https://doi.org/10.31891/2307-5740-2025-338-106
УДК 336

ЗАТОНАЦЬКИЙ Дмитро
ДНУ «Інститут освітньої аналітики»
https://orcid.org/0000-0002-4828-9144
e-mail: dzatonat@gmail.com

МІЖДИСЦИПЛІНАРНИЙ ВИМІР КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ВІД КЛАСИЧНОГО ТРАКТУВАННЯ ДО КОМПЛЕКСНОЇ МОДЕЛІ

Стаття пропонує міждисциплінарний огляд еволюції дефініції «критична інфраструктура» – від класичного, переважно матеріально-об'єктного трактування до комплексної моделі, що інтегрує фізичні та кіберкомпоненти, соціальні й культурно-символічні виміри. На основі порівняння підходів США, ЄС, Великої Британії, Японії та КНР показано, як безпекові пріоритети, інституційні рамки та історичний досвід формують різні критерії ідентифікації та пріоритезації секторів КІ. Обґрунтовано зростання ролі системно-мережевих методологій для моделювання взаємозалежностей і каскадних збоїв, а також необхідність інтегрованої парадигми фізичного захисту та кіберстійкості. Український контекст подано крізь призму воєнної агресії РФ та євроінтеграційного курсу: проаналізовано Закон України «Про критичну інфраструктуру» від 16.11.2021 р. № 1882-IX, висвітлено зміщення акцентів від вузької оборонно-енергетичної оптики до ризик-орієнтованого, функціонально й соціально вмотивованого підходу. Доведено, що війна стала каталізатором перегляду міжнародних практик і засвідчила потребу розширити перелік критичних секторів та синхронізувати управління ризиками на перетині державної політики, ринку та технологій. Практична значущість дослідження полягає у формуванні двошарової (вузької та широкої) дефініції «критична інфраструктура» й у виробленні рекомендацій щодо поєднання чіткої класифікації секторів, інструментів зниження ризиків та ефективної координації заінтересованих сторін з метою підвищення загальної стійкості системи та зміцнення економічної безпеки.

Ключові слова: інфраструктура, критична інфраструктура, кіберстійкість, фізичний захист, кіберзахист, економічна безпека, воєнні загрози, євроінтеграція.

ZATONATSKIY Dmytro
SSI "Institute of Educational Analytics"

INTERDISCIPLINARY DIMENSION OF CRITICAL INFRASTRUCTURE: FROM CLASSICAL TREATMENT TO COMPREHENSIVE MODEL

Over the past decades, scientific and political discourse has increasingly focused on the issue of critical infrastructure (CI), which is considered a system-forming factor of stability, economic sustainability, and national security. The article offers an interdisciplinary overview of the evolution of the definition of "critical infrastructure" - from the classical, predominantly material-object interpretation to a comprehensive model that integrates physical and cyber components, social and cultural-symbolic dimensions. Based on a comparison of the approaches of the USA, EU, Great Britain, Japan and the PRC, it is shown how security priorities, institutional frameworks and historical experience shape different criteria for identifying and prioritizing CI sectors. The growing role of system-network methodologies for modeling interdependencies and cascading failures, as well as the need for an integrated paradigm of physical protection and cyber resilience, is substantiated. The Ukrainian context is presented through the prism of the Russian Federation's military aggression and the European integration course: the Law of Ukraine "On Critical Infrastructure" dated 11/16/2021 No. 1882-IX is analyzed, the shift in emphasis from a narrow defense and energy perspective to a risk-oriented, functional and socially motivated approach is highlighted. It is proven that the war became a catalyst for reviewing international practices and demonstrated the need to expand the list of critical sectors and synchronize risk management at the intersection of state policy, market and technology. The practical significance of the study lies in the formation of a two-layer (narrow and broad) definition of "critical infrastructure" and in developing recommendations for combining a clear classification of sectors, risk reduction tools and effective coordination of stakeholders in order to increase the overall stability of the system and strengthen economic security.

Keywords: infrastructure, critical infrastructure, cyber resilience, physical protection, cyber defense, economic security, military threats, European integration.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Протягом останніх десятиліть у науковому та політичному дискурсі дедалі більше уваги приділяється проблематиці критичної інфраструктури (КІ), яка розглядається як системоутворюючий фактор стабільності, економічної стійкості та національної безпеки. Суспільні процеси, що супроводжуються глобалізацією, зростанням технологічної взаємозалежності, геополітичною нестабільністю та виникненням нових форм загроз, зумовили необхідність переосмислення самого змісту дефініції «критична інфраструктура» та розширення її складових. Відтак, саме еволюція наукових поглядів на визначення КІ стала відправною точкою для формування сучасних стратегій захисту держави й суспільства від багатогранних викликів.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проблематика дефініції та класифікації критичної інфраструктури широко представлена в українській та зарубіжній науковій літературі, а також у міжнародних і національних нормативних актах. Українські дослідники пропонують різні підходи до окреслення КІ: від системи взаємопов'язаних об'єктів, що забезпечують основу економіки, оборони та нацбезпеки (О. Герасименко) [1], до комплексного конгломерату стратегічних матеріальних і інформаційних елементів, покликаних гарантувати повноцінний життєвий цикл та добробут людини (С. Теленик) [2]. Низка авторів наголошує на поєднанні матеріальних і нематеріальних складників та їхній критичності для сталого функціонування держави (О. Єрменчук) [3], а також акцентує на фізичних і віртуальних системах і ресурсах, вразливість яких породжує суттєві загрози публічній безпеці (І. Уряднікова, В. Заплатинський) [4]. Узагальнюючі трактування підкреслюють роль КІ як сукупності об'єктів і систем, що забезпечують безперебійність суспільних функцій і добробут громадян (Р. Плахотнюк) [5], а також важливість формалізованих процедур ідентифікації, категоризації та паспортизації (І. Єфіменко, А. Саковський, Є. Білозьоров) [6].

