УДК 330.3:338.4
JEL Classification: H54; H56; L52; P51

ТЕОРЕТИЧНІ ПІДХОДИ ДО СУТНОСТІ ПОНЯТТЯ «КРИТИЧНА ІНФРАСТРУКТУРА»: МІЖНАРОДНИЙ, ПРОСТОРОВИЙ І РЕЗИЛЬЄНТНІСНИЙ ВИМІРИ

©2025 **ХАУСТОВА В. Є., ТРУШКІНА Н. В.**

УДК 5330.3:338.4
JEL Classification: H54; H56; L52; P51

Хаустова В. Є., Трушкіна Н. В.

Теоретичні підходи до сутності поняття «критична інфраструктура»: міжнародний, просторовий і резильєнтнісний виміри

У статті здійснено ґрунтовний теоретико-методологічний аналіз та систематизацію підходів до сутності поняття «критична інфраструктура» з урахуванням міжнародного, просторового та резильєнтнісного вимірів. Актуальність дослідження зумовлена зростанням воєнних, техногенних, кліматичних і кіберзагроз, а також викликами повоєнного відновлення України, що потребує переосмислення ролі критичної інфраструктури у забезпеченні стійкості територій, безперервності надання життєво важливих послуг і стабільного функціонування національної економіки. Методологічну основу дослідження становлять бібліометричний аналіз наукових публікацій, індексованих у базі Scopus, порівняльний аналіз національних і наднаціональних підходів до визначення критичної інфраструктури, а також узагальнення положень міжнародних нормативно-правових документів і сучасних наукових концепцій у сфері безпеки, управління ризиками та резильєнтності. Поєднання бібліометричних і якісних аналітичних методів дозволило простежити еволюцію наукових підходів до трактування критичної інфраструктури та ідентифікувати ключові напрями трансформації цього поняття у сучасних умовах. У результаті дослідження виокремлено й систематизовано домінуючі теоретичні підходи до трактування критичної інфраструктури, зокрема функціональний, наслідково-орієнтований, системно-мережевий, просторовий, ризик-орієнтований і резильєнтнісний. Обґрунтовано, що більшість наявних визначень має фрагментарний характер і зосереджується переважно на секторальних або функціональних аспектах, не враховуючи повною мірою територіальну локалізацію інфраструктурних об'єктів, міжсекторальні взаємозалежності, мережеву структуру інфраструктурних систем та потенціал виникнення каскадних ефектів у разі їх порушення. Доведено, що інтеграція просторового та резильєнтнісного підходів дозволяє розширити традиційне розуміння критичної інфраструктури, трактуючи її не як статичну характеристику окремих об'єктів, а як динамічну властивість інфраструктурних систем, що формується під впливом територіальних умов, рівня міжсекторальної взаємозалежності, спектра загроз і спроможності до адаптації та відновлення. На цій основі обґрунтовано інтегрований підхід до визначення критичної інфраструктури, який поєднує просторовий, резильєнтнісний і ризик-орієнтований виміри та створює методологічні передумови для комплексного оцінювання рівня критичності інфраструктурних систем. Практичне значення отриманих результатів полягає у можливості їх використання для вдосконалення державної політики у сфері критичної інфраструктури, розроблення стратегій просторового розвитку й територіальної безпеки, а також імплементації принципів Build Back Better у повоєнній розбудові економіки України з урахуванням завдань підвищення стійкості та адаптивності інфраструктурних систем.

Ключові слова: *національна економіка, критична інфраструктура, просторовий вимір, системно-мережевий підхід, міжсекторальні взаємозалежності, ризик-орієнтований підхід, резильєнтність, загрози, каскадні ефекти, інфраструктурна безпека, управління ризиками, принцип Build.*

DOI: *https://doi.org/10.32983/2222-0712-2025-4-336-351*

Рис.: *4.* ***Табл.:*** *4.* ***Бібл.:*** *40.*

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 330.3:338.4
JEL Classification: H54; H56; L52; P51

Khaustova V. Ye., Trushkina N. V. The Theoretical Approaches to the Essence of the Concept of «Critical Infrastructure»: International, Spatial, and Resilience Dimensions

The article conducts a comprehensive theoretical and methodological analysis and systematization of approaches to the essence of the concept of «critical infrastructure», considering international, spatial, and resilience dimensions. The relevance of the study is driven by the increasing military, technological, climatic, and cyber threats, as well as the challenges of Ukraine's post-war recovery, which necessitate a reassessment of the role of critical infrastructure in ensuring territorial resilience, continuity of essential services, and the stable functioning of the national economy. The methodological foundation of the study consists of a bibliometric analysis of scientific publications indexed in the Scopus database, a comparative analysis of national and supranational approaches to defining critical infrastructure, as well as a synthesis of international regulatory documents and contemporary scientific conceptions in the fields of security, risk management, and resilience. The combination of bibliometric and qualitative analytical methods made it possible to trace the evolution of scientific approaches to the interpretation of critical infrastructure and identify key directions in the transformation of this concept under modern conditions. The study highlights and systematizes the dominant theoretical approaches to interpreting critical infrastructure, including the functional, consequence-oriented, system-network, spatial, risk-oriented, and resilience approaches. It has been substantiated that most existing definitions are fragmentary in nature and focus primarily on sectoral or functional aspects, without fully taking into account the territorial location of infrastructure facilities, intersectoral interdependencies, the network structure of infrastructure systems, and the potential for cascading effects in case of disruptions. It has been demonstrated that integrating spatial and resilience approaches allows for an expansion of the traditional understanding of critical infrastructure, interpreting it not as a static characteristic of individual facilities, but as a dynamic property of infrastructure systems, shaped by territorial conditions, the level of intersectoral interdependence, the range of threats, and the capacity for adaptation and recovery. On this basis, an integrated approach to identifying critical infrastructure has been substantiated, which combines spatial, resilience, and risk-oriented dimensions and creates the methodological prerequisites for a comprehensive assessment of the criticality level of infrastructure systems. The practical significance of the obtained results lies in their potential use for improving State policy in the field of critical infrastructure, developing spatial development and territorial security strategies, as well as implementing the Build Back Better principles in the post-war reconstruction of Ukraine's economy, taking into account the objectives of increasing the resilience and adaptability of infrastructure systems.

Keywords: *national economy, critical infrastructure, spatial dimension, system-network approach, intersectoral interdependencies, risk-oriented approach, resilience, threats, cascading effects, infrastructure security, risk management, Build Back Better principle,*

Fig.: *4.* ***Tabl.:*** *4.* ***Bibl.:*** *40.*

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. Сучасний етап розвитку національних економік характеризується зростанням уразливості базових систем життєзабезпечення, що зумовлено поєднанням воєнних загроз, кліматичних змін, техногенних ризиків, цифровізації та поглибленням міжсекторальних взаємозалежностей соціально-економічних процесів. За таких умов особливого значення набуває критична інфраструктура, порушення функціонування якої здатне спричиняти масштабні економічні, соціальні та безпекові наслідки, що виходять далеко за межі окремих секторів або територій [1–3].

За оцінками міжнародних організацій, збої в роботі інфраструктурних систем мають виражений мультиплікативний характер і призводять до значних втрат у виробництві, логістиці, фінансовій сфері та соціальній інфраструктурі [1–5]. Світовий банк та Організація економічного співробітництва та розвитку наголошують, що зростання складності й взаємопов'язаності інфраструктурних мереж істотно підвищує ризики каскадних відмов, які знижують загальну стійкість економік до криз і шоків [4; 5].

За експертними оцінками, глобальні економічні втрати, пов'язані з руйнуванням або деградацією інфраструктури внаслідок воєнних конфліктів, природних катастроф і надзвичайних ситуацій, обчислюються сотнями мільярдів доларів США щорічно, тоді як непрямі втрати в окремих країнах можуть досягати 2–10% валового внутрішнього продукту [4–6].

Додатковим чинником зростання вразливості критичної інфраструктури є підвищення частоти та масштабів надзвичайних подій. За даними Управління ООН зі зниження ризику лих [3], кількість великих катастроф у світі з початку 1990-х років зросла понад у чотири рази, що значною мірою пов'язано з кліматичними змінами, урбанізацією та

посиленням техногенного навантаження на інфраструктурні мережі. Паралельно з цим зростає роль кіберзагроз: щорічні глобальні економічні втрати від кібератак, спрямованих на об'єкти критичної інфраструктури, перевищують 150 млрд дол. США, а кількість суб'єктів господарювання, що зазнають суттєвих збоїв унаслідок кіберінцидентів, демонструє стійку тенденцію до зростання [2].

Особливої гостроти зазначені проблеми набувають в умовах повоєнного відновлення, коли критична інфраструктура розглядається не лише як об'єкт фізичної реконструкції, а як базова передумова відновлення економічної активності, забезпечення доступу населення до життєво важливих послуг і стабілізації соціально-економічного середовища.

За оцінками міжнародних фінансових інституцій [7; 8], витрати на відновлення об'єктів критичної інфраструктури формують найбільшу частку загальних потреб у фінансуванні повоєнної реконструкції та модернізації економіки, тоді як відсутність чіткого концептуального підґрунтя для визначення критичності інфраструктурних об'єктів ускладнює процеси пріоритизації та знижує ефективність державної політики.

В українському контексті масштаби руйнувань критичної інфраструктури, насамперед енергетичної, транспортної та комунальної, є безпрецедентними. За результатами спільної оцінки Світового банку, Уряду України, Європейського Союзу та ООН [9], прямі інфраструктурні збитки станом на 2024 р. перевищили 100 млрд дол. США, з яких близько половини припадає на енергетичний сектор, а майже третина – на транспортну й логістичну інфраструктуру. Це актуалізує потребу в науково обґрунтованому підході до ідентифікації та управління критичною інфраструктурою з урахуванням просторових, мережевих і ризикових характеристик.

