	руйнування будівель, транспортних шляхів, мереж	природні процеси в літосфері
Природні (метеорологічні)	зливи, град, бурі, урагани, заморозки, спека, сильні морози, ожеледь, снігопади, пилові бурі, тумани	переривання енергопостачання, транспортні збої, руйнування інфраструктури	екстремальні погодні явища
Природні (гідрологічні)	повені, паводки, зсуви, затоплення, підтоплення, льодоходи, селі, посухи	пошкодження гідротехнічних споруд, підтоплення систем життєзабезпечення	водні аномалії, зміни гідрорежиму

Закінчення табл. 6

1	2	3	4
Природні (медико-біологічні)	інфекційні захворювання людей (епідемії, пандемії), тварин (панзоотії), рослин (панфітотії)	масові захворювання, зупинка транспорту, дефіцит кадрів, ланцюгові збої у постачанні	природні епідеміологічні процеси, біологічні загрози
Економічні	фінансові кризи, дефіцит енергоресурсів, санкції, інфляційні коливання	недофінансування, зрив проєктів, зупинка виробництва	макроекономічна нестабільність
Політичні / регуляторні	зміна законодавства, політичні конфлікти, корупційні дії	втрата керованості систем, блокування проєктів	управлінська нестабільність, державна політика
Екологічні / кліматичні	деградація земель, забруднення води, зміна клімату, підвищення температури	пошкодження інфраструктури, зростання аварійності	антропогенний вплив, глобальні зміни клімату

Джерело: запропоновано авторами

- руйнування енергетичної інфраструктури, що зумовлює каскадні наслідки для транспортної, комунікаційної та водопостачальної систем;
- кібератаки на органи державної влади, військові та фінансові структури;
- інформаційно-психологічні операції, спрямовані на підрив суспільної довіри до державних інститутів;
- економічні ризики, пов'язані з блокуванням логістичних ланцюгів, експортних потоків і залучення інвестицій;
- екологічні загрози, зумовлені техногенними аваріями та цілеспрямованим руйнуванням промислових об'єктів.

Управління такими загрозами сьогодні базується на концепції резильєнтності критичної інфраструктури, що передбачає системну превентивну оцінку ризиків, диверсифікацію джерел енергії й постачання, створення резервних систем управління та комунікацій, посилення кіберзахисту, міжвідомчу координацію й розвиток державно-приватного партнерства у сфері безпеки.

Проведеним дослідженням уточнено зміст поняття «загрози розвитку критичної інфраструктури» як багатовимірного феномену, що поєднує технічні, соціальні, економічні та інформаційні компоненти. Запропонована класифікація загроз формує наукову основу для створення інтегрованої системи моніторингу й управління ризиками, яка може бути використана під час розроблення Національної стратегії резильєнтності критичної інфраструктури України.

Порівняльний аналіз підходів українських і зарубіжних авторів засвідчив еволюцію від секторальних і ризик-орієнтованих моделей до системно-резильєнтних концепцій, що охоплюють міжсекторальні зв'язки, гібридні сценарії та функціональну стійкість. Водночас зберігається відсутність уніфікованих критеріїв критичності та показників стійкості, що ускладнює порівняння між секторами та міжнародну гармонізацію оцінок.

Еволюція теоретичних підходів відображає поступ до інтегрованої концепції резильєнтності до всіх небезпек, у межах якої здійснюється об'єднання природних, техногенних, воєнних, кібернетичних і соціальних загроз у єдину систему ризик-менеджменту критичної інфраструктури. Після 2022 року особливу вагу набули гібридні та кіберзагрози, що поєднують інформаційні, економічні та технологічні чинники. Для підвищення ефективності державної політики у сфері безпеки доцільно:

- розробити Національну стратегію розвитку критичної інфраструктури, орієнтовану на інноваційність, сталий розвиток і цифрову трансформацію;
- імплементувати вимоги Директиви ЄС 2022/2557 щодо оцінювання ризиків, міжсекторальних сценаріїв та програм стійкості;
- внести зміни до Закону України «Про критичну інфраструктуру», доповнивши його економічними стимулами для операторів, стандартами «аудиту резильєнтності» та механізмами звітності про ризики;
- забезпечити узгодженість стратегічних документів із питань національної, економічної та енергетичної безпеки;
- створити систему моніторингу індикаторів загроз і стійкості, зокрема рівня зношеності активів, частоти інцидентів, кіберстійкості та частки інвестицій у відновлення.