Міжнародний дискурс еволюціонує від безпеково-утилітарних підходів до багатовимірних моделей критичності. У США вихідні рамки задав PDD-63, що інституціоналізував завдання зменшення вразливості критичних елементів у публічному та приватному секторах [7], а ширше бачення закріплене Патріотичним актом 2001 р. В ЄС базові підходи було формалізовано в Директиві 2008/114/ЄС з акцентом на підтримці життєво важливих суспільних функцій та транскордонних ефектах [8]; практики держав-членів ОЕСР демонструють пріоритет енергетики, ІКТ, транспорту, охорони здоров'я, водопостачання та фінансів як «хребта» життєдіяльності [9]. У цьому контексті українська доктрина та законодавство логічно вписуються в глобальну тенденцію до комплексного, функціонально орієнтованого та ризик-чутливого підходу до визначення та захисту КІ.

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Попри очевидну концептуальну значущість КІ для економічної та національної безпеки, у науковій літературі та нормативній практиці зберігається фрагментарність підходів до її визначення. Вузькі матеріально-об'єктні трактування співіснують із широкими функціональними інтерпретаціями, що охоплюють як фізичні, так і віртуальні компоненти, соціальні та культурно-символічні виміри. Така розбіжність ускладнює уніфікацію критеріїв ідентифікації, категоризації та пріоритезації елементів КІ, створюючи методологічну невизначеність у політиках стійкості й дерегулювання ризиків. Отже, поза сумнівом залишається актуальність досліджень, що стосуються проблеми трактування та концептуалізації дефініції «критична інфраструктура.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є визначення дефініції «критична інфраструктура» із використанням міждисциплінарного підходу від класичного, переважно матеріально-об'єктного трактування до комплексної моделі, що інтегрує фізичні та кіберкомпоненти, соціальні й культурно-символічні виміри..

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Започатковуючи історіографічний зріз еволюції уявлень про критичну інфраструктуру, доречно звернутися до ранніх підходів, сформованих у руслі безпекового дискурсу періоду «жорсткої» сек'юритизації державних пріоритетів. Так, у низці ранніх досліджень, що стосувалися передусім питань військової безпеки, КІ ототожнювалась виключно з тими об'єктами, порушення функціонування яких могло спричинити суттєві економічні або оборонні наслідки. Йшлося насамперед про енергетичні системи, транспортні мережі, об'єкти оборонного значення. Такий підхід відображав прагматичну потребу держав забезпечити безперервність функціонування базових секторів, які безпосередньо впливали на їхню обороноздатність та економічний потенціал. Проте з часом критерії визначення того, що відноситься до КІ, зазнали суттєвої трансформації. Зокрема, дедалі частіше в академічних працях і нормативно-правових актах підкреслюється значення таких сфер, як інформаційно-комунікаційні технології, фінансові системи, охорона здоров'я, продовольча безпека тощо. Ба більше, в деяких національних підходах до складу КІ почали включати навіть культурні об'єкти, національні пам'ятки, атака на які може мати значний психологічний та символічний ефект.

У контексті зростаючої геополітичної нестабільності, технологічної взаємозалежності та системних вразливостей взаємозв'язок між критичною інфраструктурою та економічною безпекою держави стає дедалі актуальнішою темою в академічному та політичному дискурсі. Критична інфраструктура, що охоплює такі сектори, як енергетика, транспорт, фінанси, телекомунікації, цифрові сервіси та інформаційні системи, формує операційну основу національних економік, забезпечує надання базових послуг і підтримує безперервність суспільних функцій. У цьому аспекті стійкість і надійність КІ розглядаються як невід'ємні компоненти економічної стабільності, стратегічної автономії та можливостей держав у сфері кризового

управління. Це дозволяє говорити про КІ не лише як про технічну чи безпекову проблему, а як про системний елемент архітектури національної та економічної безпеки.

