УДК 330.3:338.1:338.2:338.4:351
JEL Classification: H56; L98; O38
DOI: https://doi.org/10.32983/2222-4459-2025-8-47-71

ІДЕНТИФІКАЦІЯ ЕЛЕМЕНТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ЗАКОРДОННИЙ І ВІТЧИЗНЯНИЙ ДОСВІД

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

УДК 330.3:338.1:338.2:338.4:351
JEL Classification: H56; L98; O38

Хаустова В. Є., Трушкіна Н. В., Проноза П. В. Ідентифікація елементів критичної інфраструктури: закордонний і вітчизняний досвід

У статті здійснено комплексне дослідження теоретико-методологічних підходів і практичних механізмів ідентифікації об'єктів критичної інфраструктури у зарубіжному та національному вимірах. Актуальність проблематики зумовлена зростанням спектра гібридних загроз, трансформацією міжнародного безпекового середовища та необхідністю формування стійкої архітектури національної безпеки України в умовах воєнного стану. Автори виходять із того, що ідентифікація критичних об'єктів і формування національного реєстру є складним завданням, що зумовлене різнорідністю інфраструктурних елементів, їх масштабною кількістю та багатовимірністю характеристик. Це потребує застосування науково обґрунтованої методології, міждисциплінарного підходу та системного оновлення інформаційної бази. Метою дослідження є узагальнення зарубіжного досвіду й аналіз української практики ідентифікації критично важливих об'єктів інфраструктури, визначення їх категоризації та секторальної класифікації з урахуванням сучасних викликів. Методологічну основу становлять системний і порівняльний аналіз, структурно-логічне узагальнення, ризик-орієнтований і модельний підходи, а також аналіз нормативно-правових актів ЄС, НАТО та України. У роботі розглянуто ключові зарубіжні моделі: французьку (інституційно-організаційну, що спирається на концепт «життєво важливих операторів»), британську (секторально-ієрархічну з багаторівневою оцінкою критичності), нідерландську (процесно-орієнтовану), німецьку (що інтегрує технічні й соціально-економічні складові) та ізраїльську (багатовимірну, яка поєднує культурно-символічний, функціонально-економічний і системно-структурний виміри). Особливу увагу приділено європейському нормативному середовищу, представленому Директивою Ради ЄС 2008/114/ЄС, Директивою (ЄС) 2022/2557 та Делегованим Регламентом Комісії (ЄС) 2023/2450, що окреслюють сучасну систему критеріїв ідентифікації та категоризації критичної інфраструктури, у тому числі на транскордонному рівні. Наукове значення має обґрунтування класифікації секторів критичної інфраструктури України за чотирма блоками – економічним, соціальним, безпековим та управлінським. Така систематизація дозволяє інтегрувати національну систему захисту до європейських і міжнародних практик, сприяє міжсекторальному аналізу ризиків і вразливостей, створює умови для проведення LMDI- та PSS-аналізу впливу окремих секторів на стійкість держави та формування індикаторів національної безпеки, узгоджених зі світовими стандартами. Крім того, уніфікація термінології та підходів підсилює можливості для залучення міжнародної технічної та фінансової допомоги. Узагальнення показує, що українська модель значною мірою відтворює підходи ЄС і НАТО, але має й унікальні риси. По-перше, це розширена деталізація економічного блоку (зокрема виділення агропромислового комплексу, держрезерву, енергетичного машинобудування). По-друге, інституалізація виборчого процесу як елемента критичної інфраструктури, що майже відсутня у класифікаціях ЄС і НАТО. Водночас міжнародні моделі більше акцентують увагу на безперервності урядування та стратегічних комунікаціях, що лише частково інтегровано в український управлінський блок. Практичне значення результатів полягає у можливості використання досліджених підходів для вдосконалення національної нормативно-правової бази, розроблення інтегральних індикаторів критичності, удосконалення механізмів ризик-менеджменту та гармонізації української системи з міжнародними стандартами. У перспективі це сприятиме формуванню більш стійкої, адаптивної та інтегрованої системи критичної інфраструктури, здатної забезпечити безперервність базових суспільних функцій і протидіяти сучасним багатовимірним загрозам.

Ключові слова: *критична інфраструктура, сектори критичної інфраструктури, об'єкти критичної інфраструктури, рівень критичності, ідентифікація, категоризація, класифікація, систематизація, нормативно-правове регулювання, ризик-орієнтований підхід, загрози, державна політика, європейська інтеграція, закордонний досвід, національна безпека, захист, стійкість, резильєнтність.*

Рис.: *2.* ***Табл.:*** *9.* ***Бібл.:*** *45.*

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*

Проноза Павло Володимирович *– доктор економічних наук, професор, професор кафедри фінансів і кредиту, Харківський національний економічний університет імені Семена Кузнеця (просп. Науки, 9а, Харків, 61166, Україна)*
E-mail: *ppv@hneu.edu.ua*
ORCID: *https://orcid.org/0000-0001-8130-4564*

UDC 330.3:338.1:338.2:338.4:351
JEL Classification: H56; L98; O38

Khaustova V. Ye., Trushkina N. V., Pronoza P. V. Identification of Critical Infrastructure Elements: International and Domestic Experience

The article provides a comprehensive study of theoretical and methodological approaches, as well as practical mechanisms for identifying critical infrastructure facilities in both international and national contexts. The relevance of the topic is driven by the expanding range of hybrid threats, the transformation of the international security environment, and the need to establish a resilient national security architecture for Ukraine under martial law. The authors contend that identifying critical facilities and creating a national registry is a complex task due to the diversity of infrastructure elements, their large scale, and the multidimensional nature of their characteristics. This necessitates the application of a scientifically grounded methodology, an interdisciplinary approach, and systematic updating of the information base. The aim of the study is to synthesize international experience and analyze Ukrainian practices for identifying critical infrastructure assets, determining their categorization and sectoral classification in light of current challenges. The methodological framework includes systemic and comparative analysis, structural-logical generalization, risk-oriented and modeling approaches, as well as the analysis of the EU, NATO, and Ukrainian legal and regulatory acts. The work examines key foreign models: the French model (institutional-organizational, based on the concept of «vital operators»), the British model (sectoral-hierarchical with multi-level criticality assessment), the Dutch model (process-oriented), the German model (integrating technical and socioeconomic components), and the Israeli model (multidimensional, combining cultural-symbolic, functional-economic, and system-structural dimensions). Particular attention is given to the European regulatory framework, represented by Council Directive 2008/114/EC, Directive (EU) 2022/2557, and Commission Delegated Regulation (EU) 2023/2450, which define the modern system of criteria for identifying and categorizing critical infrastructure, including at the cross-border level. The scientific value lies in the substantiation of the classification of Ukraine's critical infrastructure sectors into four blocks – economic, social, security, and managerial. This systematization allows for the integration of the national protection system into European and international practices, facilitates cross-sectoral analysis of risks and vulnerabilities, creates conditions for conducting LMDI and PSS analyses of the impact of individual sectors on the State resilience, and for developing national security indicators aligned with global standards. Furthermore, the unification of terminology and approaches strengthens the capacity to attract international technical and financial assistance. The summary shows that the Ukrainian model largely mirrors the approaches of the EU and NATO, while also maintaining unique features. First, there is an expanded detailing of the economic sector (notably the inclusion of the agro-industrial complex, the State reserve, and energy engineering). Second, the institutionalization of the electoral process as an element of critical infrastructure, which is almost absent in the EU and NATO classifications. At the same time, international models place greater emphasis on governance continuity and strategic communications, which are only partially integrated into the Ukrainian administrative framework. The practical significance of the results lies in the possibility of using the studied approaches to refine the national legal and regulatory framework, develop comprehensive criticality indicators, improve risk management mechanisms, and harmonize the Ukrainian system with international standards. In the long term, this will facilitate the development of a more resilient, adaptive, and integrated critical infrastructure system, capable of ensuring the continuity of essential societal functions and countering contemporary multidimensional threats.