Попри широке використання терміна «критична інфраструктура» у науковому, нормативно-правовому та управлінському дискурсі, його змістовне наповнення залишається неоднозначним. У різних країнах і наукових школах це поняття трактується по-різному, що зумовлено відмінностями безпекових пріоритетів, рівня соціально-економічного розвитку, територіальної організації та історичних умов формування інфраструктурних систем [10–12]. Відсутність узгодженого теоретичного підходу ускладнює міждержавні порівняння, формування спільних стандартів управління та інтеграцію просторового виміру в політику розвитку й відновлення територій.

З огляду на це, зростає наукова й практична потреба в систематизації теоретичних підходів до визначення сутності критичної інфраструктури з урахуванням міжнародного досвіду, просторових характеристик її розміщення та резильєнтнісної логіки розвитку. Саме поєднання міжнародного, просторового й резильєнтнісного вимірів дозволяє перейти від статичних класифікаційних трактувань до динамічного розуміння критичності як змінної характеристики, що формується під впливом багатовекторних загроз, мережевих взаємозалежностей і здатності систем забезпечувати безперервність та відновлення функцій.

Аналіз останніх досліджень і публікацій. Як свідчить аналіз джерел, сучасний науковий дискурс щодо критичної інфраструктури характеризується одночасно високою інтенсивністю досліджень і відсутністю уніфікованої дефініції цього поняття. Це ускладнює зіставлення результатів, вироблення порівнюваних критеріїв ідентифікації об'єктів, пріоритизацію їх захисту та формування політики резильєнтності.

Це підтверджується результатами бібліометричного аналізу публікацій, які проіндексовано у міжнародній наукометричній базі даних Scopus і сформовано за запитом TITLE-ABS-KEY ("Critical Infrastructure" and (Definition or Concept or Framework)). Для вибірки публікацій застосовувалися обмеження за типом документів (Article, Review), мовою (англійська), релевантними галузями знань (інженерія, соціальні науки, економіка й управління, науки про довкілля) та виключенням публікацій із афіліацією з російською федерацією.

Отримана вибірка у 1894 документи відображає стійке позиціонування проблематики на перетині безпекових студій, управління ризиками, інфраструктурного планування, кібербезпеки та відновлення. Водночас саме кількісне зростання публікацій не знімає ключової методологічної проблеми: понятійне «ядро» критичної інфраструктури залишається варіативним і залежить від національних пріоритетів, домінуючих загроз, рівня технологічного розвитку та інституційних практик управління [10].

Значний внесок у пояснення причин розбіжностей у трактуванні поняття зробили K. Smith та I. D. Wilson, які порівняли національні, нормативні та наукові підходи й показали, що навіть за наявності спільної «ядрової» логіки (критичність як умова функціонування суспільства та економіки) визначення суттєво відрізняються за акцентами: від секторально-об'єктних переліків до наслідково-орієнтованих і мережево-залежних трактувань, що враховують взаємозалежності, уразливості та потенціал каскадних ефектів [10]. Така постановка питання має принципове значення для теорії, оскільки зміщує фокус із «важливості» сектора як такого на очікувані втрати від порушення функцій і на структурні залежності всередині інфраструктурних мереж, які здатні мультиплікувати наслідки збоїв [10]. Саме тому упродовж останнього десятиліття в літературі посилився перехід від підходів з визначення переліків секторів до системно-мережевих моделей критичної інфраструктури як складної соціо-технічної системи.

Найбільш чіткою системно-мережева логіка простежується у роботах, присвячених взаємозалежностям і каскадним відмовам. M. Ouyang [13] у ґрунтовному огляді з моделювання і симуляції взаємозалежних інфраструктур підкреслює, що критичність формується не властивостями ізольованого об'єкта, а структурою мережі, характером міжсекторальної взаємодії та масштабами соціально-економічних наслідків порушення функціонування. Розвиваючи цю логіку, E. Zio [14] акцентує, що аналіз уразливостей і ризику критичної інфраструктури потребує інтеграції різних перспектив моделювання, адже складність, невизначеність і нелінійність взаємодій роблять підходи недостатніми для обґрунтування рішень щодо захисту та підвищення стійкості.

Прикладом еволюції інструментарію є підхід F. Wang, J. J. Magoua та N. Li [15], які застосували HLA-ко-симуляцію

для відтворення каскадних відмов між доменними моделями різних секторів, що дозволяє більш реалістично аналізувати поширення збоїв і системні ризики на перетині інфраструктурних доменів. Важливо, що у межах системних досліджень дедалі чіткіше окреслюється і просторовий вимір критичності. Так, M. Ouyang [16] доводить, що просторово локалізовані атаки/впливи та «критичні локації» мережі можуть запускати різні траєкторії каскадних ефектів, а отже, критичність має виразний територіальний характер і не може бути адекватно описана без урахування географії вузлів, коридорів і зон концентрації ризиків.

Паралельно із системно-мережевими моделями сформувалася резильєнтнісна парадигма, у межах якої критична інфраструктура інтерпретується через здатність витримувати шоки, адаптуватися й відновлювати функції після порушень, забезпечуючи безперервність життєво важливих послуг. У систематичному огляді M. Sathurshan et al. [17] показано, що, попри швидке зростання кількості прикладних методик оцінювання резильєнтності, у науковому полі зберігаються розбіжності щодо атрибутів резильєнтності, наборів індикаторів і логіки оцінювання на різних фазах події (ex-ante, during, ex-post). Це ускладнює порівнянність результатів і пріоритизацію інвестицій у стійкість і резильєнтність [17].

Крім цього, у резильєнтнісному напрямку посилюється увага до відновлення як до керованого процесу модернізації, а не лише «повернення до попереднього стану». Саме цю ідею концептуалізує підхід Build Back Better («відбудувати краще» або «відбудувати з підвищенням стійкості»), який інтерпретує реконструкцію як можливість зменшити вразливості та підвищити адаптивність інфраструктурних систем у довгостроковій перспективі.

Публікація R. Der Sarkissian, Y. Diab, M. Vuillet [11] демонструє, що застосування Build Back Better до критичної інфраструктури вже має помітний перелік публікацій, однак потребує глибшої інтеграції у теоретичні моделі та дефініції, зокрема щодо критеріїв поліпшення відбудови, механізмів інституційного забезпечення та узгодження з рамками управління ризиками.

Суттєва частина новітніх досліджень зосереджується на цифровізації та кіберризиках, що трансформують розуміння критичної інфраструктури як кіберфізичної системи. У науковій праці P. Fountas et al. [18] узагальнено результати досліджень у сфері виявлення несанкціонованих вторгнень (intrusion detection) у критичних інфраструктурах і показано сталість фокусу на виявленні аномалій, шкідливого програмного забезпечення, механізмах автентифікації та застосуванні методів машинного навчання. При цьому підкреслюється, що інтелектуалізація кіберзахисту має поєднувати технологічні рішення із системним урахуванням взаємозалежностей і сценаріїв каскадування, оскільки саме каскадні наслідки визначають системну критичність [18].

Паралельно зростає кількість робіт, присвячених цифровим двійникам, моніторингу та data-driven підходам до управління надійністю, ризиками й відновленням інфраструктурних систем. Зокрема, G. Lampropoulos, X. Larrucea та R. Colomo-Palacios [19] показують потенціал цифрових двійників (digital twin) для ситуаційної обізнаності, прогнозування відмов і підтримки прийняття рішень у критичній інфраструктурі, водночас наголошуючи на бар'єрах інтероперабельності, якості даних і кіберстійкості цифрових контурів управління. У підсумку це зміщує дослідницький фокус від статичного розуміння інфраструктури до динамічного, у межах якого критичність дедалі частіше розглядається як змінна характеристика, що залежить від стану мережі, поточних ризиків і здатності системи до керованої адаптації.

Зазначені змістовні тенденції узгоджуються з бібліометричними картами, які побудовано у VOSviewer на основі вибірки Scopus. Карта співвживання ключових слів (*рис. 1*) засвідчує центральність терміна «критична інфраструктура» та її тісні (щільні) зв'язки з оцінюванням ризиків, безпекою, управлінням надзвичайними ситуаціями, змінами клімату, кібератаками та методами машинного навчання, що відображає домінування ризик-орієнтованої, безпекової та технологічної тематики у сучасних дослідженнях.

Для узагальнення тематичної структури дискурсу та її інтерпретації у контексті теоретичних підходів доцільно згрупувати ключові напрями у кластери (*табл. 1*).

Як видно з *табл. 1*, сучасні дослідження критичної інфраструктури мають виразно міждисциплінарний характер і розгортаються на стику інженерних, безпекових, екологічних та управлінських підходів. Узгодження ризик-орієнтованого, мережево-системного та резильєнтнісного бачення простежується у тому, що критичність дедалі частіше інтерпретується через наслідки порушення функцій, взаємозалежності та здатність системи протистояти шокам і відновлюватися [10; 13; 14; 17].

Одночасно посилення кібербезпекового й цифрового кластерів відображає кіберфізичну трансформацію критичної інфраструктури та розширення інструментарію (AI/ML, моніторинг, цифрові двійники) як для захисту, так і для управління ризиками та відновленням [18; 19]. Водночас просторовий аспект критичності, хоча й імпліцитно присутній у межах ризикових і системних досліджень, залишається менш формалізованим у термінах саме понятійно-категоріальних конструкцій, що є важливим сигналом для подальшого теоретичного узагальнення [16].

Слід зазначити, що часова візуалізація ключових слів (*рис. 2*) доповнює кластерний зріз, відображаючи еволюцію пріоритетів дискурсу упродовж 2018–2024 рр. У ранні періоди (з 2018 р.) більш вираженими є напрямки, які пов'язано з управлінням катастрофами, кліматичними ризиками та міжсекторальними взаємозалежностями (зокрема disaster management, climate change, interdependencies, water supply), що кореспондує із системними підходами до надійності та ризику [13; 16].