Особливу складність становить відсутність єдиного універсального визначення КІ, що обумовлює багатоваріантність наукових і практичних підходів. В одних концепціях підкреслюється пріоритет матеріальних об'єктів – виробничих, енергетичних, транспортних, у той час як інші дослідники акцентують увагу на функціональних системах, без яких неможливе існування сучасного суспільства. Так, О.М. Герасименко вважає, що критичною інфраструктурою є система взаємопов'язаних або окремих об'єктів інфраструктури, які складають та/або забезпечують основу для вирішення завдань економіки, оборони, національної безпеки України, руйнація або пошкодження яких призведе до заподіяння шкоди національним інтересам України [1]. Ну думку С.С. Теленик критична інфраструктура є системним комплексом стратегічних матеріальних та інформаційних об'єктів виробничої, невиробничої, соціальної сфери, а також окремими складовими частинами цього комплексу, в т.ч. ключовими ресурсними, покликаними забезпечувати повноцінний життєвий цикл, безпеку, охорону здоров'я, добробут людини, сталий розвиток суспільства й економіки держави, підтримання її суверенітету з огляду на те, що зловмисне втручання у функціонування, а також пошкодження, руйнація або виведення з ладу системи або її елементів внаслідок диверсій, техногенних чи природних катастроф, спроможне призвести до тяжких наслідків: жертв чи поневірянь, шкоди національним інтересам, знецінення надбань людини і держави [2]. О.П. Єрменчук визначає критичну інфраструктуру, як систему надзвичайно важливих матеріальних та нематеріальних об'єктів національної інфраструктури (а також їх власність та результати діяльності), що забезпечують її стале функціонування, руйнація або пошкодження яких (наявними загрозами) може призвести до людських жертв і значних матеріальних збитків із найсерйознішими негативними наслідками для життєдіяльності суспільства, соціально-економічного розвитку країни та національної безпеки [3]. І.В. Уряднікова та В.М. Заплатинський під критичною інфраструктурою розуміють фізичні та віртуальні системи, об'єкти і ресурси – руйнування, знищення або зниження дієздатності яких, призведе до суттєвих загроз країні (регіону або місту), її національної безпеки, життєдіяльності та здоров'ю населення [4]. На думку Р.В. Плахотнюк критична інфраструктура – це сукупність об'єктів і систем, що забезпечують безперебійне функціонування суспільства і економіки, а також забезпечують національну безпеку та добробут громадян [5]. І. Єфіменко, А. Саковський та Є. Білозьоров вважають, що критичною інфраструктурою є сукупність та/або комплекс об'єктів інфраструктури, які мають життєво важливе значення для економіки, національної безпеки та оборони країни і які відповідно до закону пройшли процедуру ідентифікації, категоризації, реєстрації та паспортизації [6]. У вітчизняних та зарубіжних наукових джерелах дефініція КІ постає не як статична категорія, а як динамічний конструкт, що постійно змінюється під впливом економічних, соціальних, технологічних та політичних чинників. Еволюція цієї дефініції також демонструє різні методологічні підходи – від прагматично-вузького до комплексно-широкого, що інтегрує соціально-гуманітарні та символічні аспекти.

Водночас наукові підходи до визначення КІ нерозривно пов'язані з розвитком міжнародного нормативного поля. У США, ЄС та країнах НАТО формування концепту «critical infrastructure» відбувалося паралельно із розробкою національних програм захисту від тероризму, кібератак та природних катастроф. Перші згадки цього концепту отримали своє відображення у директиві PDD-63 (Presidential Decision Directive), яка була підписана президентом США Б. Клінтоном у 1996 році. Зазначеною Директивою критичну інфраструктуру було віднесено до національних життєво важливих інтересів, визначено цілі та сформовано концепцію зменшення її уразливості в громадському і приватному секторі. І найголовніше, закладено вимогу щодо забезпечення безпеки критичних елементів інфраструктури [7].

Історично КІ великою мірою асоціювалася з фізичними, контрольованими державою активами, такими як мости, електростанції та водопровідні системи, особливо в періоди геополітичної напруженості під час «холодної війни». Ці активи розглядали як життєво важливі для національної оборони та цивільної життєдіяльності. З часом, особливо після терактів 11 вересня 2001 р. та потужних стихійних лих, визначення КІ розширилося і тепер включає спектр як фізичних, так і кіберсистем, порушення роботи яких може мати руйнівний вплив на безпеку, економіку й громадське здоров'я країни. У Сполучених Штатах це ширше бачення кодифіковане в Патріотичному акті 2001 р., що визначає КІ як системи та активи, фізичні чи віртуальні, настільки життєво важливі, що їхня недієздатність загрожуватиме національній безпеці, економічному процвітанню, громадському здоров'ю або безпеці. Згодом питанням критичної інфраструктури та її безпеки почали приділяти увагу в інших країнах, зокрема: Німеччині, Великій Британії, Нідерландах, Чеській Республіці, Словаччині, Польщі, Угорщині та ін. Важливим у цьому процесі є те, що у деяких національних законодавствах при визначенні дефініції «критична інфраструктура» акцентовано на функціях та послугах. Саме функції та послуги об'єктів критичної інфраструктури, якими забезпечують суспільство, бізнес та державу, є в основі визначення їх критичності, що дає методологічні можливості для встановлення критеріїв відбору елементів критичної інфраструктури та пріоритетності їх захисту. З часом Європейський Союз формалізував дефініцію «критична інфраструктура» в Директиві 2008/114/ЄС, посилаючись на КІ як на елементи, системи або їхні частини, необхідні для підтримки життєво важливих

суспільних функцій, здоров'я, безпеки, захищеності та економічного чи соціального добробуту, де збій у роботі або руйнування матимуть серйозні наслідки для принаймні двох держав-членів [8].