Keywords: *critical infrastructure, critical infrastructure sectors, critical infrastructure facilities, level of criticality, identification, categorization, classification, systematization, regulatory framework, risk-based approach, threats, State policy, European integration, foreign experience, national security, protection, resilience, robustness.*

Fig.: *2.* ***Tabl.:*** *9.* ***Bibl.:*** *45.*

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*

Pronoza Pavlo V. *– Doctor of Sciences (Economics), Professor, Professor of the Department of Finance and Credit, Simon Kuznets Kharkiv National University of Economics (9a Nauky Ave. , Kharkiv, 61166, Ukraine)*
E-mail: *ppv@hneu.edu.ua*
ORCID: *https://orcid.org/0000-0001-8130-4564*

Світовий досвід переконливо демонструє, що питання захисту та забезпечення стійкості критичної інфраструктури посідають ключове місце у державній політиці, зокрема в площині підтримання національної безпеки. Такий пріоритет є обґрунтованим, адже критична інфраструктура відіграє визначальну роль у стабільному функціонуванні стратегічно важливих секторів економіки та держави загалом, а також у гарантуванні належного рівня обороноздатності. Інфраструктурні об'єкти критичного значення формують інституційну основу захисту, безперервного функціонування, резервування та надійності економічної системи. Тому упродовж останніх років процес ідентифікації елементів критичної інфраструктури розглядається більшістю урядів як елемент без-

пекової та оборонної політики, а також необхідна складова механізмів підвищення резильєнтності національної економіки.

Таким чином, дослідження окресленої проблематики зберігає високий рівень актуальності та формує перспективний вектор подальших наукових розвідок, спрямованих на розроблення та удосконалення підходів до категоризації критично важливих об'єктів інфраструктури як у міжнародному, так і національному вимірі.

Питання розроблення методичних підходів до ідентифікації елементів критичної інфраструктури у більшості провідних країн світу входять до кола наукових інтересів зарубіжних та українських вчених. Аналіз наукових праць зарубіжних вчених (G. Cáceres [1]; A. Fekete et al. [2]; G. Galvan, J. Agarwal [3]; B. Leitner et al. [4]; P. Novotny, M. Janosikova [5]; C. Pursiainen, E. Kytömaa [6]; D. Rehak et al. [7; 8]; V. Vasylius et al. [9]; D. Vidriková, K. Boc [10]) показує, що здебільшого у публікаціях зустрічаються такі ключові слова, як критична інфраструктура, критичні елементи або об'єкти, критерії, резильєнтність, ризики безпеки, оцінювання ризиків тощо (табл. 1).

На підставі узагальнення наукових джерел встановлено, що українські дослідники (О. Єрменчук [11]; П. Підюков, О. Калиновський [12]; С. Теленик [13]; О. Яременко, Я. Страхніцький [14] та інші) приділяють особливу увагу теоретичним підходам до визначення поняття критичної інфраструктури та його переосмисленню. Як зазначають П. Підюков і О. Калиновський [12], критична інфраструктура розглядається як багаторів-

Таблиця 1

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

Ключове слово	Джерело								
	G. Galvan, J. Agarwal	P. Novotny, M. Janosikova	D.Vidriková, K. Boc	D. Rehak et al. (2019)	V. Vasylius et al.	D. Rehak et al. (2020)	G. Cáceres	B. Leitner et al.	A. Fekete et al.
Критична інфраструктура			+	+		+	+	+	+
Критичні активи	+								
Ідентифікація						+			
Критерій								+	+
Інфраструктурні мережі	+								
Система критичної інфраструктури		+							
Призначення		+							
Критичні елементи (у т. ч. регіональні)		+	+	+	+	+		+	
Аналіз безпекового середовища			+						
Ризики безпеки			+				+		
Адаптивність				+					
Відновлюваність				+					
Надійність				+					
Резильєнтність				+	+				
Захист критичної інфраструктури					+				
Каскадні ефекти						+			
Національна оборона та безпека							+		
Оцінювання ризиків								+	+
Ризик-менеджмент									+
Стратегія									+

Джерело: складено авторами на основі даних [1–5; 7–10].

нева система стратегічно значущих матеріальних і нематеріальних ресурсів національної інфраструктури. До її складу належать підприємства й установи різних форм власності, а також їхня майнова база та результати функціонування. Вказана система є фундаментом для стабільного функціонування життєво важливих галузей, серед яких: енергетика; ядерна та хімічна промисловість; транспортно-комунікаційний комплекс; банківсько-фінансова сфера; інформаційно-телекомунікаційні системи; продовольче забезпечення; охорона здоров'я; сфера житлово-комунального господарства [12].

У науковому дискурсі сформувався різноманітний арсенал методів і критеріїв, які розроблено та апробовано дослідниками (Д. Бірюков, С. Кондратов [15]; Д. Бобро [16]; А. Корченко, В. Козачок, А. Гізун [17]; О. Мельничук [18]; Л. Щербак [19]) задля ідентифікації об'єктів критичної інфраструктури, що дозволяє забезпечити системність і обґрунтованість процесів їх віднесення до відповідної категорії.

У дослідженнях Л. Щербака [19] критична інфраструктура представлена як комплекс стратегічно важливих об'єктів, що охоплюють енергетичні та транспортні магістральні мережі, нафто- і газопроводи, морські порти, канали урядового та швидкісного зв'язку, системи життєзабезпечення мегаполісів, високотехнологічні виробничі підприємства, установи військово-промислового комплексу та центральні органи державної влади. Учений підкреслює, що пріоритетним аспектом є не лише ідентифікація зазначених об'єктів, але й визначення рівня їхньої критичності з огляду на потребу у безперебійному функціонуванні та мінімізації ризиків виникнення збоїв в автоматизованих системах, що забезпечують їхню роботу [19].