Узагальнюючи, можна стверджувати, що сучасна наука переходить до уніфікованої системи класифікації загроз розвитку критичної інфраструктури, яка охоплює джерела, механізми, об'єкти, наслідки та тривалість дії. Водночас зберігаються прогалини у стандартизації метрик резильєнтності та бракує емпіричних досліджень для валідації моделей.

Для України перспективними напрямами є адаптація європейських методик оцінювання ризиків і стійкості, розроблення інтегральних індексів резильєнтності (CIRIX), посилення кіберстійкості енергетичної, транспортної та цифрової інфраструктури. Подальші дослідження доцільно спрямувати на вдосконалення нормативно-правової бази, інтеграцію критеріїв резильєнтності у стратегічне планування та забезпечення сталого повоєнного відновлення економіки України.

ЛІТЕРАТУРА

1. Хаустова В. Є., Трушкіна Н. В. Ризики та загрози національній безпеці: сутність і класифікація. *Бізнес Інформ*. 2024. № 10. С. 6–22.

DOI: 10.32983/2222-4459-2024-10-6-22

2. Хаустова В. Є., Решетняк О. І. Резильєнтність економіки: сутність і виклики для України. *Бізнес Інформ*. 2023. № 7. С. 30–41.

DOI: 10.32983/2222-4459-2023-7-30-41

3. Кизим М. О., Хаустова В. Є., Трушкіна Н. В. Сутність поняття «критична інфраструктура» з позицій національної безпеки України. *Бізнес Інформ*. 2022. № 12. С. 58–78.

DOI: 10.32983/2222-4459-2022-12-58-78

4. Хаустова В., Трушкіна Н., Зінченко В. Ключові виклики відновлення критичної інфраструктури України в умовах повоєнної розбудови економіки // Повоєнне відновлення економіки України: проблеми та напрямки вирішення : кол. моногр. / за ред. В. Є. Хаустової. Харків : ФОП Лібуркіна Л. М., 2023. С. 7–33.

DOI: https://doi.org/10.32983/978-617-7801-41-1

5. Стратегія національної безпеки України : Указ Президента України від 14.09.2020 р. № 392/2020 (із змінами, у редакції від 07.01.2025 р.). URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

6. Концепція забезпечення національної системи стійкості : Указ Президента України від 27.09.2021 р. № 479/2021. URL: https://zakon.rada.gov.ua/laws/show/479/2021#n11

7. Андрієнко Д., Горюнов Д., Грудова В. та ін. Звіт про прямі збитки інфраструктури від руйнувань внаслідок військової агресії росії проти України станом на листопад 2024 року. Київ : Київська школа економіки, 2025. 28 с. URL: https://kse.ua/wp-content/uploads/2025/02/KSE_Damages_Report-November-2024-UA.pdf

8. Звіт про прямі збитки інфраструктури від руйнувань внаслідок військової агресії Росії проти України станом на початок 2024 року. Київ : Київська школа економіки, 2024. 39 с. URL: https://kse.ua/wp-content/uploads/ 2024/04/01.01.24_Damages_Report.pdf

9. Updated Ukraine Recovery and Reconstruction Needs Assessment Released: Press Release No 2024/ECA/063. *World Bank Group*. 2024. February 15. URL: https://www.worldbank.org/en/news/press-release/2024/02/15/updated-ukraine-recovery-and-reconstruction-needs-assessment-released

10. Ukraine. Rapid damage and needs assessment (RDNA3). February 2022 – December 2023. Washington, DC: World Bank, 2024. 182 p. URL: https://documents1.worldbank.org/curated/en/099021324115085807/pdf/P1801741bea12c012189ca16d95d8c2556a.pdf

11. Updated Ukraine Recovery and Reconstruction Needs Assessment Released: Press Release No 2025/ECA/079. *World Bank Group*. 2025. February 25. URL: https://www.worldbank.org/en/news/press-release/2025/02/25/updated-ukraine-recovery-and-reconstruction-needs-assessment-released

12. Ukraine. Rapid damage and needs assessment (RDNA4). February 2022 – December 2024. Washington, DC : World Bank, 2025. 200 p. URL: https://openknowledge.worldbank.org/server/api/core/bitstreams/96bd9c94-c327-49b4-8aff-fe125686f04e/content

13. Kwilinski A., Trushkina N. Impact of Cyber Risks and Threats on the Critical Infrastructure Development: Visualization of Scientific Research. *Proceedings of the 12th International Conference on Applied Innovation in IT* (ICAIIT). 2024. Vol. 12. Iss. 2. P. 107–119.