У Сполученому Королівстві критична інфраструктура визначається в Національній стратегії кібербезпеки Великої Британії та низці суміжних урядових документів як сукупність елементів, систем і мереж, які є необхідними для безперебійного функціонування суспільства та економіки країни. До них відносять енергетику, водопостачання, транспорт, охорону здоров'я, комунікації та фінансові послуги. Важливим акцентом британського підходу є усвідомлення того, що саме ці сектори становлять базис для функціонування державних інститутів, бізнесу та щоденного життя громадян. До того ж Велика Британія з початку 2000-х років приділяє особливу увагу проблематиці кібербезпеки, розглядаючи її як ключовий аспект захисту критичної інфраструктури. Такий акцент зумовлений кількома факторами: швидким розвитком цифрових технологій, активним переходом фінансового сектору й комунікацій у віртуальну сферу, а також досвідом численних кібератак, які мали місце на території країни. Британська стратегія, таким робом, поєднує класичне розуміння фізичних об'єктів інфраструктури з акцентом на кіберзагрози, що робить її однією з найбільш збалансованих у Європі.

Японія також має власне нормативне визначення критичної інфраструктури, закріплене в Законі «Про захист життєво важливої інфраструктури». Під КІ в японському праві розуміють об'єкти та системи, необхідні для забезпечення безперервності життєдіяльності країни, зокрема у сфері енергетики, транспорту, зв'язку, охорони здоров'я та фінансів. Японський підхід базується на двох ключових принципах: по-перше, забезпеченні стійкості функціонування інфраструктурних систем, а по-друге – гарантуванні їх відновлюваності у разі надзвичайних ситуацій. Це пояснюється специфічними умовами країни: Японія регулярно стикається з потужними землетрусами, цунамі, тайфунами та іншими природними катастрофами. Саме цей досвід зумовив наголос на необхідності не лише захищати об'єкти, а й швидко їх відновлювати після можливих руйнувань. Тобто японський підхід орієнтований на довгострокову стійкість і мінімізацію наслідків катастроф, що робить його унікальним серед інших світових моделей.

Китайська Народна Республіка закріпила поняття критичної інфраструктури у Законі «Про національну безпеку КНР» та ряді галузевих документів. Визначення, запропоноване Китаєм, є надзвичайно широким: до КІ належать об'єкти, які становлять основу для забезпечення національної безпеки, економічного розвитку, соціальної стабільності та добробуту населення. У цьому переліку знайшли своє місце енергетика, транспорт, водопостачання, телекомунікації, фінанси, оборонна промисловість та інші сектори, які вважаються стратегічними. Особливість китайського підходу полягає у двох аспектах: по-перше, у максимальному охопленні секторів, що забезпечує універсальність поняття; по-друге, у наголошенні на необхідності національного контролю та захисту від іноземних загроз. Це відповідає загальній політико-економічній стратегії КНР, спрямованій на збереження державного суверенітету та контроль над ключовими секторами в умовах глобальної конкуренції та зростання міжнародних ризиків. Китайська дефініція є яскравим прикладом того, як національні пріоритети визначають рамки для тлумачення дефініції «критична інфраструктура».

Аналізуючи підходи різних країн, можна дійти висновку, що дефініція критичної інфраструктури скрізь формується під впливом унікальних політичних, економічних та безпекових умов. Так, у США наголос робиться на кібербезпеці та протидії терористичним загрозам. Це зумовлено насамперед досвідом терактів 11 вересня 2001 року, які стали точкою відліку для кардинального перегляду підходів до захисту інфраструктури, а також великою кількістю кібератак на фінансові й енергетичні системи країни. У Європейському Союзі головним завданням є координація та інтеграція підходів держав-членів, адже функціонування інфраструктури окремої країни тісно пов'язане з інфраструктурою сусідів. Це логічно випливає з політичної та економічної інтеграції ЄС, що робить проблематику захисту КІ міждержавною, а не суто національною. Велика Британія, як і США, акцентує увагу на кібербезпеці, розуміючи, що сучасна економіка й управлінські процеси значною мірою залежать від інформаційних систем та цифрових технологій. Китай же концентрується на внутрішньому контролі та протидії зовнішнім загрозам, що відображає його політичну й економічну модель розвитку. Водночас японський підхід виділяється серед інших завдяки увазі до природних катастроф і здатності інфраструктури до швидкого відновлення, що є прямим наслідком географічних та кліматичних умов цієї країни. Отже, на прикладі зазначених держав можна побачити, як національні інтереси й історичний досвід формують різні інтерпретації поняття «критична інфраструктура».