Починаючи з 2020–2021 рр. посилюється резильєнтнісна проблематика та логіка відновлення, включно з інтерпретацією реконструкції через Build Back Better [11; 17]. У 2022–2024 рр. пріоритетними стали теми кіберзагроз і цифрових рішень (cyber threats, IoT, machine learning, anomaly detection, authentication, digital twin), що відображає зміщення дослідницького фокусу до data-driven управління та кіберстійкості критичної інфраструктури [18; 19].

Загалом аналіз останніх досліджень і публікацій дозволяє констатувати: попри суттєвий прогрес у розвитку системно-мережевих, резильєнтнісних і цифрових під-

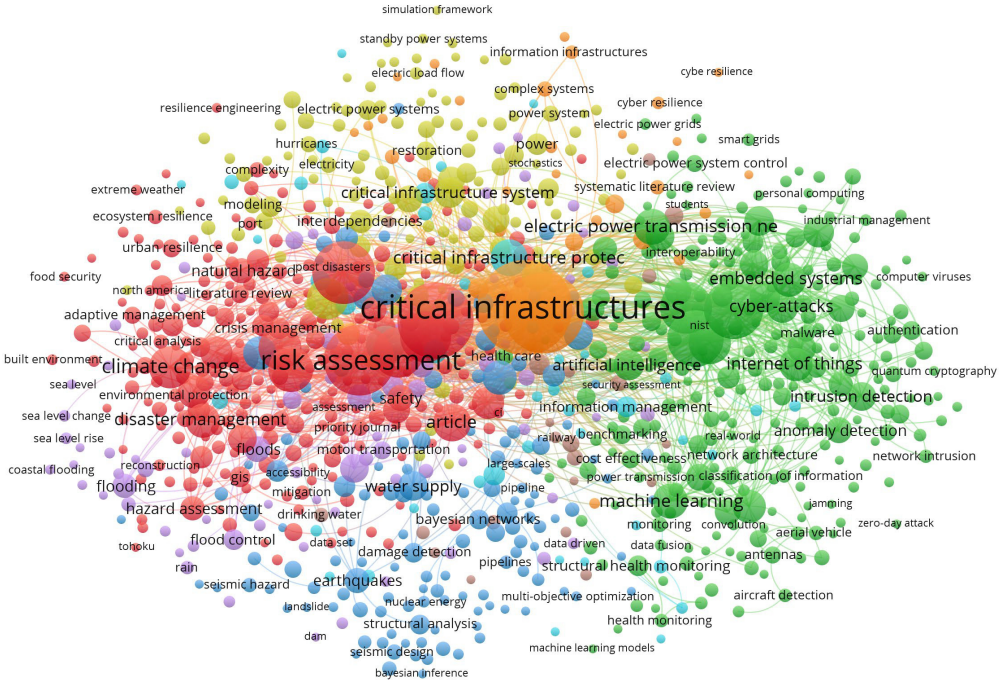

Рис. 1. Концептуальне поле досліджень критичної інфраструктури, сформоване на основі карти співвживання ключових слів у міжнародній наукометричній базі даних Scopus

Примітка: розмір вузлів відображає частоту використання ключових слів; кольори – тематичні кластери; зв'язки між вузлами – інтенсивність співвживання понять.

Джерело: побудовано авторами на основі бази даних Scopus з використанням програмного забезпечення VOSviewer

Таблиця 1

Тематичні кластери досліджень з питань розвитку критичної інфраструктури

Назва тематичного кластера	Домінуючі ключові терміни	Змістовна характеристика	Трактування критичної інфраструктури
Ризик-орієнтований кластер	Оцінювання ризиків, оцінювання небезпек, уразливість, безпека	Ідентифікація загроз, уразливостей та наслідків порушення функціонування, включно з каскадними ефектами	Критичність визначається масштабами потенційних втрат і системними наслідками відмов
Кластер кліматичних і природних загроз	Зміна клімату, повені, землетруси, управління надзвичайними ситуаціями, екстремальні погодні явища	Вплив кліматичних змін і природних катастроф на надійність та стійкість інфраструктурних систем	КІ як елемент адаптації територій до кліматичних / природних ризиків
Кібербезпековий кластер	Кібератаки, виявлення вторгнень, шкідливе програмне забезпечення, автентифікація, безпека	Кіберзагрози та захист цифрових компонентів КІ (кіберфізичні системи)	Критичність пов'язується з цифровою вразливістю та здатністю протистояти кібератакам
Інфраструктурно-секторальний кластер	Електроенергетичні системи, водопостачання, трубопроводи, передавальні мережі	Функціонування окремих інфраструктурних секторів і технічна надійність	КІ трактується через секторальну значущість та роль у життєзабезпеченні
Кластер цифровізації та інтелектуалізації	Машинне навчання, штучний інтелект, цифровий двійник, моніторинг, оптимізація	Інтелектуальні й data-driven технології для моніторингу, управління та прогнозування відмов	КІ як динамічна система, критичність якої залежить від якості управління та аналітики
Кластер резильєнтності та відновлення	Резильєнтність, відновлення, відбудова за принципом «краще, ніж було», адаптація	Адаптація, відновлення та забезпечення безперервності функцій після криз	Критичність пов'язується зі спроможністю підтримувати безперервність послуг у довгостроковій перспективі

Джерело: складено авторами на основі бібліометричного аналізу бази даних Scopus із використанням програмного забезпечення VOSviewer

Рис. 2. Часова динаміка ключових слів у дослідженнях критичної інфраструктури

Джерело: побудовано авторами на основі бази даних Scopus з використанням програмного забезпечення VOSviewer

ходів, у літературі зберігається концептуальна прогалина – просторовий вимір рівня критичності часто фігурує як контекст для аналізу ризиків або відновлення, але рідше стає повноцінним компонентом узагальнених дефініцій [16]. Навіть у роботах, де доведено роль «критичних локацій» у запуску каскадних ефектів, результати лише частково інтегруються у понятійно-категоріальні рамки критичної інфраструктури [16].

За цих умов подальша систематизація теоретичних підходів є доцільною у напрямі поєднання міжнародного (термінологічного, нормативно-правового), просторового (територіальна локалізація, вузли/коридори, нерівномірність доступу) та резильєнтісного (здатність «протистояти – адаптуватися – відновлюватися») вимірів як взаємопов'язаних складових єдиної концептуальної рамки, що узгоджує дефініцію з логікою системних ризиків, каскадних ефектів і вимогами Build Back Better [10; 11; 14; 16; 17].

Мета цього дослідження полягає в обґрунтуванні та систематизації наукових підходів до визначення сутності поняття «критична інфраструктура» з урахуванням міжнародного, просторового, резильєнтісного та ризик-орієнтованого вимірів, а також формулюванні інтегрованого авторського трактування критичної інфраструктури, релевантного для вирішення завдань повоєнної розбудови економіки України.

Досягнення поставленої мети забезпечено застосуванням комплексу загальнонаукових і спеціальних методів, що поєднують оглядово-узагальнену логіку з інструментами виявлення структури сучасного наукового дискурсу та зіставленням існуючих теоретичних підходів. Теоретико-методологічною та інформаційною базою дослідження слугували наукові публікації, які індексовано у міжнародних наукометричних базах даних (насамперед Scopus), а також міжнародні й національні нормативні документи, аналітичні звіти та офіційні матеріали інституцій ЄС і НАТО, а також органів державної влади окремих країн.

На першому етапі дослідження застосовано бібліометричний аналіз, який дозволив ідентифікувати основні напрями розвитку наукового дискурсу щодо критичної інфраструктури, визначити домінуючі тематичні поля та простежити еволюцію дослідницьких акцентів у часовому вимірі. Використання інструментів візуалізації бібліометричних даних забезпечило можливість виокремлення ключових концептів і категорій, що формують сучасні підходи до розуміння критичності інфраструктурних систем, а також підвищило обґрунтованість подальшої теоретичної систематизації.

На другому етапі, з метою узагальнення та впорядкування підходів до сутності критичної інфраструктури, використано методи аналізу й синтезу, абстрагування та узагальнення, а також логіко-структурний метод. Це дало змогу виокремити та систематизувати функціональний, наслідково-орієнтований, системно-мережевий, просторовий, ризик-орієнтований і резильєнтісний підходи, а також уточнити їх понятійні акценти та рамки застосування. Для зіставлення трактувань критичної інфраструктури у нормативних джерелах різних юрисдикцій застосовано порівняльний метод, що дозволило виявити спільні елементи дефініцій, відмінності у критеріях критичності та

концептуальні прогалини у національних і наднаціональних підходах.

Дослідження просторового виміру критичної інфраструктури здійснено з використанням системного та територіально-функціонального підходів, які забезпечили розгляд інфраструктурних об'єктів як елементів просторово локалізованих мереж, критичність яких визначається не лише галузевою належністю, а й роллю у забезпеченні життєво важливих послуг, мережевою вузловістю, концентрацією потоків, міжсекторними взаємозалежностями та територіальною нерівномірністю доступу до інфраструктурних сервісів.

Ризик-орієнтований підхід застосовано для обґрунтування динамічного характеру критичності, що змінюється під впливом багатовекторних загроз (воєнних, техногенних, кліматичних і кіберризиків), а також потенціалу каскадних ефектів у взаємопов'язаних інфраструктурних мережах.