У 2015 р. колектив науковців Національного інституту стратегічних досліджень із залученням українських і зарубіжних експертів і за підтримки Офісу зв'язку НАТО в Україні підготували «Зелену книгу з питань захисту критичної інфраструктури в Україні» [20], у якій надали пропозиції щодо переліку секторів критичної інфраструктури. До ключових секторів критичної інфраструктури віднесено такі: паливно-енергетичний комплекс, транспорт, мережі життєзабезпечення, телекомунікації та зв'язок, фінансово-банківський сектор, органи влади та правопорядку, сектор безпеки і оборони, хімічна промисловість, служба екстреної допомоги та цивільного захисту, харчова промисловість та агропромисловий комплекс [20].

З точки зору О. Мельничука [18], можна виділити п'ять основних методологічних підходів до ідентифікації об'єктів критичної інфраструктури, а саме: ризик-орієнтований, модельний, експертний, соціологічний та комбінований (табл. 2).

Як підкреслює автор [18], ідентифікація рівня критичності інфраструктурного об'єкта передбачає багатовимірний аналітичний підхід, що охоплює три взаємопов'язані площини: по-перше, внутрішню системну спроможність, яка зумовлюється специфічними характеристиками та

Таблиця 2

Підходи та методи ідентифікації об'єктів критичної інфраструктури

Підходи	Характеристика
Ризик-орієнтований підхід	Здійснення розрахунків частоти проявлення небезпек, тобто ймовірнісний аналіз небезпеки та наслідків. До переліку «критичних» об'єктів віднесено ті об'єкти інфраструктури, які отримають найвище значення за результатами оцінки «критичності»
Модельний підхід	Об'єкти дослідження, особливо якщо вони недоступні чи втручання в їх роботу неможливе, замінюються відповідними моделями, за допомогою яких вивчається їх характеристики, поведінка та реакція при зміні параметрів внутрішнього і зовнішнього середовища
Метод експертних оцінок (метод Дельфі)	Визначення ймовірності критичності різних об'єктів інфраструктури досвідченими фахівцями-експертами
Соціологічний підхід	Проведення соціологічного дослідження з метою вирішення наявної соціальної проблеми розвитку критичної інфраструктури
Комбінований підхід	Поєднання індивідуальних і колективних експертних оцінок і використання дослідницьких способів, що включає в себе одночасно два або більше із вищенаведених методів

Джерело: складено авторами на основі опрацювання [18].

потенційними відхиленнями у разі порушення режиму його функціонування; по-друге, оцінювання зовнішніх детермінант впливу, що формують додаткові ризики для стабільності об'єкта; по-третє, дослідження його взаємозалежностей з іншими елементами інфраструктурної мережі з огляду на можливість виникнення «каскадних» ефектів у разі відмови. У межах такого підходу критичність доцільно розглядати крізь призму трьох універсальних атрибутів – структурних складових, часових параметрів та якісних характеристик [18]. Відповідно, процес оцінювання критичності інфраструктурних об'єктів потребує врахування необхідності уточнення наслідків, пов'язаних із деградацією або збоїм у роботі, при цьому виключаючи непрямі ефекти; аналізу зовнішніх впливів, що виходять за межі безпосереднього місця відмови; а також інтеграції результатів оцінки взаємозалежностей і потенційних каскадних наслідків для забезпечення цілісної характеристики об'єкта [18].

Д. Бірюков та С. Кондратов [15] зазначають, що процес категоризації об'єктів критичної інфраструктури забезпечує можливість розроблення та застосування диференційованих підходів до їхньої безпеки. При цьому враховуються як рівень потенційної загрози реалізації акту незаконного втручання чи терористичного акту, так і прогнозовані масштаби негативних наслідків для суспільства та держави [15].

При цьому варто зазначити, що, на думку значної кількості провідних українських науковців і фахівців (Л. Арсенович [21]; Д. Бірюков, С. Кондратов [15]; Д. Бірюков, С. Кондратов, О. Насвіт, О. Суходоля [20]; І. Гора [22]), гарантування захищеності та стійкості критичної інфраструктури належить до стратегічних векторів державної політики у сфері національної безпеки. Так, Л. Арсенович [21] акцентує увагу на необхідності вдосконалення захисту критичної інфраструктури в системі національної безпеки України шляхом запровадження в умовах воєнного стану «моделі взаємодії і координації». Науковець зазначає, що підвищення концентрації ресурсів і засобів для охорони інфраструктурних об'єктів різних типів зумовило потребу в їх класифікації та послідовному впорядкуванні, що призвело до появи самого поняття «критична інфраструктура» [21].

Системний аналіз наукових публікацій свідчить про посилення уваги дослідницької спільноти до створення багатовимірного методологічного апарату, що поєднує підходи, методи, критерії та індикатори ідентифікації об'єктів критичної інфраструктури. Цей інструментарій має на меті забезпечення їх надійності, безперервності функціонування та стійкості до зовнішніх і внутрішніх загроз. Водночас літературний огляд та одержані результати власних попередніх досліджень [23; 24] підтверджують необхідність продовження подальших розробок і напрацювань у цій сфері в умовах трансформації міжнародного безпекового середовища [25] та зростання кількості загроз [26; 27] різного рівня та характеру.

З огляду на зазначене, **мета цієї статті** полягає в ідентифікації основних підходів до визначення критично важливих об'єктів інфраструктури на основі опрацювання та узагальнення зарубіжного та українського досвіду в цій сфері. Для досягнення поставленої мети застосовано комплекс наукових підходів і методів, серед яких: порівняльний аналіз, метод класифікації, структурно-логічного узагальнення, а також системний, ризик-орієнтований і модельний підходи.

Дослідження зарубіжного досвіду свідчить, що формування методологічних засад ідентифікації об'єктів, систем і сервісів, віднесених до критичних на національному рівні, а також створення комплексної бази даних для їх реєстрації є надзвичайно складним завданням. Така складність зумовлена значною неоднорідністю об'єктів і систем, які належать до різних секторів критичної інфраструктури, їх масштабною кількістю, а також необхідністю врахування широкого спектра характеристик з огляду на можливі загрози різного походження.

Критична інфраструктура охоплює велику кількість різнорідних об'єктів, що для забезпечення їх системності та керованості підлягають секторальному групуванню. Водночас як кількісні параметри виокремлених секторів, так і принципи їхньої класифікації значною мірою залежать від методологічних підходів, що застосовуються у конкретних країнах. Така варіативність зумовлена відмінностями у рівні соціально-економічного розвитку, структурі національних економік, особливостях регуляторної політики та спектрі актуальних загроз, що обумовлює різні підходи до визначення складу та меж секторів критичної інфраструктури [28] (табл. 3).

Аналіз переліку секторів критичної інфраструктури в країнах-членах ОЕСР [28] (див. табл. 3) показує, що існує універсальне ядро секторів, яке визнається критично важливим практично в усіх державах. До нього належать енергетика, транспорт, інформаційно-комунікаційні технології, фінансова система, державне управління та охорона здоров'я. Ці сфери визначаються як базові елементи життєзабезпечення суспільства та функціонування держави.