Україна, інтегруючись у європейський безпековий простір, змушена переосмислювати власні підходи до визначення дефініції «критична інфраструктура». Воєнна агресія проти нашої держави наочно продемонструвала вразливість традиційних секторів, що потребує не лише адаптації зарубіжного досвіду, але й розробки власної комплексної моделі. Така модель має враховувати специфіку політичної ситуації, воєнні загрози, економічні виклики та соціальні потреби. На відміну від багатьох зарубіжних країн, для яких у центрі уваги – соціальний добробут або технологічна стійкість, для України кінцевою метою захисту КІ є збереження національних інтересів, територіальної цілісності й державного суверенітету. Разом з тим інтеграція у європейський простір передбачає поступове наближення до підходів ЄС, що поєднують функціональність, соціальну стабільність та міждержавну координацію.

В Україні визначення КІ, критеріїв віднесення до її об'єктів і порядок захисту наведено в Законі України «Про критичну інфраструктуру» від 16.11.2021 р. № 1882-IX [10]. Зокрема, критична інфраструктура визначається як сукупність об'єктів критичної інфраструктури, тобто об'єктів інфраструктури, систем, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [10]. Також у Законі закріплено порядок визначення критичності об'єкту та його захисту. Якщо порівняти дефініції критичної інфраструктури, то стає очевидним, що в розвинутих країнах, на відміну від України, це визначення є більш соціально орієнтованим, тобто в ньому підкреслюється важливість суспільного добробуту як кінцевої мети захисту КІ. Визначення, застосовуване в Україні, має більш практичний характер, зокрема кінцевою метою є національні інтереси.

Сучасні дослідження демонструють, що критична інфраструктура є складним міждисциплінарним феноменом, вивчення якого вимагає залучення економічної теорії, безпекознавства, права, соціології та навіть психології масових процесів. Важливим у цьому контексті є й питання методології: від обґрунтування критеріїв віднесення того чи іншого сектору к об'єктам КІ до вибору моделей її захисту, які здатні адекватно реагувати на транснаціональні загрози. Звідси випливає, що розуміння сутності КІ має не лише теоретичне, а й безпосереднє практичне значення, адже воно впливає на визначення державних пріоритетів, формування стратегій інвестиційного розвитку, розподіл ресурсів і організацію системи національної безпеки. Слід зауважити, що наразі більшість країн використовує найбільш загальне визначення КІ, причому кожна країна індивідуально встановлює перелік секторів, які до неї належать (рис. 1.).