DOI: 10.25673/118123

14. Кібератаки на бізнес України 2025: Нові Вектори Загроз та Захист // Synchron. 2025. URL: https://synchron.ua/cyberattacks-on-ukrainian-business-2025-uk/#:~:text

15. Luiijf H. A. M., Nieuwenhuijs A. H. Extensible threat taxonomy for critical infrastructures. *International Journal of Critical Infrastructures*. 2008. Vol. 4. Iss. 4. P. 409–417.

DOI: 10.1504/IJCIS.2008.020159

16. Chen Z., Xu G., Mahalingam V. et al. A Cloud Computing Based Network Monitoring and Threat Detection System for Critical Infrastructures. *Big Data Research*. 2016. Vol. 3. P. 10–23.

DOI: 10.1016/j.bdr.2015.11.002

17. Kure H. I., Islam S. Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure. *Journal of Universal Computer Science*. 2019. Vol. 25. Iss. 11. P. 1478–1502.

18. Ghafir I., Saleem J., Hammoudeh M. et al. Security threats to critical infrastructure: the human factor. *Journal of Supercomputing*. 2018. Vol. 74. Iss. 10. P. 4986-5002.

DOI: 10.1007/s11227-018-2337-2.

19. Wells E. M., Boden M., Tseytlin I., Linkov I. Modeling critical infrastructure resilience under compounding threats: A systematic literature review. *Progress in Disaster Science*. 2022. Vol. 15. Article 100244.

DOI: 10.1016/j.pdisas.2022.100244

20. Jovanović A., Schernberg H., Brem S., Chakravarty S., Jelić M. Indicator-based assessment of extreme threats (XTs) and their impacts on the resilience of geographical areas and critical infrastructures. *Environment Systems and Decisions*. 2023. Vol. 43. Iss. 4. P. 599–624.

DOI: 10.1007/s10669-023-09950-x

21. Djenna A., Harous S., Saidouni D. E. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences (Switzerland)*. 2021. Vol. 11. Iss. 10. Article 4580.

DOI: 10.3390/app11104580

22. Geppert K., Konieczny J. Analysis of potential threats to the critical infrastructure of the 31st Tactical Air Base in the context of the security of the Poznań Agglomeration. *Przegląd Strategiczny – National Security*. 2023. Iss. 16. P. 219–235.

DOI: 10.14746/ps.2023.1.16

23. Mehdiyev S. A., Hashimov M. A. Analysis of Threats and Cybersecurity in the Oil and Gas Sector within the Context of Critical Infrastructure. *International Journal of Information Technology and Computer Science*. 2024. Vol. 16. Iss. 1. P. 43–53.

DOI: 10.5815/ijitcs.2024.01.05

24. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. *Стратегічні пріоритети. Сер. Економіка*. 2015. № 4 (37). С. 83-93.

25. Герасименко О. М. Загрози об'єктам критичної інфраструктури України в умовах воєнного стану. *Науковий вісник Ужгородського національного університету. Сер. : Право*. 2024. Вип. 84. Ч. 3. С. 257–262.

DOI: 10.24144/2307-3322.2024.84.3.39.

26. Єрменчук О. Оцінка загроз критичній інфраструктурі як важлива складова частина діяльності із захисту державної безпеки. *Jurnalul Juridic Național: Teorie și Practică – Національний юридичний журнал: теорія і практика*. 2018. № 5 (50). С. 50–54.

27. Єрменчук О. В. Наукові та методичні засади формування системи захисту критичної інфраструктури в Україні : монографія. Хмельницький : ХУУП імені Леоніда Юзькова, 2023. 312 с.

28. Іванюта С. П. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки (моніторинг реалізації Стратегії національної безпеки) : аналіт. записка. Київ : НІСД, 2017. 10 с. URL: https://www.niss.gov.ua/doslidzhennya/nacionalna-bezpeka/zagrozi-kritichniy-infrastrukturi-ta-ikh-vpliv-na-stan-nacionalnoi

29. Іванюта С. П., Панов Є. М., Іваненко О. І., Гапон С. В. Оцінка ризиків критичній інфраструктурі України в умовах російської військової агресії. *Вісник Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Сер. : Хімічна інженерія, екологія та ресурсозбереження*. 2024. № 2 (23). С. 47-61.