Таблиця 3

Перелік секторів критичної інфраструктури у країнах-членах Організації економічного співробітництва та розвитку

Країна	Сектори критичної інфраструктури																
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Австралія	+		+	+	+	+	+	+	+		+		+		+		
Австрія	+		+	+	+		+	+	+	+	+	+	+				+
Бельгія	+		+	+	+			+	+					+			+
Велика Британія	+	+	+	+	+		+	+	+	+	+	+	+	+	+		+
Греція	+		+	+													
Естонія	+		+		+			+	+								+
Ізраїль	+	+	+	+	+		+	+	+	+	+	+	+		+	+	+
Ірландія	+		+	+		+											
Ісландія	+		+	+		+											
Іспанія	+	+	+	+	+		+	+	+	+	+		+	+			+
Італія	+		+	+		+											
Канада	+	+	+	+	+		+	+	+	+	+					+	
Латвія	+		+	+	+	+		+	+	+	+	+	+		+		+
Люксембург	+		+	+	+		+	+	+	+	+	+	+				+
Мексика	+		+	+		+											
Нідерланди	+	+	+	+	+	+			+		+	+	+				+
Німеччина	+		+	+	+		+	+	+	+	+	+					+
Нова Зеландія	+		+	+	+												+
Норвегія	+	+	+	+	+	+	+	+	+	+	+	+	+			+	+
Південна Корея	+	+	+	+	+	+		+	+	+							+
Польща	+		+	+	+		+	+	+	+			+				+
Португалія	+			+													
Словаччина	+		+	+	+			+	+				+				
Словенія	+		+	+		+											

Закінчення табл. 3

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Сполучені Штати Америки	+	+	+	+	+	+	+	+	+	+	+		+		+	+	+
Туреччина	+		+	+		+	+	+	+							+	+
Фінляндія	+		+	+	+		+	+	+				+		+	+	+
Франція	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+
Чехія	+	+	+	+	+	+	+	+	+	+	+						
Чилі	+		+	+		+		+				+					
Швейцарія	+		+	+	+		+	+	+	+	+		+				
Швеція	+		+	+			+	+	+	+	+						+

Примітки: (1) енергетика; (2) ядерний сектор; (3) інформаційно-комунікаційні технології; (4) транспорт; (5) водопостачання; (6) дамби для захисту від повеней; (7) постачання та розподіл продовольства; (8) сфера охорони здоров'я; (9) фінанси і банківська система; (10) державне управління; (11) громадська безпека; (12) правоохоронна діяльність; (13) хімічна промисловість; (14) космічний сектор; (15) оборонна промисловість; (16) критичне виробництво; (17) інші сектори.

Джерело: складено авторами на основі опрацювання [28].

Водночас простежуються суттєві відмінності у широті охоплення секторів. Так, Велика Британія, Іспанія, Канада, Німеччина, США, Франція включають понад 10 секторів, що свідчить про високий рівень деталізації та комплексний підхід до захисту. Натомість країни з меншою економічною диверсифікацією (Греція, Ірландія, Ісландія, Нова Зеландія, Португалія) обмежуються 3-5 секторами [28].

Специфічними для окремих держав є ядерний сектор (Велика Британія, Ізраїль, Канада, Нідерланди, США, Франція); дамби та водні споруди (Австралія, Ірландія, Ісландія, Італія, США); космічний сектор (Бельгія, Велика Британія, Франція) та оборонна промисловість (Велика Британія, Латвія, США, Фінляндія, Франція) [28]. Це свідчить про залежність визначення критичності від національних пріоритетів і стратегічних викликів.

Загалом можна констатувати тенденцію до розширення переліку секторів у більшості країн світу. Вибір залежить від рівня розвитку економіки, геополітичного положення та безпекових загроз. Таким чином, попри універсальність базових секторів, системи критичної інфраструктури залишаються національно специфічними, що зумовлює потребу у виробленні міжнародних стандартів захисту з можливістю їхньої адаптації до локальних умов.

Слід наголосити, що у контексті складної та багатовимірної безпекової ситуації на Близькому Сході, особливе значення для наукових досліджень і практики державного управління має ізраїльський досвід ідентифікації критичної інфраструктури. У цій країні напрацьовано підхід, що ґрунтується на виокремленні трьох ключових ознак, які визначають критерії віднесення об'єктів до категорії критично важливих.

По-перше, розглядається символічна значущість інфраструктурних об'єктів, яка відображає їхню роль у збереженні національної ідентичності та культурної спадщини [15]. Саме з цієї причини до числа пріоритетних для захисту включаються музеї, архіви, культові споруди та інші пам'ятки, які виступають маркерами колективної пам'яті та ідентичності суспільства. Ізраїльські фахівці також відносять до цієї групи інформаційні ресурси, що забезпечують легітимність і стабільність державної влади: офіційні сайти урядових органів, центральні засоби масової інформації та інші комунікаційні платформи. Їхня втрата, навіть за відсутності безпосередніх фізичних руйнувань, здатна суттєво підірвати довіру населення та завдати відчутного удару по міжнародному іміджу держави.

По-друге, враховується ступінь залежності базових процесів життєзабезпечення населення від функціонування певних інфраструктур [15]. У межах цього критерію критично важливими визнаються системи електропостачання (лінії електропередач), водопостачання і водовідведення, а також телекомунікаційні мережі загального користування, які забезпечують координацію та управління іншими секторами. Втрата або порушення функціонування зазначених систем здатні призвести до дестабілізації суспільного життя та унеможливити виконання державою своїх базових функцій.

По-третє, важливою умовою виступає наявність системних взаємозв'язків між різними об'єктами інфраструктури та ризик виникнення каскадних ефектів у разі відмови окремих елементів [15]. Ізраїльські експерти наголошують, що інфраструктури функціонують у тісній взаємодії, і відмова одного сегмента може спричинити ланцюгову реакцію з негативними наслідками для інших секторів. Водночас вони відзначають, що глибинний характер цих взаємозалежностей досі вивчений неповною мірою, а комплексна оцінка потенційних ризиків залишається відкритим завданням для науковців і практиків.

Таким чином, ізраїльська модель ідентифікації критичної інфраструктури відзначається комплексним і багаторівневим характером: вона поєднує культурно-символічний, функціонально-економічний і системно-структурний виміри, що дозволяє розглядати інфраструктуру не лише як технічну чи матеріальну основу життєзабезпечення, але й як ключовий чинник забезпечення національної безпеки та стійкості держави.

Як свідчить аналіз, цікавим і корисним є досвід європейських країн, у яких на сьогодні використовуються різноманітні методології ідентифікації об'єктів критичної інфраструктури. Консорціум під керівництвом голландської дослідницької організації TNO [29] умовно класифікував існуючі методики за трьома основними типами:

1) підхід, який засновано на послугах (наприклад, Швейцарія), де уряд ідентифікує критично важливі активи на підставі галузевих критеріїв, що визначають порогові значення/рівень обслуговування активів;
2) підхід, який засновано на операторі (наприклад, Франція), де завдання визначення того, які активи чи послуги є критично важливими, залишається за окремими операторами критично важливих об'єктів інфраструктури;
3) підхід, що засновано на активах або гібридах (наприклад, у Великій Британії), у якому використовуються елементи підходів, орієнтовані як на послуги, так і на оператора.