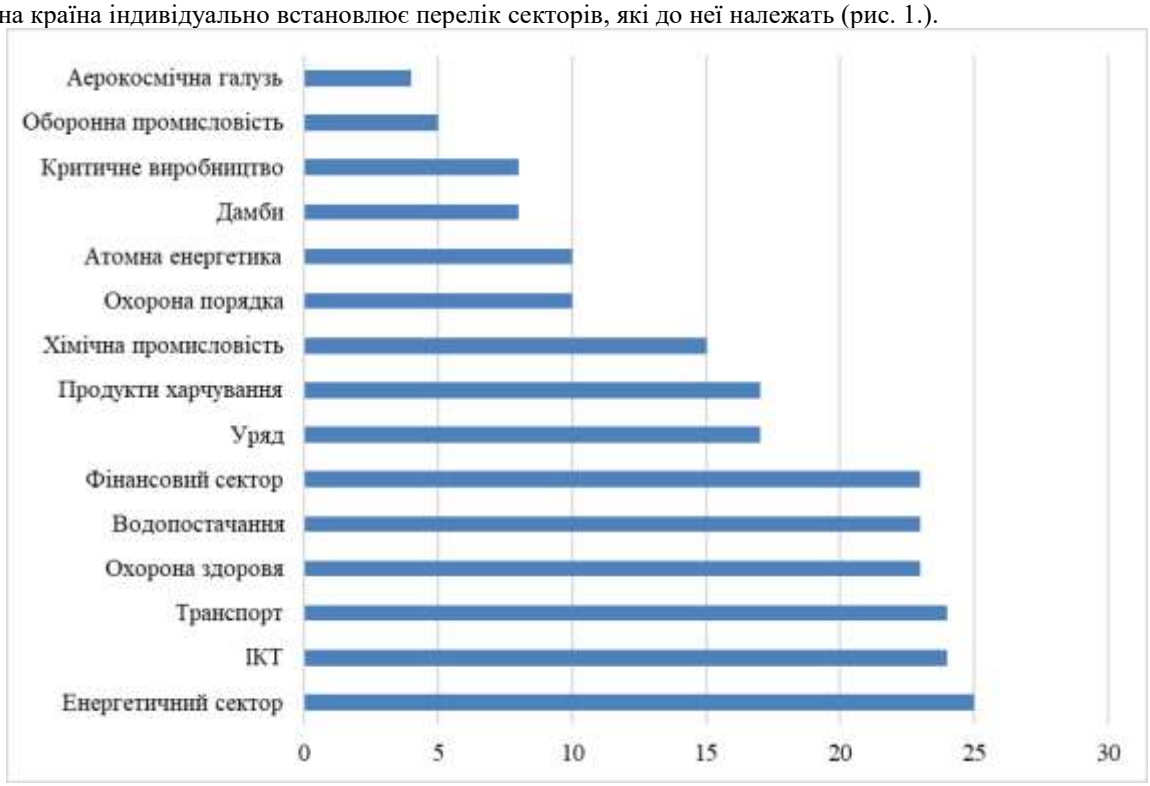

Рис. 1. Сектори, що відносяться до критичної інфраструктури в країнах ОЕСР
Джерело: складено автором на основі даних ОЕСР [9]

Правові та стратегічні рамки для визначення критично важливих об'єктів КІ суттєво відрізняються в різних юрисдикціях, але мають спільні структурні елементи. Ці рамки зазвичай включають визначення критичних секторів, оцінку загроз і ризиків, планування стійкості та співпрацю між державним і приватним секторами. Якщо подивитися на країни ОЕСР, то відповідно до документів 25 держав, які мали нормативно закріплений перелік, найчастіше до критичної інфраструктури відносили такі сектори, як енергетика, інформаційно-комунікаційні технології та транспорт, охорона здоров'я, водопостачання та фінансовий сектор. Саме вони визнавалися «хребтом» життєдіяльності суспільства та базисом функціонування економіки, адже від їхньої стійкості залежала здатність держави підтримувати безперервність соціально-економічних процесів. Найрідше до складу КІ включали критичне виробництво, оборонну промисловість та аерокосмічний сектор. Таке вибіркове віднесення мало пояснення: вважалося, що зазначені сфери, будучи стратегічними, уже традиційно перебувають під контролем держави, а тому не потребують окремого віднесення до категорії КІ. Однак практика останніх років, а особливо війна в Україні, показала недосконаліть такого розподілу секторів. Збройна агресія проти України стала своєрідним «краш-тестом» для всієї системи міжнародних уявлень про критичну інфраструктуру, адже на практиці виявилося, що недооцінені та формально «не критичні» сектори фактично мають життєво важливе значення. Наприклад,

хімічна промисловість, яка в більшості країн ОЕСР не належало до секторів КІ, опинилися відкритими до саботажу й терористичних атак у країнах Європи. Це спричинило зупинку виробництва, економічні втрати, руйнування екологічних балансів і стало наочним показником того, що зазначені сектори також потребують посиленого захисту та нормативного врегулювання. Ба більше, воєнний досвід довів, що інфраструктура оборонно-промислового комплексу є так само вразливою до кібератак і фізичних диверсій, як і енергетика чи транспорт. Таким робом, європейська та міжнародна практика потребує перегляду базових підходів до класифікації секторів КІ з урахуванням воєнних і гібридних загроз.

У цьому контексті все більшого значення набуває проблема взаємозалежності інфраструктурних секторів. Основні категорії КІ – енергетика, водопостачання, транспорт, охорона здоров'я, фінансові системи та ІКТ – утворюють основу сучасних суспільств, формуючи складну й динамічну мережу взаємозв'язків. Ці сектори за своєю сутністю не є автономними: відмова або виведення з ладу одного може спровокувати каскадні ефекти в інших. Як уточнює Е. Зіо, збої в одному секторі можуть швидко поширюватися на інші через фізичні й функціональні взаємозв'язки. Наприклад, кібератака на систему управління енергією може призвести до каскадних збоїв у транспорті та телекомунікаціях. Тому стійкість КІ повинна аналізуватися не ізольовано, а як частина складної адаптивної системи. Топологічні та логічні моделі (наприклад, теорія графів, дерева відмов) широко використовуються для картування та моделювання цих взаємозалежностей, хоча автор критикує їхні обмеження у врахуванні емерджентної поведінки та нелінійної динаміки [11]. Сучасна наукова думка у цьому напрямі підкреслює, що традиційні методи оцінки ризиків і вразливостей, які базуються на лінійних підходах, не здатні врахувати ефект «доміно», характерний для глобалізованого світу. У результаті навіть локальна аварія чи диверсія може перерости в системну кризу національного або міжнародного масштабу.