DOI: 10.20535/2617-9741.2.2024.307360

30. Магомедов А. О. Ризики та загрози для об'єктів критичної інфраструктури та шляхи їх подолання. *Інвестиції: практика та досвід*. 2024. № 15. С. 216–222.

DOI: 10.32702/2306-6814.2024.15.216

31. Мельник Д. С. Побудова моделі загроз національній критичній інфраструктурі України як основа забезпечення її безпеки та стійкості. *Вісник Харківського національного університету внутрішніх справ*. 2024. № 1 (104). С. 237–250.

DOI: 10.32631/v.2024.1.20

32. Мурасов Р. К., Мельник Я. В. Результати оцінювання загроз критичній інфраструктурі методом експертного оцінювання. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2023. № 3 (48). С. 83–88.

DOI: 10.33099/2311-7249/2023-48-3-83-88

33. Невольніченко А. І., Чумаченко С. М., Михайлова А. В., Пиріков О. В., Мурасов Р. К. Моделювання загроз виникнення надзвичайних ситуацій на об'єктах критичної інфраструктури з використанням методу системної динаміки. *Таврійський науковий вісник. Сер. : Технічні науки*. 2022. № 3. С. 89–97.

DOI: 10.32851/tnv-tech.2022.3.10

34. Помаза-Пономаренко А. Л. Збитки, нанесені бойовими діями об'єктам критичної інфраструктури в Україні: механізми оцінювання та відновлення. *Успіхи і досягнення у науці*. 2025. № 1 (11). С. 601–611.

DOI: 10.52058/3041-1254-2025-1(11)-601-611

35. Чеховська М. М., Лісовська О. Л. Загрози критичній інфраструктурі України в сучасних умовах. *Ефективна економіка*. 2025. № 2.

DOI: 10.32702/2307-2105.2025.2.10

36. Khaustova V., Ilyash O. Military and economic potential of the countries of the world: assessment and analysis of the impact on international security // International Economic Policy for the Polycrisis / edited uy Konrad Raczkowski, Piotr Komorowski. Routledge, 2024.

DOI: 10.4324/9781003487913-9

37. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX (із змінами, у редакції від 21.09.2024 р.). URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

38. Стратегія енергетичної безпеки : Розпорядженням Кабінету Міністрів України від 04.08.2021 р. № 907-р. URL: https://zakon.rada.gov.ua/ laws/show/907-2021-%D1%80#Text

39. Стратегія економічної безпеки України : Указ Президента України від 11.08.2021 р. № 347/2021. URL: https://zakon.rada.gov.ua/laws/show/347/2021#Text

40. Про затвердження вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності : Постанова Кабінету Міністрів України від 01.04.2025 р. № 367. URL: https://zakon.rada.gov.ua/laws/ show/367-2025-%D0%BF#Text

41. Хаустова В. Є. Трансформація моделі економіки України у повоєнний період : монографія. Харків : Лібуркіна Л. М., 2025. 152 с.

DOI: https://doi.org/10.32983/978-617-7801-52-7

REFERENCES

Andriienko, D., Horiunov, D., Hrudova, V., et al. (2025). *Zvit pro priami zbytku infrastruktury vid ruinuvan vnaslidok viiskovoi agresii rosii proty Ukrainy stanom na lystopad 2024 roku* [Report on direct infrastructure losses from destruction due to Russian military aggression against Ukraine as of November 2024]. Kyiv: Kyiv School of Economics. https://kse.ua/wp-content/uploads/2025/02/KSE_Damages_Report-November-2024-UA.pdf

Bobro, D. H. (2015). *Vyznachennia kryteriiv otsinky ta zahrozy krytychnii infrastrukturi* [Definition of assessment criteria and threats to critical infrastructure]. *Stratehichni Priorytety. Ser. Ekonomika*, *4*(37), 83-93.