Методологічні засади ідентифікації критично важливих об'єктів інфраструктури закріплено у Директиві Ради ЄС 2008/114/ЄС від 8 грудня 2008 р. «Про ідентифікацію та позначення європейських критично важливих інфраструктур та оцінювання потреби у підвищенні рівня їхнього захисту» [30]. Попри те, що формально дія цього документа поширюється лише на об'єкти транспортної та енергетичної сфер, у ньому опосередковано закладено можливість використання визначених підходів і для національного рівня, включно з іншими секторами.

Методологія передбачає послідовне проходження кількох етапів [30; 31] (табл. 4).

Таблиця 4

Етапи методології ідентифікації критично важливих об'єктів інфраструктури в ЄС

Етап	Зміст етапу	Ключові акценти
1. Галузевий відбір	Використання галузевих критеріїв для попереднього визначення критичних інфраструктур у межах сектору	Сектори: енергетика, транспорт (з можливістю поширення на інші)
2. Визначення потенційних ЄКВОІ	Застосування визначення критично важливої інфраструктури відповідно до ст. 2(a) Директиви	Оцінка значення впливу: національні методи + міжсекторальні критерії. Для систем життєзабезпечення: наявність альтернатив, час збоїв/відновлення
3. Транскордонний критерій	Ідентифікація об'єктів, що мають вплив за межами однієї держави-члена ЄС (ст. 2(b) Директиви)	Увага до інфраструктур життєзабезпечення: альтернативність, тривалість наслідків перебоїв
4. Міжгалузева перевірка	Застосування міжгалузевих критеріїв для остаточного відбору потенційних європейських критично важливих об'єктів інфраструктури (ЄКВОІ)	Критерії: масштаб впливу, наявність альтернатив, час збою/відновлення. Об'єкти, що відповідають, повідомляються тим країнам ЄС, на які вони справляють значний вплив

Джерело: складено авторами на основі опрацювання [30; 31].

Як видно з табл. 4, представлена у Директиві Ради ЄС 2008/114/ЄС [30] чотирьохетапна методологія ідентифікації критично важливих об'єктів інфраструктури дає змогу забезпечити комплексний та системний підхід до відбору об'єктів, які становлять загальноєвропейське значення. Її зміст передбачає поєднання галузевого та міжгалузевого аналізу, що дозволяє враховувати як специфіку окремих секторів (енергетика, транспорт), так і взаємозалежність між ними.

Ключовим у цьому процесі є врахування транскордонного елементу, адже значна частина інфраструктур має потенціал впливати не лише на національний, а й на регіональний рівень безпеки. Це особливо актуально для систем життєзабезпечення, де тривалість збою або відновлення та наявність альтернативних рішень визначають масштаб можливих наслідків.

Отже, методологія ЄС формує підґрунтя для: 1) уніфікації підходів до ідентифікації критичної інфраструктури на рівні держав-членів; 2) забезпечення прозорих критеріїв відбору об'єктів з урахуванням їхньої важливості; 3) підвищення рівня захищеності та стійкості інфраструктур, що мають стратегічне значення для функціонування Європейського Союзу.

Делегований Регламент Комісії (ЄС) 2023/2450 від 25 липня 2023 року [32], ухвалений на підставі Директиви Європейського Парламенту та Ради (ЄС) 2022/2557 «Про стійкість критично важливих об'єктів» [33], визначає невичерпний перелік основних послуг, що мають вирішальне значення для забезпечення життєво важливих суспільних функцій та економічної діяльності (табл. 5). Згідно з положеннями статті 5(1) зазначеної Директиви, перелік послуг має використовуватися компетентними органами держав-членів ЄС як базовий інструмент для проведення оцінки ризиків, що, у свою чергу, слугує підґрунтям для визначення критично важливих суб'єктів [32].

Особливістю підходу Європейської Комісії є те, що цей перелік сформульовано у загальних категоріях, з урахуванням можливих відмінностей держав-членів за розміром, щільністю населення чи географічним розташуванням. Водночас він обмежується лише тими послугами, які надаються суб'єктами, визначеними у Додатку до Директиви (ЄС) 2022/2557 [33], і відповідають критеріям «основних послуг» у розумінні статті 2(5) цієї Директиви. Крім того, Регламент уточнює, що поняття «основні послуги» слід тлумачити у контексті ширших положень Директиви, а саме як послуги,

Таблиця 5

Основні сектори та послуги згідно з Делегованим Регламентом Комісії (ЄС) 2023/2450

Сектор	Основні послуги
Енергетика	Постачання електроенергії; експлуатація, обслуговування та розвиток систем розподілу й передачі; генерація; ринок електроенергії; зберігання енергії; постачання, транспортування, виробництво, зберігання та переробка нафти й газу; виробництво, транспортування та зберігання водню; централізоване теплопостачання й охолодження
Транспорт	Авіаційні перевезення та управління аеропортами; залізничні перевезення та управління інфраструктурою; водний транспорт і діяльність портів; автомобільні перевезення та управління дорожнім рухом; громадський пасажирський транспорт
Банківський сектор	Прийом депозитів і кредитування (банківські установи)
Фінансова ринкова інфраструктура	Функціонування торговельних майданчиків; робота клірингових систем
Охорона здоров'я	Надання медичних послуг; діяльність референс-лабораторій ЄС; дослідження і розробка лікарських засобів; виробництво фармацевтичних препаратів і медичних виробів; дистрибуція лікарських засобів
Питна вода	Забезпечення та розподіл питної води
Водовідведення	Збирання, очищення та утилізація стічних вод
Цифрова інфраструктура	Інтернет-обмінні пункти (IXP); послуги DNS; реєстри доменів верхнього рівня (TLD); хмарні обчислення; дата-центри; мережі доставки контенту (CDN); довірчі послуги; електронні комунікаційні послуги та мережі
Державне управління	Послуги центральних органів влади, визначених законодавством держав-членів
Космічний сектор	Функціонування наземної інфраструктури, що забезпечує надання космічних послуг
Виробництво, переробка та розподіл продуктів харчування	Великомасштабне виробництво та переробка продуктів харчування; послуги ланцюгів постачання (зберігання, логістика); гуртовий розподіл харчових продуктів

Джерело: складено авторами на основі опрацювання [32; 33].

що забезпечують функціонування суспільно значущих сфер, економіки, громадського здоров'я, безпеки та охорони довкілля [32]. При цьому підкреслюється, що сфера застосування Директиви не поширюється на діяльність органів державного управління, пов'язану з національною безпекою, обороною, громадською безпекою та правоохоронними функціями.