Методологічним підґрунтям формулювання авторського трактування поняття «критична інфраструктура» став інтеграційний підхід, який поєднує результати бібліометричного узагальнення, теоретичної систематизації та міжнародного порівняння з просторовою інтерпретацією критичності й резильєнтісною логікою забезпечення безперервності та відновлюваності функцій. Додатково враховано принципи Build Back Better (відбудови з підвищенням стійкості) як рамку відбудови, що орієнтує реконструкцію інфраструктури не лише на відновлення потужностей, а й на зниження вразливостей, підвищення адаптивності та довгострокової стійкості територій. Застосування зазначеної методології сформувало наукове підґрунтя для вироблення інтегрованої концептуальної рамки критичної інфраструктури та визначення напрямів її використання у державній політиці та просторовому плануванні в умовах повоєнної відбудови економіки України.

Викладення основного матеріалу дослідження. Як показує аналіз, множинність трактувань поняття «критична інфраструктура» (КІ) у сучасній науковій і прикладній літературі зумовлена різницею дослідницьких оптик і практичних завдань: від нормативної ідентифікації об'єктів та формування переліків – до управління ризиками, міжсекторальними взаємозалежностями, резильєнтністю, відновленням і трансформацією інфраструктурних систем у посткризових умовах [13; 20–23; 24]. Унаслідок цього критичність дедалі частіше інтерпретується не як статична ознака сектора чи окремого активу, а як динамічний результат поєднання функціональної незамінності, мережевої ролі елементів, їхніх уразливостей та масштабу наслідків відмов, включно з каскадними ефектами, що поширюються через міжсекторальні ланцюги постачання й управління [13; 20–23; 24]. Такий зсув у розумінні критичної інфраструктури є принципово важливим для країн, що перебувають в умовах багатовекторних загроз, оскільки підсилює потребу переходу від логіки визначення переліку об'єктів до логіки безперервності, відновлюваності та адаптивності інфраструктурних послуг у просторі [23; 25; 26].

Узагальнення наукових джерел і практик державного управління [13; 21; 22; 25; 28] дозволяє констатувати, що наявні підходи до визначення критичної інфраструктури, як правило, розглядаються ізольовано – через окремі об'єктні, функціональні, наслідкові або ризик-орієнтовані ракурси.

Водночас у літературі бракує систематизованого бачення, яке б відображало логіку еволюції цих підходів, їх методологічні обмеження та можливості інтеграції у завданнях управління і повоєнного відновлення.

У зв'язку з цим у статті запропоновано авторську типологію підходів до визначення критичної інфраструктури (*табл. 2*), яку побудовано не за принципом переліку, а за принципом зміни фокусу критичності – від ідентифікації об'єктів і секторів до аналізу мережевих взаємозалежностей, ризиків, резильєнтності та трансформаційного відновлення.

Таблиця 2

Типологія підходів до визначення критичної інфраструктури

Підхід	Ключова логіка	Типові критерії критичності	Типові індикатори / ознаки	Обмеження
1	2	3	4	5
Об'єктно-секторальний	КІ як сукупність секторів/активів, «важливих за визначенням»	належність до визначеного сектору; формальні критерії державної класифікації	включення до переліку; регуляторний статус; категоризація об'єктів	слабко відображає взаємозалежності; критичність «не рухається» разом із контекстом загроз
Функціонально-сервісний	КІ як основа життєво важливих функцій і послуг	безперервність надання послуг; масштаб суспільних втрат від припинення	час допустимого простою; охоплення населення / економіки; незамінність сервісу	недостатньо пояснює каскадування та «чому саме тут» виникають системні відмови
Наслідковий (impact-based)	КІ через масштаб негативних наслідків відмови	рівень шкоди для безпеки, економіки, здоров'я/життя; поріг наслідків	«значний/руйнівний вплив»; втрати ВВП; ризики для життя; соціальна дестабілізація	часто слабко формалізує простір і механізми поширення відмов; залежить від методики оцінки впливу
Системно-мережевий	КІ як «система систем» з нелінійними залежностями	інтердепендентність, каскадні ефекти, роль вузлів у мережі	центральність вузлів; «single points of failure»; вузькі місця (bottlenecks); зв'язаність мереж	висока складність оцінювання; потреба у даних про мережеву топологію

Закінчення табл. 2

1	2	3	4	5
Ризик-орієнтований	Критичність як функція ризиків у конкретному контексті	загрози × уразливості × наслідки; сценарність	сценарії порушення; імовірність /частота; експозиція; очікувані збитки	чутливість до якості даних; складність порівняння територій без уніфікації метрик
Резильєнтніс-ний	КІ як чинник стійкості та відновлюваності	здатність витримувати, адаптуватися й відновлюватися; безперервність	time-to-recover; резервування; адаптаційні механізми; інституційна спроможність	фрагментарність метрик; різні рамки вимірювання резильєнтності
Просторовий	КІ як територіально локалізована мережа вузлів / коридорів / зон сервісу	просторове охоплення послуг; критичні вузли й коридори; територіальна нерівномірність ризиків	зони доступності; коридори постачання; агломераційні хаби; транскордонні зв'язки	недостатня формалізація у дефініціях; потреба у ГІС / просторових даних
Build Back Better (BBB)	Відновлення КІ як трансформація «краще, ніж було»	зниження вразливостей, модернізація, довгострокова стійкість	підсилення резервності; зміна розміщення; нові стандарти стійкості	концептуальна незрілість для КІ; ризик декларативності без інституційних механізмів

Джерело: складено авторами на основі опрацювання й узагальнення [13; 20–23; 25–27; 29–31]

Зміст *табл. 2* демонструє, що ранні дефініції критичної інфраструктури тяжіють до об'єктно-секторальної логіки, де критичність фіксується через належність до «критичних» секторів або формальне включення до переліку, що є зручним для регуляторної інвентаризації та побудови системи відповідальності [20; 21]. Водночас обмеженням такого підходу є те, що він слабко відображає міжсекторальні залежності й не враховує, що критичність може суттєво змінюватися залежно від конфігурації мереж, стану резервування, географії загроз та «вузьких місць» у ланцюгах постачання [13; 21; 22].

Тому логічним розвитком стала функціонально-сервісна перспектива, у якій центральним об'єктом аналізу є не актив, а результат – безперервність життєво важливих послуг та масштаб соціально-економічних втрат у разі їх припинення [21; 31]. Однак і цей підхід потребує доповнення системною логікою, оскільки сам собою не пояснює механізмів каскадування збоїв, коли локальна відмова перетворюється на міжсекторальну кризу через інтердепендентності [13; 21; 22].

Подальший розвиток дискурсу пов'язано із системно-мережевим підходом, у межах якого критична інфраструктура розглядається як «система систем», де критичність визначається не властивістю ізольованого елемента, а його роллю у топології мережі, характером взаємозалежностей та потенціалом каскадних ефектів. Це означає, що критичні елементи часто є «невидимими» у логіці визначення переліку (наприклад, вузол зв'язку чи підстанція певного рівня напруги), але саме вони можуть виступати точками системної відмови, якщо мають високу мережеву центральність або є вузькими місцями в коридорах постачання [13; 21; 22].

У цій логіці ризик-орієнтований підхід уточнює поняття критичності як контекстної змінної: вона залежить від спектра загроз (природних, техногенних, воєнних, кібернетичних), уразливостей, сценаріїв порушення функціонування та очікуваних збитків [21; 26; 29]. Отже, критичність доцільно трактувати як характеристику, що актуалізується внаслідок взаємодії ризиків і мережевих залежностей, а не як незмінну властивість сектора.

На цьому підґрунті сформувалася резильєнтнісна парадигма, у межах якої критична інфраструктура інтерпретується через здатність витримувати шоки, адаптуватися й відновлювати функції з забезпеченням безперервності критичних послуг [23; 26; 27]. Тут принципово, що резильєнтність виходить за межі технічної надійності та охоплює організаційні, інституційні, соціальні й економічні компоненти, включно з фазовістю управління подією (до, під час, після) [23; 26; 27].

У практичній площині це означає перехід від суто охоронної логіки до логіки «керованої стійкості», коли об'єктом політики стають не лише заходи захисту, а й відновлюваність, адаптація та трансформація інфраструктурних систем у довгостроковому горизонті [23; 24]. Саме у цій парадигмі формується концепція Build Back Better, що розглядає відновлення критичної інфраструктури як можливість знизити вразливості, підвищити резервність, перепроєктувати інфраструктурні рішення відповідно до майбутніх ризиків і забезпечити стійкість територій [22; 25].

Водночас аналіз джерел підкреслює, що застосування Build Back Better до критичної інфраструктури потребує подальшої концептуалізації, зокрема щодо критеріїв «покращення» та механізмів інституційного закріплення змін, аби уникнути ситуації, коли BBB залишається декларацією без вимірюваних результатів [22; 25].

Паралельно посилюється цифровий вимір критичності, оскільки критична інфраструктура дедалі частіше постає як кіберфізична система, у якій цифрові контури управління, промислові мережі, IoT-компоненти й інформаційна безпека стають визначальними чинниками системної стабільності [32; 33]. Кіберзагрози здатні виступати

тригерами порушень і каскадних ефектів, що переводить критичність із площини фізичного активу у площину керованості та кіберстійкості [32]. Водночас data-driven управління, цифрові двійники та інші інструменти підвищують ситуаційну обізнаність і якість прогнозування, але загострюють вимоги до інтероперабельності, якості даних і захищеності цифрових контурів, що має бути враховано при сучасних дефініціях і підходах до управління критичною інфраструктурою [33].

Логічним продовженням типології є міжнародний вимір (*табл. 3*), оскільки національні категорії, як правило, поєднують кілька підходів, але різняться тим, що саме розуміється під критичною інфраструктурою (актив / система / мережа / послуга) та за якою логікою фіксується «критичність» (функціональною, наслідковою, адміністративно-регуляторною, мережевою).