Cabinet of Ministers of Ukraine. (2021, August 4). *Stratehiia enerhetychnoi bezpeky* [Energy Security Strategy] (Order No. 907-r). https://zakon.rada.gov.ua/ laws/show/907-2021-%D1%80#Text

Cabinet of Ministers of Ukraine. (2025, April 1). *Pro zatverdzhennia vymoh shchodo upravlinnia ryzykamy bezpeky na obiektakh krytychnoi infrastruktury I katehorii krytychnosti* [On approval of requirements for security risk management at critical infrastructure facilities of criticality category I] (Resolution No. 367). https://zakon.rada.gov.ua/laws/ show/367-2025-%D0%BF#Text

Chekhovska, M. M., & Lisovska, O. L. (2025). *Zahrozy krytychnii infrastrukturi Ukrainy v suchasnykh umovakh* [Threats to critical infrastructure of Ukraine in modern conditions]. *Efektyvna Ekonomika*, *2*. https://doi.org/10.32702/2307-2105.2025.2.10

Chen, Z., Xu, G., Mahalingam, V., et al. (2016). A cloud computing based network monitoring and threat detection system for critical infrastructures. *Big Data Research*, *3*, 10–23. https://doi.org/10.1016/j.bdr.2015.11.002

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences (Switzerland)*, *11*(10), Article 4580. https://doi.org/10.3390/app11104580

Geppert, K., & Konieczny, J. (2023). Analysis of potential threats to the critical infrastructure of the 31st Tactical Air Base in the context of the security of the Poznań Agglomeration. *Przegląd Strategiczny – National Security*, *16*, 219–235. https://doi.org/10.14746/ps.2023.1.16

Ghafir, I., Saleem, J., Hammoudeh, M., et al. (2018). Security threats to critical infrastructure: The human factor. *Journal of Supercomputing*, *74*(10), 4986–5002. https://doi.org/10.1007/s11227-018-2337-2

Herasymenko, O. M. (2024). *Zahrozy obiektam krytychnoi infrastruktury Ukrainy v umovakh voiennoho stanu* [Threats to critical infrastructure facilities of Ukraine under martial law]. *Naukovyi Visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia : Pravo*, *84*(3), 257–262. https://doi.org/10.24144/2307-3322.2024.84.3.39

Ivaniuta, S. P. (2017). *Zahrozy krytychnii infrastrukturi ta yikh vplyv na stan natsionalnoi bezpeky (monitorynh realizatsii Stratehii natsionalnoi bezpeky)* [Threats to critical infrastructure and their impact on national security (monitoring the implementation of the National Security Strategy)]. Kyiv: NISD. https://www.niss.gov.ua/doslidzhennya/nacionalna-bezpeka/zagrozi-kritichniy-infrastrukturi-ta-ikh-vpliv-na-stan-nacionalnoi

Ivaniuta, S. P., Panov, Ye. M., Ivanenko, O. I., & Hapon, S. V. (2024). *Otsinka ryzykiv krytychnii infrastrukturi Ukrainy v umovakh rosiiskoi viiskovoi ahresii* [Risk assessment for Ukraine's critical infrastructure in the context of Russian military aggression]. *Visnyk Natsionalnoho Tekhnichnoho Universytetu Ukrainy «Kyivskyi Politekhnichnyi Instytut imeni Ihoria Sikorskoho». Seriia : Khimichna Inzheneriia, Ekolohiia ta Resursozberezhennia*, *2*(23), 47-61. https://doi.org/10.20535/2617-9741.2.2024.307360

Jovanović, A., Schernberg, H., Brem, S., Chakravarty, S., & Jelić, M. (2023). Indicator-based assessment of extreme threats (XTs) and their impacts on the resilience of geographical areas and critical infrastructures. *Environment Systems and Decisions*, *43*(4), 599–624. https://doi.org/10.1007/s10669-023-09950-x

Khaustova, V., & Ilyash, O. (2024). Military and economic potential of the countries of the world: Assessment and analysis of the impact on international security. In K. Raczkowski & P. Komorowski (Eds.), *International economic policy for the polycrisis*. Routledge. https://doi.org/10.4324/9781003487913-9

Khaustova, V., Trushkina, N., & Zinchenko, V. (2023). *Kliuchovi vyklyky vidnovlennia krytychnoi infrastruktury Ukrainy v umovakh povoiennoi rozbudovy ekonomiky* [Key challenges of restoring Ukraine's critical infrastructure in the context of post-war economic development]. In V. Ye. Khaustova (Ed.), *Povoienne vidnovlennia ekonomiky Ukrainy: problemy ta napriamky vyrishennia* [Post-war reconstruction of Ukraine's economy: Problems and directions of solution] (pp. 7–33). Kharkiv: FOP Liburkina L. M. https://doi.org/10.32983/978-617-7801-41-1