Розглянемо передові практики деяких європейських країн щодо ідентифікації об'єктів критичної інфраструктури. Так, у 2014 році в Нідерландах було здійснено масштабну реформу державної політики у сфері забезпечення стійкості критичної інфраструктури. Ключовим результатом цих змін став перехід від традиційного підходу, заснованого на визначенні «критично важливих секторів», до більш функціонально орієнтованої концепції «критично важливих процесів» [29].

Під критично важливими процесами розуміють ті види діяльності, відмова чи порушення яких здатні спричинити суттєві соціальні дестабілізаційні наслідки. На відміну від секторального підходу, де вся галузь визначалася як критично важлива, сучасна модель дозволяє виокремлювати лише ті процеси, що становлять реальну загрозу у разі їх зупинки. Це забезпечує можливість більш цілеспрямованого та раціонального використання наявних інструментів і ресурсів [34].

Оцінка рівня критичності процесів здійснюється відповідно до встановлених критеріїв впливу, зокрема економічних збитків, масштабів фізичних наслідків і соціальних ризиків. Водночас система оцінки є динамічною: трансформація суспільних відносин, еволюція спектра загроз чи результати аналізу попередніх інцидентів можуть стати підставою для перегляду переліку процесів, віднесених до категорії критично важливих [35].

З метою підвищення ефективності управління ризиками передбачено класифікацію критично важливих процесів за двома рівнями значущості – категоріями **А** та **В**. Процеси категорії А мають більш вагомий потенційний ефект від відмови, ніж процеси категорії В. Такий поділ використовується для визначення пріоритетності реагування під час кризових ситуацій, а також для ухвалення рішень щодо розподілу ресурсів і розроблення заходів із посилення стійкості інфраструктури [34].

До категорії А віднесено: національне транспортування та розподіл електроенергії; видобу-

ток природного газу; постачання нафти; зберігання, виробництво та переробку ядерних матеріалів; питне водопостачання; управління водними ресурсами.

До категорії В належать: регіональне розподілення електроенергії та газу; управління повітряним рухом і польотами; управління морськими та внутрішніми перевезеннями ресурсів; фінансовий сектор (банківські послуги, електронні перекази між банками та з населенням); взаємодія аварійно-рятувальних служб; мобілізація поліції; державні послуги, що ґрунтуються на безперебійному функціонуванні цифрових інформаційних систем і систем обробки даних [34; 35].

Відповідальність за проведення оцінки критично важливих процесів покладається на профільні міністерства. При цьому координаційну функцію виконує Міністерство юстиції та безпеки, яке здійснює регулярний перегляд методологічних підходів, аби забезпечити їхню актуальність, а також визначає необхідність включення нових процесів до переліку критично важливих.

У Німеччині система критичної інфраструктури структурована у дві великі групи секторів, які разом охоплюють дев'ять складових. Перша група – це життєво необхідна базова технічна інфраструктура, до якої належать енергетичне забезпечення, інформаційні та комунікаційні технології, транспортна система, водопостачання та системи утилізації побутових відходів. Друга група – життєво необхідна інфраструктура соціально-економічних послуг, що включає охорону здоров'я та продовольче забезпечення, служби екстреної допомоги й аварійно-рятувальні формування, органи управління у надзвичайних ситуаціях, інститути політичного управління (парламент, уряд, державні органи влади, правоохоронні структури), фінансовий та страховий сектор, засоби масової інформації й об'єкти культурної спадщини [20; 35].

Особливістю німецької моделі є високий рівень взаємозалежності між цими двома групами секторів. Соціально-економічні служби у своїй діяльності значною мірою спираються на стабільне функціонування базової технічної інфраструктури (зокрема електроенергії, телекомунікацій чи транспортних мереж). Водночас технічна інфраструктура не може повноцінно функціонувати без належного забезпечення соціально-економічними послугами, такими як правова підтримка, діяльність органів державної влади, медичні установи чи служби екстреного реагування [20; 35].

У Франції державна політика у сфері захисту критичної інфраструктури ґрунтується не на безпосередній ідентифікації окремих активів, а на визначенні так званих *«життєво важливих операторів»* (ЖВО) [35]. Саме на них покладається відповідальність за подальше виявлення та класифікацію об'єктів, що мають стратегічне значення. Відповідно до положень **Кодексу оборони**, уповноважений міністр – координатор галузі – призначає оператора життєво важливим суб'єктом після консультацій з іншими відповідними міністерствами. Процедура призначення починається з офіційного повідомлення потенційного оператора, яке водночас слугує підставою для консультаційного діалогу між державою та приватним суб'єктом.

Статус ЖВО надається за умови дотримання двох ключових критеріїв [36]:

- діяльність оператора повністю або частково належить до сфери, яка визнається життєво важливою;
- оператор здійснює управління хоча б однією інституцією, інфраструктурою чи об'єктом, виведення з ладу яких унаслідок терористичних актів, диверсій чи інших зловмисних дій може призвести до загрози виживанню нації, здоров'ю чи життю населення.

Статус «життєво важливого об'єкта» можуть отримати: 1) асоціації, фонди та міжнародні організації; 2) державні служби, органи місцевого самоврядування та їхні об'єднання, державні установи, незалежні адміністративні органи; 3) у разі корпоративної структури – материнські або дочірні компанії (причому кілька дочірніх структур однієї групи також можуть бути визнані ЖВО) [36].

Призначення здійснюється після консультацій з оператором, а якщо відповідальність перетинається між кількома міністерствами, визначається координатор. Зазвичай координуюче міністерство відповідає за сектор, у якому оператор здійснює основну діяльність. При цьому ЖВО може делегувати частину функцій на умовах субпідряду чи аутсорсингу, але він зобов'язаний забезпечити, щоб партнери дотримувалися стандартів безпеки та сприяли зміцненню захисту критичної інфраструктури. Важливим обов'язком ЖВО є розроблення *«планів безпеки оператора»,* які включають аналіз ризиків та перелік об'єктів, запропонованих до віднесення у категорію життєво важливих [36].

На відміну від Франції, у Великій Британії застосовується секторальний підхід. Держава виокремлює *дев'ять критично важливих секторів і двадцять підлеглих критичних служб***,** що, своєю чергою, охоплюють активи, які підлягають ідентифікації. Міністерства, відповідальні за сектори, здійснюють початковий відбір активів та операто-

рів, базуючись на їхній ринковій частці. Паралельно Центр захисту національної інфраструктури проводить власну незалежну оцінку. На підставі узгоджених даних формується перелік активів і процесів, чия відмова може спричинити системні наслідки [35].

Для класифікації використовується шестирівнева шкала критичності – від CAT0 до CAT5. Вона ґрунтується на трьох міжгалузевих критеріях [35]:

- вплив на життя населення;
- економічні наслідки;
- вплив на надання життєво важливих послуг.