Для методично коректного зіставлення доцільно використовувати порівняльну матрицю, у якій відображаються: (1) об'єкт визначення; (2) домінуючий критерій критичності; (3) акценти на резильєнтності та безперервності; (4) включення віртуальних/цифрових компонентів; (5) роль взаємозалежностей [24; 30; 31; 34; 35].

Така матриця виступає методологічним ядром міжнародного аналізу, оскільки дозволяє перейти від описових дефініцій до зіставлення управлінських імплікацій: які системи підпадають під політику розвитку критичної інфраструктури, як задаються пріоритети та які інструменти управління ризиками й резильєнтністю формуються на їхній основі [24].

Інтерпретація *табл. 3* дозволяє зробити висновок, що більшість міжнародних підходів комбінують функціональну та наслідкову логіку, проте різняться тим, як саме визначають «поріг критичності», що включають у межі критичної інфраструктури та наскільки явно фіксують цифрові компоненти й міжсекторальні взаємозалежності [24; 30; 31; 34; 35].

Таблиця 3

Порівняльний аналіз міжнародних підходів до визначення критичної інфраструктури

Країна / інституція	Що розуміється під критичною інфраструктурою	Що розглядається під поняттям «критичність»	Практичний коментар для інтерпретації
ЄС	актив / система / частина; у сучасній рамці – критичні суб'єкти / послуги	істотний вплив у разі порушення, акцент на спроможності забезпечувати та відновлювати послуги	перехід від «охорони» до «continuity & recovery», релевантний для повоєнних трансформацій
США	фізичні та віртуальні системи й активи	«debilitating impact» на безпеку, економіку, здоров'я	поріг руйнівного впливу як механізм пріоритизації та концентрації ресурсів
Канада	процеси / системи / мережі / активи / послуги	необхідність для здоров'я, безпеки, добробуту та ефективності уряду, системної взаємозалежності	акцент на interdependencies та міжсекторальній координації як основі стійкості
Велика Британія	елементи інфраструктури / мережі / процеси	major detrimental impact на життєво важливі послуги / нацбезпеку	формула major detrimental impact означає «значний шкідливий вплив» і задає поріг серйозності наслідків
Німеччина	життєво важливі структури / об'єкти	стійкий дефіцит постачання та значні порушення суспільного порядку / безпеки	критерій «дефіциту постачання» прив'язує критичність до безперервності ланцюга
Франція	«життєва» інфраструктура	шкода нацбезпеці/ потенціалу / здоров'ю / життю	сильний безпековий акцент і складність заміни як неявного критерію
Італія	система / ресурс / процес / структура (у т. ч. віртуальна)	ослаблення нормального функціонування країни	широка рамка, придатна для кіберфізичної інфраструктури
Іспанія	стратегічні інфраструктури / системи базових сервісів	обмежені / відсутні альтернативи, суттєвий вплив	критерій «безальтернативності» корисний для пріоритизації інвестицій/ резервування
Польща	системи та функціонально пов'язані об'єкти / послуги	важливість для безпеки й функціонування держави	пряма прив'язка до інститутів і функціонування держави; широка предметність
Фінляндія	базові структури / послуги / функції	необхідність для життєвих функцій суспільства (security of supply)	логіка «стійкості постачання» добре узгоджується з резильєнтністю
Україна	об'єкти / суб'єкти, які пов'язано з процесами та/ або послугами	значущість для економіки й безпеки; негативний вплив на сектор національної безпеки та оборони, довкілля, життя/здоров'я	доцільно формалізувати мережеву роль, каскадність і просторові критерії для пріоритизації

Джерело: складено авторами на основі опрацювання [24; 30; 31; 34; 35]

Так, для США і Великої Британії характерне нормативне підсилення наслідковості через порогові формулювання впливу, які використовуються як інструмент пріоритизації (зокрема формула major detrimental impact – «значний шкідливий вплив», що вказує на високий рівень серйозності наслідків від порушення функціонування) [31; 35].

Для ЄС характерна еволюція до рамки резильєнтності критичних суб'єктів з акцентом на здатності забезпечувати та відновлювати послуги, що зближує дефініцію критичної інфраструктури з практикою управління ризиками й безперервністю надання сервісів [24]. Канада, своєю чергою, виразно підкреслює взаємозалежності як концептуальну вісь політики КІ, що є методологічно цінним для моделювання каскадних ефектів [34]. Важливим є й те, що окремі країни прямо розширюють межі критичної інфраструктури на віртуальні та цифрові компоненти (США, Італія, частково ЄС), що набуває особливої актуальності в умовах кіберфізичної трансформації інфраструктурних систем [30; 31; 33].

З огляду на завдання повоєнного відновлення України, міжнародний аналіз доцільно доповнювати просторовим виміром, оскільки територіальна конфігурація інфраструктурних мереж (вузли, коридори, зони доступності, транскордонні зв'язки) визначає масштаби наслідків порушень і можливості резервування. Попри те, що просторові аспекти імпліцитно присутні в поняттях «мережі» та «послуги», вони рідко формалізуються як елемент дефініції, хоча на практиці без просторового фокусу неможливо здійснити адресну пріоритизацію захисту, відновлення та інвестицій [13; 25; 28].

З метою методологічного усунення цієї прогалини доцільно виокремити просторові підходи, які можуть бути інтегровані в сучасне трактування критичної інфраструктури (*табл. 4*), оскільки саме вони дозволяють перейти від абстрактної критичності до конкретної карти управлінських рішень: де підсилювати резервування, які коридори дублювати, які вузли захищати першочергово та як перерозподіляти потужності для зниження територіальної експозиції до ризиків [13; 21; 22; 25; 29].

Таблиця 4

Просторові підходи до інтерпретації критичності інфраструктури

Просторовий підхід	Сутність просторової логіки критичності	Приклади елементів критичної інфраструктури	Прикладне значення для пріоритизації
Вузловий (nodal)	критичність формується через роль вузла як хаба мережі; відмова вузла спричиняє диспропорційні наслідки	підстанції, диспетчерські центри, транспортні хаби, вузли зв'язку/дата-центри	виявлення «single points of failure», концентрація захисту та резервування на вузлах
Коридорно-мережевий	критичність зумовлюється коридорами, перетинами, «bottlenecks», що забезпечують потокові зв'язки	енергомагістралі, логістичні маршрути, цифрові магістралі, перетини мереж	диверсифікація маршрутів, дублювання коридорів, підвищення зв'язаності
Територіально-сервісний (service-area)	критичність проявляється через зони доступності послуг і критичні прогалини забезпечення	ареали водопостачання, медичної доступності, покриття зв'язком	встановлення мінімальних стандартів послуг; адресне закриття прогалин
Ризико-територіальний	критичність залежить від експозиції території до загроз та можливості їх поширення мережею	зони воєнних, кліматичних, техногенних, кіберризиків	поєднання ризик-аналізу з просторовим плануванням і пріоритизацією інвестицій
BBB-просторовий	відновлення як оптимізація розміщення/потужностей для зниження уразливостей	перенесення/підсилення вузлів, дублювання потужностей, нові стандарти	перехід від «відтворення» до «стійкішої конфігурації» у довгостроковому горизонті

Джерело: складено авторами на основі опрацювання [13; 21; 22; 24; 25; 29–31]

Подальше узагальнення результатів теоретичного аналізу зумовлює необхідність їх інтеграції у єдину концептуальну рамку, здатну відобразити взаємозв'язок між різними підходами до визначення критичної інфраструктури. У зв'язку з цим у статті запропоновано інтегровану схему еволюції та поєднання теоретичних підходів до сутності критичної інфраструктури (*рис. 3*), яка демонструє причинно-наслідковий перехід від об'єктно-секторальних і функціональних трактувань до системно-мережевих, ризик-орієнтованих, резильєнтнісних і просторових підходів, а також логіку включення принципів Build Back Better як рамки трансформаційного відновлення в умовах повоєнних викликів.

Запропонована схема дозволяє перейти від описового порівняння підходів до прикладної логіки просторової пріоритизації заходів захисту, резервування та інвестицій у відновлення критичної інфраструктури. Як видно з *рис. 3*, об'єктно-секторальний підхід задає початкове поле ідентифікації (визначення того, які об'єкти слід вважати критично важливими та стратегічними); функціонально-сервісний – переводить фокус на безперервність надання послуг; системно-мережевий – пояснює механізми каскадування; ризик-орієнтований – інтерпретує критичність як контекстну й сценарну характеристику; резильєнтнісний – фіксує вимір «витримати – адаптуватися – відновити». А підхід Build Back Better підкреслює, що відновлення має бути

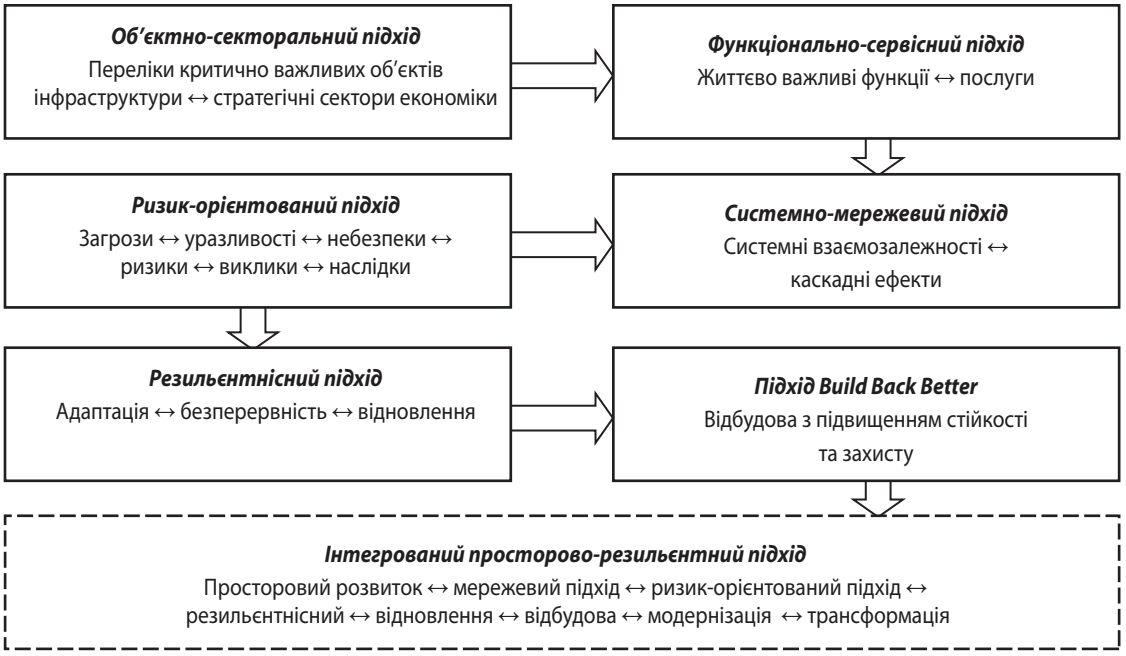

Рис. 3. Еволюція та інтеграція теоретичних підходів до сутності критичної інфраструктури

Джерело: побудовано авторами на основі [36–39]

спрямовано не на повернення до попереднього стану, а на зниження уразливостей і підвищення довгострокової стійкості [13; 20–23; 25–27].