Khaustova, V. Ye. (2025). *Transformatsiia modeli ekonomiky Ukrainy u povoiennyi period* [Transformation of the economic model of Ukraine in the post-war period]. Kharkiv: Liburkina L. M. https://doi.org/10.32983/978-617-7801-52-7

Khaustova, V. Ye., & Reshetniak, O. I. (2023). *Rezylientnist ekonomiky: sutnist i vyklyky dlia Ukrainy* [Resilience of the economy: Essence and challenges for Ukraine]. *Biznes Inform*, *7*, 30–41. https://doi.org/10.32983/2222-4459-2023-7-30-41

Khaustova, V. Ye., & Trushkina, N. V. (2024). *Ryzyky ta zahrozy natsionalnii bezpetsi: sutnist i klasyfikatsiia* [Risks and threats to national security: Essence and classification]. *Biznes Inform*, *10*, 6–22. https://doi.org/10.32983/2222-4459-2024-10-6-22

Kure, H. I., & Islam, S. (2019). Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure. *Journal of Universal Computer Science*, *25*(11), 1478–1502.

Kwilinski, A., & Trushkina, N. (2024). Impact of cyber risks and threats on the critical infrastructure development: Visualization of scientific research. *Proceedings of the 12th International Conference on Applied Innovation in IT (ICAIIT)*, *12*(2), 107–119. https://doi.org/10.25673/118123

Kyiv School of Economics. (2024). *Zvit pro priami zbytku infrastruktury vid ruinuvan vnaslidok viiskovoi agresii Rosii proty Ukrainy stanom na pochatok 2024 roku* [Report on direct infrastructure losses from destruction due to the Russian military aggression against Ukraine as of the beginning of 2024]. Kyiv. https://kse.ua/wp-content/uploads/2024/04/01.01.24_Damages_Report.pdf

Kyzym, M. O., Khaustova, V. Ye., & Trushkina, N. V. (2022). *Sutnist poniattia «krytychna infrastruktura» z pozytsii natsionalnoi bezpeky Ukrainy* [The essence of the concept of "critical infrastructure" from the standpoint of national security of Ukraine]. *Biznes Inform*, *12*, 58–78. https://doi.org/10.32983/2222-4459-2022-12-58-78

Luiijf, H. A. M., & Nieuwenhuijs, A. H. (2008). Extensible threat taxonomy for critical infrastructures. *International Journal of Critical Infrastructures*, *4*(4), 409–417. https://doi.org/10.1504/IJCIS.2008.020159

Mahomedov, A. O. (2024). *Ryzyky ta zahrozy dlia obiektiv krytychnoi infrastruktury ta shliakhy yikh podolannia* [Risks and threats to critical infrastructure facilities and ways to overcome them]. *Investytsii: Praktyka ta Dosvid*, *15*, 216–222. https://doi.org/10.32702/2306-6814.2024.15.216

Mehdiyev, S. A., & Hashimov, M. A. (2024). Analysis of threats and cybersecurity in the oil and gas sector within the context of critical infrastructure. *International Journal of Information Technology and Computer Science*, *16*(1), 43–53. https://doi.org/10.5815/ijitcs.2024.01.05

Melnyk, D. S. (2024). *Pobudova modeli zahroz natsionalnii krytychnii infrastrukturi Ukrainy yak osnova zabezpechennia yii bezpeky ta stiikosti* [Building a model of threats to the national critical infrastructure of Ukraine as a basis for ensuring its safety and sustainability]. *Visnyk Kharkivskoho Natsionalnoho Universytetu Vnutrishnikh Sprav*, *1*(104), 237–250. https://doi.org/10.32631/v.2024.1.20

Murasov, R. K., & Melnyk, Ya. V. (2023). *Rezultaty otsiniuvannia zahroz krytychnii infrastrukturi metodom ekspertnoho otsiniuvannia* [Results of critical infrastructure threat assessment by expert evaluation method]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, *3*(48), 83–88. https://doi.org/10.33099/2311-7249/2023-48-3-83-88