На відкритому рівні ці критерії мають описовий та якісний характер, тоді як на класифікованому рівні їм надано кількісні показники для об'єктивного вимірювання. Додатково застосовуються специфічні критерії, що відрізняються залежно від сектора.

У результаті формується обмежений перелік активів із найвищим рівнем критичності. Лише ті, що належать до категорії 3 і вище, визнаються справді критично важливими. Остаточна пріоритизація здійснюється шляхом поєднання рівня критичності (CAT) із показниками ймовірності атаки, що визначається на основі оцінки вразливостей та конкретних типів загроз. При цьому масштаб ймовірності є динамічним і може переглядатися кілька разів на рік залежно від актуальних ризиків [35].

Необхідно підкреслити, що порівняльний аналіз підходів Франції та Великої Британії до ідентифікації критично важливих елементів інфраструктури свідчить про наявність принципових відмінностей у методологічних засадах. Франція орієнтується на інституційно-організаційний підхід, у центрі якого перебуває життєво важливий оператор (ЖВО). Саме оператори несуть відповідальність за виявлення активів та розроблення планів безпеки, що забезпечує високий рівень гнучкості та партнерську взаємодію між державою і приватним сектором. Такий підхід спрямований на децентралізоване управління ризиками та врахування особливостей діяльності конкретних суб'єктів.

Велика Британія, навпаки, застосовує секторально-ієрархічну модель, у межах якої держава визначає перелік критичних секторів та служб, а активи піддаються багаторівневій оцінці критичності за єдиними критеріями. Ключову роль відіграють державні інституції (міністерства та Центр захисту національної інфраструктури), що здійснюють відбір і класифікацію. Такий підхід є більш централізованим та стандартизованим, що дозволяє формувати обмежений, але надзвичайно пріоритетний перелік об'єктів.

Отже, французька модель забезпечує більшу адаптивність та відповідальність операторів, тоді як британська система відзначається високим рівнем уніфікації та жорсткою пріоритизацією активів. Обидва підходи є взаємодоповнювальними з точки зору сучасної практики захисту критичної інфраструктури: перший надає можливість врахувати галузеву специфіку, другий – забезпечує стратегічну концентрацію ресурсів на об'єктах найвищої критичності.

Розглянемо досвід України щодо ключових аспектів ідентифікації критично важливих об'єктів інфраструктури.

Слід зауважити, що уряд України, спираючись на передову закордонну практику, приділяє значну увагу вдосконаленню нормативно-правового забезпечення розвитку критичної інфраструктури та розробленню відповідних методичних рекомендацій щодо категоризації її об'єктів. І особливої актуальності ці питання набули у воєнний період.

У Концепції забезпечення національної системи стійкості, яку затверджено Указом Президента України від 27.09.2021 р. № 479/2021 [37], зазначено, що безпеку та захищеність об'єктів критичної інфраструктури визнано одним із базових елементів національної системи стійкості. І до об'єктів критичної інфраструктури, функціонування яких має забезпечити розвиток національної системи стійкості та економіки країни в цілому, віднесено: 1) стійке постачання продовольства, водопостачання, енергопостачання, постачання теплової енергії; 2) стійке функціонування транспортних систем; 3) кібербезпеку; 4) захищеність та безперебійне функціонування інформаційних і комунікаційних послуг; 5) забезпечення оборони та правопорядку; 6) здатність системи охорони здоров'я функціонувати в умовах посилених навантажень [37].

У Законі України від 16.11.2021 р. № 1882-IX «Про критичну інфраструктуру», розрізнять такі поняття, як «ідентифікація об'єкта критичної інфраструктури», «категоризація об'єктів інфраструктури», «категорія критичності (критерії) об'єкта критичної інфраструктури», «реєстр об'єктів критичної інфраструктури», «рівень критичності об'єкта критичної інфраструктури», «сектор критичної інфраструктури» [38] (табл. 6).

Відповідно до ст. 9 Закону України від 16.11.2021 р. № 1882-IX «Про критичну інфраструктуру» для забезпечення цілісності національної системи захисту та підтримання стійкості критичної інфраструктури, з урахуванням функціональної специфіки реалізації життє-

Таблиця 6

Визначення основних термінів, які стосуються ідентифікації об'єктів критичної інфраструктури згідно із Законом України «Про критичну інфраструктуру»

Термін	Визначення
Ідентифікація об'єкта критичної інфраструктури	процедури віднесення об'єкта інфраструктури до об'єктів критичної інфраструктури
Категоризація об'єктів інфраструктури	віднесення об'єктів інфраструктури до категорій критичності об'єктів інфраструктури
Категорія критичності (критерії) об'єкта критичної інфраструктури	ступінь (відносний рівень) важливості об'єкта критичної інфраструктури, класифікована (категоризована) залежно від його впливу на виконання життєво важливих функцій та/або надання життєво важливих послуг
Реєстр об'єктів критичної інфраструктури	автоматизована система, що містить перелік найбільш важливої для життєдіяльності суспільства та держави критичної інфраструктури, щодо якої встановлюються особливі вимоги із забезпечення її безпеки та стійкості і здійснюється моніторинг їх дотримання
Рівень критичності об'єкта критичної інфраструктури	відносна міра важливості об'єкта, якою враховується його вплив на можливість виконання життєво важливих функцій та надання життєво важливих послуг
Об'єкти критичної інфраструктури	об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам
Сектор критичної інфраструктури	сукупність об'єктів критичної інфраструктури, які належать до одного сектору (галузі) економіки та/або мають спільну функціональну спрямованість

Джерело: складено авторами на основі [38].

во важливих суспільних послуг, здійснюється виокремлення секторів критичної інфраструктури [38] (рис. 1).

Такий підхід забезпечує систематизацію та цільову спрямованість управлінських рішень у сфері національної безпеки. У межах визначених секторів окреслюються особливості формування та реалізації державної політики у сфері захисту критичної інфраструктури. Інституційне забезпечення цього процесу покладається на секторальні органи, які виконують координаційні та регуляторні функції, а також відповідають за створення і ведення секторальних переліків об'єктів критичної інфраструктури. Це сприяє впровадженню диференційованих механізмів управління ризиками та підвищенню рівня резильєнтності системи [38].

Як зазначається у законодавчому акті, перелік секторів критичної інфраструктури та коло суб'єктів, уповноважених на формування і реалізацію державної політики у відповідних сферах, визначається Кабінетом Міністрів України як центральним координуючим органом виконавчої влади [38]. З метою адаптації національної системи до динамічних внутрішніх і зовнішніх викликів, цей Перелік може підлягати періодичному перегляду та оновленню на основі критеріїв критичності, закріплених у законодавстві.

Таким чином, забезпечується гнучкість, відповідність актуальним загрозам і стратегічна стійкість системи публічного управління у сфері захисту критичної інфраструктури.