Отже, *рис. 3* слід інтерпретувати як концептуальну схему еволюції підходів до розуміння критичної інфраструктури. Стрілки на схемі відображають не заміну одного підходу іншим, а послідовне нашарування та інтеграцію концептуальних логік, у межах яких критичність переходить від статичної ознаки належності до сектору чи об'єкта до динамічної характеристики, що формується через мережеві взаємозалежності, ризики, резильєнтність і просторовий контекст.

Центральне місце у схемі посідає інтегрований просторово-резильєнтнісний підхід, який синтезує попередні концептуальні рівні та орієнтований на прикладні завдання управління й повоєнного відновлення. У цьому підході критичність описується як характеристика територіально локалізованих вузлів і коридорів, що забезпечують надання послуг у межах зон обслуговування та водночас зазнають неоднорідної експозиції до ризиків [13; 21–22; 25; 28].

Окремого узагальнення потребує просторова модель, яка дає змогу перейти від концептуального розуміння критичності до прикладної логіки пріоритизації захисту та інвестицій у відновлення (*рис. 4*).

Даний рисунок відображає просторову модель інтерпретації критичної інфраструктури з позицій забезпечення резильєнтності економіки. Схему доцільно читати від мережевого ядра (вузли та коридори), що формує основу міжсекторальної та міжрегіональної зв'язаності, до зовнішніх контурів, які репрезентують зони надання послуг, територіальну експозицію до ризиків і резервні механізми безперервності.

Окремий контур Build Back Better інтерпретується як рамка трансформаційного відновлення, що задає напрям модернізації просторової конфігурації інфраструктури з метою зниження уразливостей і підвищення довгострокової стійкості [13; 21; 22; 24; 25; 29].

Така композиція моделі пояснює, що критичність у повоєнний період є просторово диференційованою: один і той самий тип інфраструктурного об'єкта може мати різний рівень критичності на різних територіях залежно від його мережевої ролі, наявності резервування та ризикового профілю [25; 28]. Водночас модель підкреслює, що управління критичною інфраструктурою має синхронізувати три контури рішень: де зосереджувати заходи захисту, де розгортати резервування і які елементи доцільно відновлювати трансформаційно, аби не відтворювати попередні вразливості [22; 25].

Як видно з *рис. 4*, у центрі моделі розташовано мережеве ядро, що складається з вузлів (енергетичні підстанції, диспетчерські центри, транспортні хаби, дата-центри, водозабори тощо) та коридорів (енергетичні, транспортні й цифрові магістралі), які забезпечують міжсекторальну та міжрегіональну зв'язаність. Саме роль вузлів у топології мережі визначає потенціал каскадних ефектів: відмова вузла з високою мережевою центральністю або критичного «перетину коридорів» здатна масштабувати збій на кілька секторів одночасно [13; 21; 22].

Наступним елементом моделі є контур зон обслуговування, який відображає просторове охоплення життєво важливими послугами територій і дозволяє інтерпретувати критичність через доступність та безперервність сервісів для населення й економіки, а також через виявлення «критичних прогалин» доступу [25; 31]. Далі формується контур зон ризиків – воєнних, кліматичних, техногенних і кібернетичних, які накладаються на мережеве ядро, підкреслюючи контекстність критичності та її залежність від територіальної експозиції до загроз [26; 29].

Рис. 4. Просторова модель розміщення і розвитку критичної інфраструктури для забезпечення резильєнтності економіки України

Джерело: побудовано авторами на основі [36–40]

Окремо в моделі виокремлено резервні контури (альтернативні маршрути, дублювання потужностей, тимчасові рішення забезпечення безперервності), що слугують інструментом зниження системних ризиків і скорочення часу відновлення. Завершальний BBB-контур відображає управлінські рішення щодо модернізації критично важливих об'єктів інфраструктури – зміцнення вузлів, оптимізацію розміщення, технологічне оновлення та підвищення стандартів стійкості, – які переводять відновлення з режиму «повернути як було» у режим «зробити стійкіше» [22; 25].

У сукупності наведена просторова модель формує концептуальну основу для переходу від концептуального осмислення критичності до прикладної логіки просторової пріоритизації захисних, резервних та відновлювальних рішень у системі управління критичною інфраструктурою.

Підсумовуючи, можна констатувати, що сучасна теорія та практика визначення критичної інфраструктури еволюціонували від статичних секторних трактувань до системних, ризик-орієнтованих, резильєнтнісних і трансформаційних підходів, у яких критичність визначається поєднанням функціональної незамінності, мережевої ролі, уразливостей і масштабів наслідків порушення функціонування [13; 21–23; 26; 27].

Водночас трактування критичної інфраструктури у різних країнах світу, як правило, недостатньо формалізують просторову складову критичності, хоча саме вона є принципово важливою для територіальної пріоритизації, резервування та планування відновлення в умовах повоєнних трансформацій [24; 25]. Це обґрунтовує доцільність інтегрованого просторово-резильєнтного трактування, у межах якого критична інфраструктура визначається як просторово локалізовані та мережево взаємозалежні системи, процеси й послуги, критичність яких проявляється через каскадні ефекти, ризики та здатність забезпечувати безперервність і відновлення.

Таким чином, під поняттям «критична інфраструктура» слід розуміти сукупність взаємопов'язаних матеріальних і нематеріальних систем, мереж, об'єктів, процесів і послуг, просторово локалізованих у межах певних територій і інтегрованих у міжсекторальні та міжрегіональні взаємозалежності, функціонування яких є визначальним для забезпечення життєво важливих функцій суспільства, резильєнтності економіки та безпеки держави, а порушення або деградація яких під впливом воєнних, техногенних, природних чи кіберзагроз здатні спричиняти значні соціально-економічні та безпекові наслідки, просторово диференційовані за масштабом і конфігурацією каскадних ефектів.

Висновки. У результаті проведеного дослідження встановлено, що поняття критичної інфраструктури у сучасному науковому та нормативному дискурсі характеризується значною концептуальною варіативністю, що зумовлено відмінностями національних моделей безпеки, соціально-економічної структури країн, рівня розвитку інфраструктурних систем та актуальності ризиків.

Аналіз наукових публікацій, міжнародних документів і національних практик країн ЄС, НАТО та України засвідчив домінування функціонального, наслідково-орієнтованого та системно-мережевого підходів до визначення критичної інфраструктури, водночас просторовий і резильєнтнісний виміри здебільшого залишаються імпліцитними або представленими фрагментарно, без належної операціоналізації в управлінських рішеннях.

Проведена систематизація підходів дозволила обґрунтувати, що жоден із наявних концептуальних підходів не є самодостатнім для розв'язання завдань управління, розвитку та повоєнного відновлення критичної інфраструктури. У сучасних умовах критичність інфраструктури формується не лише через її функціональну значущість або масштаб потенційних наслідків відмови, а й через просторову роль у мережевих структурах, рівень міжсекторальних взаємозалежностей, територіальну концентрацію ризиків та здатність систем до адаптації й відновлення. Це підтверджує доцільність переходу від статичних класифікаційних трактувань до динамічного розуміння критичності як змінної характеристики, що актуалізується у конкретному просторово-мережевому та ризиковому контексті.

Наукова новизна дослідження полягає в обґрунтуванні та формулюванні інтегрованого трактування критичної інфраструктури, яке поєднує просторовий, резильєнтнісний і ризик-орієнтований підходи. Запропоноване авторське визначення дозволяє розглядати критичну інфраструктуру як динамічну соціо-технічну систему, критичність якої є змінною характеристикою, що залежить від ролі об'єктів у територіальних мережах, потенціалу каскадних ефектів та спроможності інфраструктурних систем забезпечувати безперервність функціонування і відновлення в умовах багатовекторних загроз. Такий підхід є принципово важливим для держав із високим рівнем територіальної неоднорідності та підвищеними безпековими ризиками, зокрема для України у повоєнний період.

Практичне значення отриманих результатів полягає у можливості їх використання для вдосконалення державної політики у сфері розвитку критичної інфраструктури та повоєнної відбудови.

Для органів державної влади обґрунтованим є перехід від суто класифікаційного підходу до інтегрованої моделі управління критичною інфраструктурою, яка враховує просторову локалізацію об'єктів, їхню роль у міжрегіональних і міжсекторальних мережах, рівень ризиків та потенційні каскадні ефекти. Це створює методологічне підґрунтя для більш обґрунтованої пріоритизації захисних і відновлювальних заходів, а також для узгодження національної політики з європейськими та євроатлантичними підходами до забезпечення резильєнтності.