Nevolnichenko, A. I., Chumachenko, S. M., Mykhailova, A. V., Pyrikov, O. V., & Murasov, R. K. (2022). *Modeliuvannia zahroz vynyknennia nadzvychainykh sytuatsii na obiektakh krytychnoi infrastruktury z vykorystanniam metodu systemnoi dynamiky* [Modeling threats of emergencies at critical infrastructure facilities using the system dynamics method]. *Tavriiskyi Naukovyi Visnyk. Seriia : Tekhnichni Nauky*, *3*, 89–97. https://doi.org/10.32851/tnv-tech.2022.3.10

Pomaza-Ponomarenko, A. L. (2025). *Zbytky, naneseni boiovymy diiamy obiektam krytychnoi infrastruktury v Ukraini: mekhanizmy otsiniuvannia ta vidnovlennia* [Damage caused by hostilities to critical infrastructure facilities in Ukraine: Assessment and restoration mechanisms]. *Uspikhy i Dosiahnennia u Nauci*, *1*(11), 601–611. https://doi.org/10.52058/3041-1254-2025-1(11)-601-611

President of Ukraine. (2020, September 14). *Stratehiia natsionalnoi bezpeky Ukrainy* [National Security Strategy of Ukraine] (Decree No. 392/2020). https://zakon.rada.gov.ua/laws/show/392/2020#Text

President of Ukraine. (2021, August 11). *Stratehiia ekonomichnoi bezpeky Ukrainy* [Strategy of Economic Security of Ukraine] (Decree No. 347/2021). https://zakon.rada.gov.ua/laws/show/347/2021#Text

President of Ukraine. (2021, September 27). *Kontseptsiia zabezpechennia natsionalnoi systemy stiikosti* [Concept of ensuring the national resilience system] (Decree No. 479/2021). https://zakon.rada.gov.ua/laws/show/479/2021#n11

Synchron. (2025). *Kiberataky na biznes Ukrainy 2025: Novi Vektory Zahroz ta Zakhyst* [Cyberattacks on Ukrainian business 2025: New threat vectors and protection]. https://synchron.ua/cyberattacks-on-ukrainian-business-2025-uk/#:~:text

Verkhovna Rada of Ukraine. (2021, November 16). *Pro krytychnu infrastrukturu* [About critical infrastructure] (Law No. 1882-IX). https://zakon.rada.gov.ua/laws/show/1882-20#Text

Wells, E. M., Boden, M., Tseytlin, I., & Linkov, I. (2022). Modeling critical infrastructure resilience under compounding threats: A systematic literature review. *Progress in Disaster Science*, *15*, Article 100244. https://doi.org/10.1016/j.pdisas.2022.100244

World Bank. (2024). *Ukraine. Rapid damage and needs assessment (RDNA3). February 2022 – December 2023*. Washing-

ton, DC. https://documents1.worldbank.org/curated/en/099021324115085807/pdf/P1801741bea12c012189ca16d95d8c2556a.pdf

World Bank. (2025). *Ukraine. Rapid damage and needs assessment (RDNA4). February 2022 – December 2024*. Washington, DC. https://openknowledge.worldbank.org/server/api/core/bitstreams/96bd9c94-c327-49b4-8aff-fe125686f04e/content

World Bank Group. (2024, February 15). *Updated Ukraine recovery and reconstruction needs assessment released: Press Release No 2024/ESA/063*. https://www.worldbank.org/en/news/press-release/2024/02/15/updated-ukraine-recovery-and-reconstruction-needs-assessment-released

World Bank Group. (2025, February 25). *Updated Ukraine recovery and reconstruction needs assessment released: Press Release No 2025/ECA/079*. https://www.worldbank.org/en/news/press-release/2025/02/25/updated-ukraine-recovery-and-reconstruction-needs-assessment-released

Yermenchuk, O. (2018). *Otsinka zahroz krytychnii infrastrukturi yak vazhlyva skladova chastyna diialnosti iz zakhystu derzhavnoi bezpeky* [Assessment of threats to critical infrastructure as an important component of state security]. *Jurnalul Juridic Național: Teorie și Practică – Natsionalnyi Yurydychnyi Zhurnal: Teoriia i Praktyka*, *5*(50), 50–54.

Yermenchuk, O. V. (2023). *Naukovi ta metodychni zasady formuvannia systemy zakhystu krytychnoi infrastruktury v Ukraini* [Scientific and methodological principles of forming a system for protecting critical infrastructure in Ukraine]. Khmelnytskyi: KhUUP imeni Leonida Yuzkova.

Стаття надійшла до редакції 10.07.2025 р.
Статтю прийнято до публікації 24.07.2025 р.