Водночас варто звернути увагу на ще одну важливу тенденцію. Дослідники дедалі більше концентруються на проблемах кіберзахисту КІ, часто нехтуючи аспектами її фізичної безпеки. Безперечно, кібератаки є одним із найбільш реальних викликів сучасності, здатним у короткостроковій перспективі паралізувати діяльність окремого підприємства або навіть цілого сектору. Наприклад, відключення електроенергії 2003 р. на північному сході США та в Канаді торкнулося понад 50 млн. осіб і спричинили економічні збитки, які оцінюються в 6 млрд. дол. США. Аналогічно, кібератака WannaCry 2017 р. паралізувала системи охорони здоров'я в багатьох країнах, що ілюструє зростаючу вразливість цифрової інфраструктури [12]. Проте при наявності належної системи кіберзахисту та швидкого реагування їхні наслідки, як правило, є тимчасовими. Натомість фізичне руйнування інфраструктурного об'єкта – внаслідок теракту, війни, природної катастрофи чи техногенної аварії – призводить до довготривалих і набагато масштабніших наслідків. Відновлення зруйнованої електростанції, транспортного вузла чи системи водопостачання може тривати роками й потребувати мільярдних витрат, тоді як ураження їхньої цифрової компоненти часто можна усунути протягом тижнів або навіть днів. Цей дисбаланс у наукових і практичних підходах потребує усвідомлення: без поєднання кібербезпеки та фізичного захисту неможливо забезпечити комплексну стійкість КІ [13; 14].

Отже, сучасні тенденції розвитку підходів до критичної інфраструктури демонструють поступову зміну акцентів: від вузького розуміння КІ як сукупності лише матеріальних об'єктів до широкого комплексного бачення, що включає кіберкомпоненти, соціальні й культурні аспекти, а також взаємозалежність між секторами. Війна в Україні стала важливим каталізатором перегляду міжнародних практик у цій сфері, підштовхнувши до усвідомлення необхідності більш гнучких і адаптивних моделей класифікації, оцінки та захисту КІ.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Проведений аналіз дає змогу констатувати, що еволюція наукових поглядів на дефініцію «критична інфраструктура» відбувалася поступово, від вузького трактування її як сукупності матеріальних об'єктів оборонного та енергетичного призначення до сучасного багатовимірного підходу, що охоплює фізичні, віртуальні, соціальні й навіть культурно-символічні компоненти. Якщо на початкових етапах домінував утилітарно-прагматичний критерій – спроможність об'єкта спричинити економічні чи оборонні втрати у разі руйнування, то сьогодні критичність визначається також через здатність інфраструктурних систем забезпечувати життєдіяльність суспільства, соціальний добробут, стійкість держави до криз та її міжнародну конкурентоспроможність. Вивчення зарубіжного досвіду засвідчило відсутність єдиного уніфікованого визначення, що з одного боку ускладнює порівняння національних практик, але з іншого – створює можливість адаптації дефініції під особливості конкретної країни. Для США ключовим акцентом стало питання кібербезпеки та боротьби з тероризмом, для ЄС – координація та інтегрованість між державами-членами, для Китаю – національний контроль і захист від зовнішніх загроз, для Японії – стійкість до природних катастроф. Україна ж, опинившись у стані воєнної агресії, актуалізувала потребу у власній, більш комплексній моделі визначення та захисту КІ, орієнтованій як на національні інтереси, так і на забезпечення соціальної стабільності. З урахуванням взаємозалежності секторів, розвитку інформаційних технологій, а також досвіду війни в Україні можна зробити висновок, що сучасна дефініція критичної

інфраструктури повинна враховувати не лише функціональну значущість об'єктів і систем, але й необхідність їх комплексного захисту – як фізичного, так і кібернетичного. Таким робом, під критичною інфраструктурою вважаємо за необхідне розуміти: сукупність об'єктів і систем, фізичних та віртуальних, функціонування яких є життєво необхідним для безпеки держави, стабільності економіки та добробуту суспільства, а їх пошкодження чи руйнація призводять до значних негативних наслідків (вузьке трактування); динамічний міждисциплінарний комплекс матеріальних і нематеріальних об'єктів, систем та ресурсів, що охоплюють енергетичний, транспортний, інформаційно-комунікаційний, фінансовий, оборонно-промисловий, соціальний та інші сектори, які забезпечують безперервність життєво важливих функцій держави та суспільства. Її стійкість є необхідною умовою економічної стабільності, національної безпеки та соціального добробуту, а руйнація чи пошкодження цих елементів унаслідок воєнних дій, терористичних атак, кібератак, техногенних аварій або природних катастроф здатні спричинити масштабні людські втрати, економічну дестабілізацію, підрив державного суверенітету й міжнародної безпеки (широке трактування).

Література

1. Герасименко О. М. Критична інфраструктура України як предмет наукового пізнання: теоретичний аспект. Науковий вісник Ужгородського Національного Університету, 2024. Випуск 85. Частина 4. С. 42 – 49.

2.Теленик С. С. Правовий зміст поняття «критична інфраструктура». National law journal: theory and practice, 2019. С. 34 – 38.

3.Єрменчук О. П. Поняття «критична інфраструктура». Інформаційна безпека людини, суспільства, держави, 2018. № 1. С. 20 – 28.

4.Уряднікова І. В., Заплатинський В. М. Наукові підходи до визначення терміну «критична інфраструктура». Вісті Донецького гірничого інституту, 2020. № 2 (47). С. 184 – 193.