Для органів регіональної та місцевої влади результати дослідження можуть бути використані під час інтеграції питань критичної інфраструктури у документи просторового планування, стратегії регіонального розвитку та плани відновлення територій. Урахування вузлово-мережевої логіки, зон обслуговування та територіальної експозиції до ризиків дозволяє підвищити обґрунтованість управлінських рішень, зменшити ймовірність виникнення системних збоїв та підвищити стійкість надання життєво важливих послуг у межах регіонів і громад.

Для операторів об'єктів критичної інфраструктури запропонований підхід формує методологічну основу для впровадження ризик-орієнтованого та резильєнтнісного управління, зокрема шляхом розвитку резервних контурів, диверсифікації мереж і підвищення адаптивної спроможності інфраструктурних систем. У контексті повоєнної відбудови це сприяє практичній реалізації принципів Build Back Better, орієнтованих не лише на відновлення втрачених потужностей, а й на довгострокове зниження структурних уразливостей.

Для міжнародних партнерів України результати дослідження можуть слугувати аналітичною основою для узгодження програм технічної допомоги та інвестицій у відновлення критичної інфраструктури з урахуванням просторових і мережевих особливостей країни. Інтеграція запропонованого підходу у спільні проєкти сприятиме підвищенню ефективності використання ресурсів та посиленню стійкості інфраструктурних систем у регіональному й транскордонному вимірах.

Отже, виходячи з вищевикладеного можна зазначити, що отримані результати мають важливі імплікації для формування державної політики у сфері розвитку та повоєнного відновлення критичної інфраструктури. По-перше, доцільним є перехід від секторальних підходів до інтегрованої моделі управління, що ґрунтується на просторовій пріоритизації, оцінюванні ризиків і мережевих взаємоза-

лежностей. По-друге, результати дослідження обґрунтовують необхідність синхронізації політики захисту, резервування та відновлення інфраструктури в межах єдиної резильєнтнісної рамки. По-третє, інтеграція принципів Build Back Better у політику відбудови дозволяє зменшити структурні уразливості та підвищити довгострокову стійкість територій, що є критично важливим для України в умовах повоєнних трансформацій та європейської інтеграції.

Перспективи подальших досліджень пов'язані з розробленням системи кількісних і просторово-орієнтованих індикаторів критичності, що дозволять інтегрувати функціональну значущість інфраструктурних об'єктів із їх роллю у мережевих структурах, рівнем міжсекторальних взаємозалежностей і територіальною експозицією до воєнних, кліматичних, техногенних загроз і кіберризиків. Важливим науково-методологічним напрямом є обґрунтування моделей оцінювання каскадних ефектів порушення функціонування критичної інфраструктури з урахуванням просторової динаміки поширення збоїв між секторами економіки та регіонами, що створює підґрунтя для прикладного аналізу системних ризиків і пріоритизації рішень з відбудови.

ЛІТЕРАТУРА

1. Good Governance for Critical Infrastructure Resilience. Paris: Organisation for Economic Co-operation and Development, 2019. 108 p. URL: https://www.oecd.org/gov/good-governance-for-critical-infrastructure-resilience.htm

2. The Global Risks Report 2024. 19th ed. Geneva : World Economic Forum, 2024. 98 p. URL: https://www.weforum.org/publications/global-risks-report-2024

3. Global Assessment Report on Disaster Risk Reduction 2023. Geneva : United Nations Office for Disaster Risk Reduction (UNDRR), 2023. 214 p. URL: https://www.undrr.org/publication/global-assessment-report-disaster-risk-reduction-2023

4. Lifelines: The Resilient Infrastructure Opportunity. Washington, DC : World Bank, 2019. 212 p.
DOI: https://doi.org/10.1596/978-1-4648-1430-3

5. Building Resilient Infrastructure for Sustainable Development. Paris: Organisation for Economic Co-operation and Development (OECD), 2018. 168 p. URL: https://www.oecd.org/environment/cc/building-resilient-infrastructure-for-sustainable-development.htm

6. The Sustainable Development Goals Report 2024. New York : United Nations, 2024. 72 p. URL: https://unstats.un.org/sdgs/report/2024

7. Rebuilding for Resilience: Infrastructure Recovery after Conflict. Washington, DC : World Bank, 2022. 156 p. URL: https://openknowledge.worldbank.org/handle/10986/37735

8. Recovery and Resilience Facility. Brussels: European Commission, 2023. 124 p. URL: https://economy-finance.ec.europa.eu/eu-recovery-instruments/recovery-and-resilience-facility_en

9. Ukraine Rapid Damage and Needs Assessment (RDNA4). Washington, DC : World Bank, 2024. 380 p. URL: https://www.worldbank.org/en/country/ ukraine/publication/rdna4

10. Smith K., Wilson I. D. Critical infrastructures: a comparison of definitions. *International Journal of Critical Infrastructures*. 2023. Vol. 19. No. 4. P. 323–339.
DOI: https://doi.org/10.1504/IJCIS.2023.132213

11. Der Sarkissian R., Diab Y., Vuillet M. The "Build-Back-Better" concept for reconstruction of critical infrastructure: A review. *Safety Science*. 2023. Vol. 157. Article 105932.
DOI: https://doi.org/10.1016/j.ssci.2022.105932

12. Sathurshan M., Gohari S., Bagchi A., Mostafavi A. Resilience of critical infrastructure systems: A systematic literature review of measurement frameworks. *Infrastructures*. 2022. Vol. 7. No. 5. Article 67.
DOI: https://doi.org/10.3390/infrastructures7050067

13. Ouyang M. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*. 2014. Vol. 121. P. 43–60.
DOI: https://doi.org/10.1016/j.ress.2013.06.040

14. Zio E. Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety*. 2016. Vol. 152. P. 137–150.
DOI: https://doi.org/10.1016/j.ress.2016.02.009

15. Wang F., Magoua J. J., Li N. Modeling cascading failure of interdependent critical infrastructure systems using HLA-based co-simulation. *Automation in Construction*. 2022. Vol. 133. Article 104008.
DOI: https://doi.org/10.1016/ j.autcon.2021.104008

16. Ouyang M. Critical location identification and vulnerability analysis of interdependent infrastructure systems under spatially localized attacks. *Reliability Engineering & System Safety*. 2016. Vol. 154. P. 106–116.
DOI: https://doi.org/10.1016/j.ress.2016.05.007

17. Sathurshan M., Saja A., Thamboo J., Haraguchi M., Navaratnam S. Resilience of Critical Infrastructure Systems: A Systematic Literature Review of Measurement Frameworks. *Infrastructures*. 2022. Vol. 7. No. 5. Article 67.
DOI: https://doi.org/10.3390/infrastructures7050067

18. Fountas P., Tsiakos K., Gkonis K., Fylakis M. A., Menis M. Intrusion Detection in Critical Infrastructures: A Literature Review. *Smart Cities*. 2021. Vol. 4. No. 3. P. 1146–1157.
DOI: https://doi.org/10.3390/smartcities4030061

19. Lampropoulos G., Larrucea X., Colomo-Palacios R. Digital Twins in Critical Infrastructure. *Information*. 2024. Vol. 15. No. 8. Article 454.
DOI: https://doi.org/10.3390/info15080454

20. Dunn M., Wigert I. International CI protection policy and research: A state of the art. Stockholm : Swedish Defence Research Agency (FOI), 2004. 82 p.

21. Pederson P., Dudenhoeffer D., Hartley S., Permann M. Critical infrastructure interdependency modeling: A survey of U.S. and international research. Idaho Falls : Idaho National Laboratory, 2006. 116 p.

22. Buldyrev S. V., Parshani R., Paul G., Stanley H. E., Havlin S. Catastrophic cascade of failures in interdependent networks. *Nature*. 2010. Vol. 464. P. 1025–1028.
DOI: https://doi.org/10.1038/nature08932

23. Bruneau M., Chang S. E., Eguchi R. T. et al. A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra*. 2003. Vol. 19. No. 4. P. 733–752.
DOI: https://doi.org/10.1193/1.1623497

24. European Parliament and Council of the European Union. Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities. *Official Journal of the European Union*. 2022. L 333. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557

25. United Nations Office for Disaster Risk Reduction. Build Back Better in Recovery, Rehabilitation and Reconstruction: Sendai Framework Guidance. Geneva : UNDRR, 2017. 52 p. URL:

https://www.undrr.org/publication/build-back-better-recovery-rehabilitation-and-reconstruction

26. International Organization for Standardization. ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements. Geneva : ISO, 2019. 34 p. URL: https://www.iso.org/standard/75106.html

27. North Atlantic Treaty Organization. Baseline Requirements for National Resilience: policy baseline and guidance materials. Brussels : NATO, 2016-2023. URL: https://www.nato.int/cps/en/natohq/topics_132722.htm

28. Rinaldi S. M., Peerenboom J. P., Kelly T. K. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*. 2001. Vol. 21. No. 6. P. 11–25.

DOI: https://doi.org/10.1109/37.969131

29. International Organization for Standardization. ISO 31000:2018 Risk management – Guidelines. Geneva : ISO, 2018. 16 p. URL: https://www.iso.org/standard/65694.html

30. Council of the European Union. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Official Journal of the European Union*. 2008. L 345. P. 75–82. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114

31. The White House. Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience. Washington, DC, 2013. 8 p. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security

32. Ahmed C. M., Mathur A. P., Fulmer H. et al. Challenges and approaches for intrusion detection in industrial control systems. *IEEE Communications Surveys & Tutorials*. 2018. Vol. 20. No. 3. P. 2152–2175.