5.Плахотнюк Р. В. Забезпечення стійкості критичної інфраструктури в Україні в умовах сучасних викликів. Економічний простір, 2024. № 195. С. 47 – 54.

6.Єфіменко І, Саковський А., Білозьоров Є. Protection of critical infrastructure as a component of Ukraine's national security. Юридичний часопис НАВС, 2023. Том 13. № 2. С. 74 – 85.

7.Presidential Decision Directive/NSC-63. Retrieved from https://irp.fas.org/offdocs/pdd/pdd-63.htm (дата звернення: 28.09.2025)

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. Retrieved from https://eur-lex.europa.eu/eli/dir/2008/114/oj/eng (дата звернення: 28.09.2025)

9.Good Governance for Critical Infrastructure Resilience. OECD Reviews of Risk Management Policies, OECD Publishing, Paris, 2019. Retrieved from https://doi.org/10.1787/02f0e5a0-en (дата звернення: 28.09.2025)

10.Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882-IX. Відомості Верховної Ради (ВВР), 2023. № 5. Ст. 13

11.Zio E. Challenges in the vulnerability and risk analysis of critical infrastructures. Reliability Engineering & System Safety, 2016. Vol. 152. P. 137 – 150. Retrieved from https://doi.org/10.1016/j.ress.2016.02.009 (дата звернення: 28.09.2025)

12.Curt C., Tacnet J. M. Resilience of critical infrastructures: Review and analysis of current approaches. Risk Analysis, 2018. Vol. 38 (11). P. 2441 – 2458. Retrieved from https://doi.org/10.1111/risa.13166 (дата звернення: 28.09.2025)

13. Rathnayaka B., Siriwardana C., Robert D., Amaratunga D., Setunge S. Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review. International Journal of Disaster Risk Reduction, 2022. Vol. 78. P. 103123. Retrieved from https://doi.org/10.1016/j.ijdrr.2022.103123 (дата звернення: 28.09.2025)

14. Ojo B., Ogborigbo J. C., Okafor M. O. Innovative solutions for critical infrastructure resilience against cyber-physical attacks. World Journal of Advanced Research and Reviews, 2024. Vol. 22(03). P. 1651-1674. Retrieved from https://doi.org/10.30574/wjarr.2024.22.3.1921 (дата звернення: 28.09.2025)

References

1. Herasymenko O. M. Krytychna infrastruktura Ukrainy yak predmet naukovoho piznannia: teoretychnyi aspekt. Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu, 2024. Vypusk 85. Chastyna 4. S. 42 – 49.

2. Telenyk S. S. Pravovyi zmist poniattia «krytychna infrastruktura». National law journal: theory and practice, 2019. S. 34 – 38.

3. Yermenchuk O. P. Poniattia «krytychna infrastruktura». Informatsiina bezpeka liudyny, suspilstva, derzhavy, 2018. № 1. S. 20 – 28.

4. Uriadnikova I. V., Zaplatynskyi V. M. Naukovi pidkhody do vyznachennia terminu «krytychna infrastruktura». Visti Donetskoho hirnychoho instytutu, 2020. № 2 (47). S. 184 – 193.

5. Plakhotniuk R. V. Zabezpechennia stiikosti krytychnoi infrastruktury v Ukraini v umovakh suchasnykh vyklykiv. Ekonomichnyi prostir, 2024. № 195. S. 47 – 54.

6. Yefimenko I, Sakovskyi A., Bilozorov Ye. Protection of critical infrastructure as a component of Ukraines national security. Yurydychnyi chasopys NAVS, 2023. Tom 13. № 2. S. 74 – 85.

7.Presidential Decision Directive/NSC-63. Retrieved from https://irp.fas.org/offdocs/pdd/pdd-63.htm

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. Retrieved from https://eur-lex.europa.eu/eli/dir/2008/114/oj/eng

9.Good Governance for Critical Infrastructure Resilience. OECD Reviews of Risk Management Policies, OECD Publishing, Paris, 2019. Retrieved from https://doi.org/10.1787/02f0e5a0-en

10. Pro krytychnu infrastrukturu: Zakon Ukrainy vid 16.11.2021 r. № 1882-IX. Vidomosti Verkhovnoi Rady (VVR), 2023. № 5. St. 13.

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

12.Curt C., Tacnet J. M. Resilience of critical infrastructures: Review and analysis of current approaches. Risk Analysis, 2018. Vol. 38 (11). P. 2441 – 2458. Retrieved from https://doi.org/10.1111/risa.13166

13. Rathnayaka B., Siriwardana C., Robert D., Amaratunga D., Setunge S. Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review. International Journal of Disaster Risk Reduction, 2022. Vol. 78. P. 103123. Retrieved from https://doi.org/10.1016/j.ijdrr.2022.103123

14. Ojo B., Ogborigbo J. C., Okafor M. O. Innovative solutions for critical infrastructure resilience against cyber-physical attacks. World Journal of Advanced Research and Reviews, 2024. Vol. 22(03). P. 1651-1674. Retrieved from https://doi.org/10.30574/wjarr.2024.22.3.1921