DOI: https://doi.org/10.1109/COMST.2018.2791584

33. Tao F., Zhang H., Liu A., Nee A. Y. C. Digital twin in industry: State-of-the-art. *IEEE Transactions on Industrial Informatics*. 2019. Vol. 15. No. 4. P. 2405–2415.

DOI: https://doi.org/10.1109/TII.2018.2873186

34. Public Safety Canada. National Strategy for Critical Infrastructure. Ottawa : Government of Canada, 2009. 16 p. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx.

35. Critical National Infrastructure (CNI): policy framework and guidance materials. London : UK Government, 2010-2023. URL: https://www.gov.uk/government/collections/critical-national-infrastructure.

36. 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: https://doi.org/10.32983/2222-4459-2022-12-58-78

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

DOI: https://doi.org/10.32983/2222-4459-2023-7-30-41

38. Хаустова В. Є., Трушкіна Н. В., Проноза П. В. Ідентифікація елементів критичної інфраструктури: закордонний і вітчизняний досвід. *Бізнес Інформ*. 2025. № 8. С. 47–71.

DOI: https://doi.org/10.32983/2222-4459-2025-8-47-71

39. Хаустова В. Є., Трушкіна Н. В. Загрози розвитку критичної інфраструктури: сутність і класифікація. *Проблеми економіки*. 2025. № 3. С. 89–104.

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

40. Bezpartochnyi M., Khaustova V., Trushkina N. Investment support for the critical infrastructure development of territorial communities in the conditions of post-war reconstruction of the Ukrainian economy. *Adaptation mechanisms of socio-economic systems to global changes and challenges: resource-efficient technologies, environmental protection, security, sustainable development*: scientific monograph. Plovdiv : Higher School of Security and Economics Publishing Complex, 2024. P. 173–193.

DOI: https://doi.org/10.5281/zenodo.12519297

REFERENCES

Ahmed C. M., Mathur A. P. & Fulmer H. (2018). Challenges and approaches for intrusion detection in industrial control systems. *IEEE Communications Surveys & Tutorials*, 3(20), 2152–2175. https://doi.org/10.1109/COMST.2018.2791584

Bezpartochnyi M., Khaustova V. & Trushkina N. (2024). *Investment support for the critical infrastructure development of territorial communities in the conditions of post-war reconstruction of the Ukrainian economy*. Plovdiv: Higher School of Security and Economics Publishing Complex. https://doi.org/10.5281/zenodo.12519297

Bruneau M., Chang S. E. & Eguchi R. T. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra*, 4(19), 733–752. https://doi.org/10.1193/1.1623497

Buldyrev S. V., Parshani R., Paul G., Stanley H. E. & Havlin S. (2010). Catastrophic cascade of failures in interdependent networks. *Nature*, 464, 1025–1028. https://doi.org/10.1038/nature08932

Council of the European Union. (2008, December 8). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114

Der Sarkissian R., Diab Y. & Vuillet M. (2023). The "Build-Back-Better" concept for reconstruction of critical infrastructure: A review. *Safety Science*, 157, 105932. https://doi.org/10.1016/j.ssci.2022.105932

Dunn M. & Wigert I. (2004). *International CI protection policy and research*: A state of the art. Stockholm: Swedish Defence Research Agency (FOI).

European Commission (2023). *Recovery and Resilience Facility*. Brussels: European Commission. https://economy-finance.ec.europa.eu/eu-recovery-instruments/recovery-and-resilience-facility_en

European Parliament & Council of the European Union. (2022, December 14). Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities. *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557

Fountas P., Tsiakos K., Gkonis K., Fylakis M. A. & Menis M. (2021). Intrusion Detection in Critical Infrastructures: A Literature Review. *Smart Cities*, 3(4), 1146–1157. https://doi.org/10.3390/smartcities4030061

ISO (2018). ISO 31000:2018 Risk management – Guidelines. Geneva: ISO. https://www.iso.org/standard/65694.html

ISO (2019). ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements. Geneva: ISO. https://www.iso.org/standard/75106.html

Khaustova V. Ye. & Reshetniak O. I. (2023). Rezylientnist ekonomiky: sutnist i vyklyky dlia Ukrainy [Economic resilience: es-

sence 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. (2025). Zahrozy rozvytku krytychnoi infrastruktury: sutnist i klasyfikatsiia [Threats to critical infrastructure development: essence and classification]. *Problemy ekonomiky*, 3, 89–104. https://doi.org/10.32983/2222-0712-2025-3-89-104

Khaustova V. Ye., Trushkina N. V. & Pronoza P. V. (2025). Identyfikatsiia elementiv krytychnoi infrastruktury: zakordonnyi i vitchyznianyi dosvid [Identification of critical infrastructure elements: foreign and domestic experience]. *Biznes Inform*, 8, 47–71. https://doi.org/10.32983/2222-4459-2025-8-47-71

Kyzym M. O., Khaustova V. Ye. & Trushkina N. V. (2022). Sutnist poniattia «krytychna infrastruktura» z pozytsii natsionalnoi bezpeky Ukrainy [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

Lampropoulos G., Larrucea X. & Colomo-Palacios R. (2024). Digital Twins in Critical Infrastructure. *Information*, 8(15), 454. https://doi.org/10.3390/info15080454

NATO. Baseline Requirements for National Resilience: policy baseline and guidance materials. https://www.nato.int/cps/en/natohq/topics_132722.htm

Organisation for Economic Co-operation and Development (2019). Good Governance for Critical Infrastructure Resilience. Paris: Organisation for Economic Co-operation and Development. https://www.oecd.org/gov/good-governance-for-critical-infrastructure-resilience.htm

Organisation for Economic Co-operation and Development (OECD) (2018). Building Resilient Infrastructure for Sustainable Development. Paris: Organisation for Economic Co-operation and Development (OECD). https://www.oecd.org/environment/cc/building-resilient-infrastructure-for-sustainable-development.htm

Ottawa : Government of Canada, Public Safety Canada. (2009). National Strategy for Critical Infrastructure. https://www.publicsafety.gc.ca/cnt/ rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx

Ouyang M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, 121, 43–60. https://doi.org/10.1016/j.ress.2013.06.040

Ouyang M. (2016). Critical location identification and vulnerability analysis of interdependent infrastructure systems under spatially localized attacks. *Reliability Engineering & System Safety*, 154, 106–116. https://doi.org/10.1016/j.ress.2016.05.007

Pederson P., Dudenhoeffer D., Hartley S. & Permann M. (2006). *Critical infrastructure interdependency modeling: A survey of U.S. and international research*. Idaho Falls: Idaho National Laboratory.

Rinaldi S. M., Peerenboom J. P. & Kelly T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 6(21), 11–25. https://doi.org/10.1109/37.969131

Sathurshan M., Saja A., Thamboo J., Haraguchi M. & Navaratnam S. (2022). Resilience of Critical Infrastructure Systems: A Systematic Literature Review of Measurement Frameworks. *Infrastructures*, 5(7), 67. https://doi.org/10.3390/infrastructures7050067

Sathurshan M., Gohari S., Bagchi A. & Mostafavi A. (2022). Resilience of critical infrastructure systems: A systematic literature review of measurement frameworks. *Infrastructures*, 5(7), 67. https://doi.org/10.3390/infrastructures7050067

Smith K. & Wilson I. D. (2023). Critical infrastructures: a comparison of definitions. *International Journal of Critical Infrastructures*, 4(19), 323–339. https://doi.org/10.1504/IJCIS.2023.132213

Tao F., Zhang H., Liu A. & Nee A. Y. C. (2019). Digital twin in industry: State-of-the-art. *IEEE Transactions on Industrial Informatics*, 4(15), 2405–2415. https://doi.org/10.1109/TII.2018.2873186

UK Government. Critical National Infrastructure (CNI): policy framework and guidance materials. https://www.gov.uk/government/collections/critical-national-infrastructure

UNDRR (2017). Build Back Better in Recovery, Rehabilitation and Reconstruction: Sendai Framework Guidance. Geneva: UNDRR. https://www.undrr.org/publication/build-back-better-recovery-rehabilitation-and-reconstruction

United Nations (2024). The Sustainable Development Goals Report 2024. New York: United Nations. https://unstats.un.org/sdgs/report/2024

United Nations Office for Disaster Risk Reduction (UNDRR) (2023). Global Assessment Report on Disaster Risk Reduction 2023. Geneva: United Nations Office for Disaster Risk Reduction (UNDRR). https://www.undrr.org/publication/global-assessment-report-disaster-risk-reduction-2023

Wang F., Magoua J. J. & Li N. (2022). Modeling cascading failure of interdependent critical infrastructure systems using HLA-based co-simulation. *Automation in Construction*, 133, 104008. https://doi.org/10.1016/j.autcon.2021.104008

Washington, DC: The White House. (2013). Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience. https://obamwhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security

World Bank (2019). Lifelines: The Resilient Infrastructure Opportunity. Washington, DC: World Bank. https://doi.org/10.1596/978-1-4648-1430-3

World Bank (2022). Rebuilding for Resilience: Infrastructure Recovery after Conflict. Washington, DC: World Bank. https://openknowledge.worldbank.org/handle/10986/37735

World Bank (2024). Ukraine Rapid Damage and Needs Assessment (RDNA4). Washington, DC: World Bank. https://www.worldbank.org/en/country/ ukraine/publication/rdna4

World Economic Forum (2024). The Global Risks Report 2024. Geneva: World Economic Forum. https://www.weforum.org/publications/global-risks-report-2024

Zio E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety*, 152, 137–150. https://doi.org/10.1016/j.ress.2016.02.009

Стаття надійшла до редакції 28.10.2025 р.
Статтю прийнято до публікації 17.11.2025 р.
Оприлюднено 01.02.2026 р.