Як зазначено у ст. 10 Закону України від 16.11.2021 р. № 1882-IX «Про критичну інфраструктуру», для уніфікації підходів до визначення рівня вимог щодо забезпечення належного рівня захисту об'єктів критичної інфраструктури, відповідно до їх системоутворюючого значення у підтриманні життєво важливих функцій у межах відповідних секторів, здійснюється їх категоризація. Вона ґрунтується на принципі диференціації рівня критичності та реалізується за категоріями [38], які наведено у табл. 7.

Процедура категоризації об'єктів критичної інфраструктури покладається на секторальні органи у сфері їх захисту, які здійснюють її з урахуванням галузевої специфіки, нормативно-правових вимог профільного законодавства та критеріїв оцінки рівня критичності [38]. Категоризація у межах відповідних секторів (підсекторів) критичної інфраструктури здійснюється у взаємодії секторальних органів та операторів

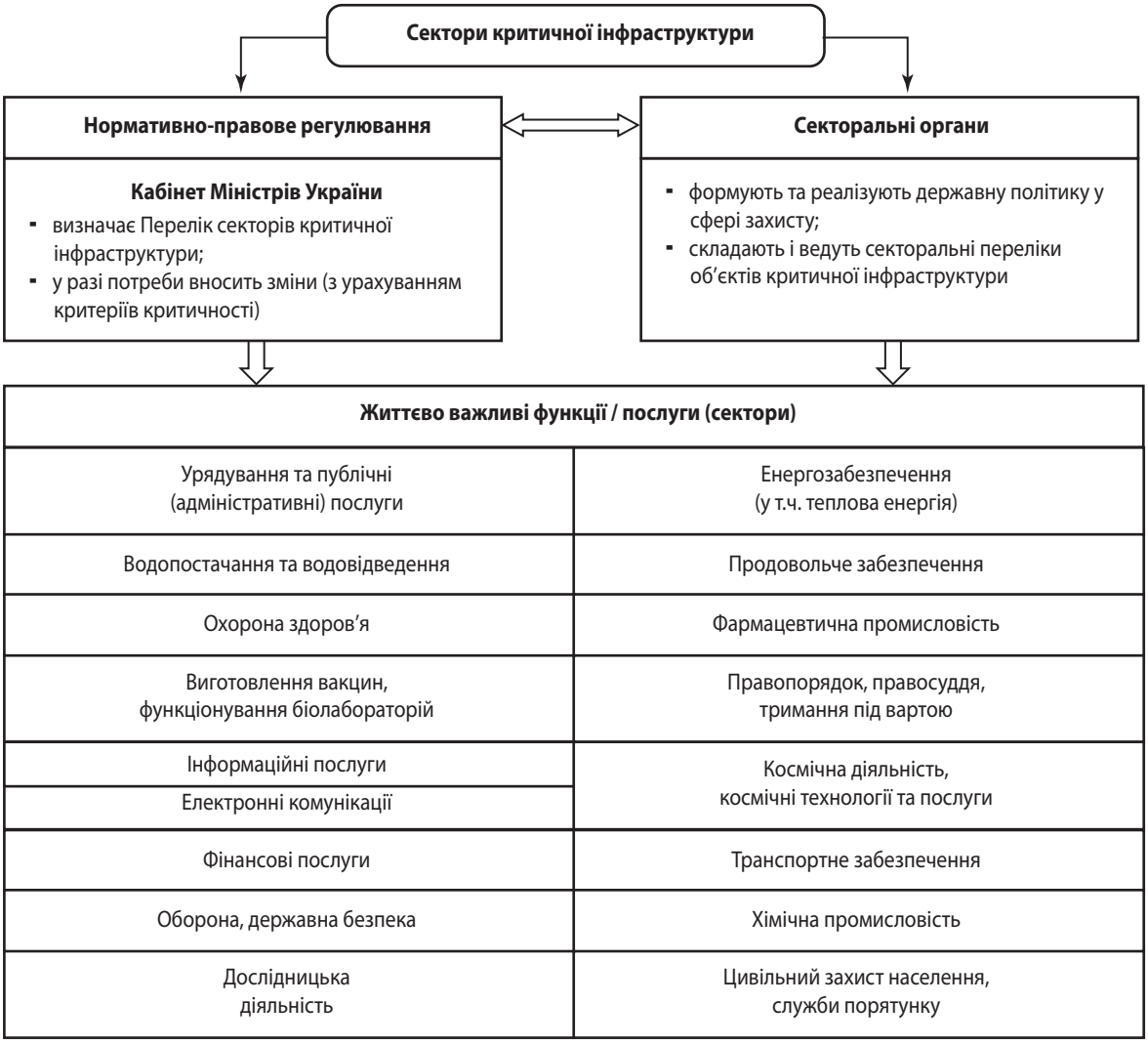

Рис. 1. Структурна схема секторів критичної інфраструктури згідно із Законом України від 16.11.2021 р. № 1882-IX «Про критичну інфраструктуру»

Джерело: побудовано авторами на основі опрацювання [38].

Таблиця 7

Законодавчо регламентовані категорії критичності об'єктів критичної інфраструктури в Україні

Категорії критичності	Сутність
I категорія	об'єкти стратегічного значення, які мають системоінтегруючу роль у масштабах держави, формують високий рівень взаємовпливу з іншими елементами критичної інфраструктури, а їх виведення з експлуатації чи суттєве порушення функціонування неминуче призводить до виникнення кризових явищ загальнодержавного характеру
II категорія	об'єкти життєвої важливості, що забезпечують стійкість функціонування на рівні адміністративно-територіальних одиниць, відмова або порушення діяльності яких зумовлює кризові процеси регіонального масштабу
III категорія	об'єкти локалізованого впливу, вихід з ладу яких створює загрозу безперервності функціонування у межах окремих громад або населених пунктів і провокує кризові явища місцевого рівня
IV категорія	об'єкти обмеженого значення, функціональна втрата чи порушення роботи яких призводить до кризової ситуації локального значення, що має вузькогалузевий або територіально обмежений характер

Джерело: побудовано авторами на основі опрацювання [38].

критичної інфраструктури на основі Методики категоризації об'єктів критичної інфраструктури, що затверджується Кабінетом Міністрів України. У банківсько-фінансовій системі її затвердження віднесено до компетенції Національного банку України. А у сферах, державне регулювання та нагляд за діяльністю яких здійснюють спеціально уповноважені органи, – до компетенції цих органів [38].

На цей час в Україні діє Постанова Кабінету Міністрів України від 09.10.2020 р. № 1109 «Деякі питання об'єктів критичної інфраструктури» (із змінами і доповненнями) [39], що містить Порядок віднесення об'єктів до критичної інфраструктури [40], у якому визначено перелік секторів критичної інфраструктури (табл. 8). Однак варто підкреслити, що дія цього Порядку не поширюється на:

- банківську та фінансову системи, категоризація об'єктів критичної інфраструктури яких здійснюється відповідно до методики, затвердженої Національним банком;
- сфери, державне регулювання і нагляд за діяльністю яких здійснюють державні органи, категоризація об'єктів критичної інфраструктури яких здійснюється відповідно до методики, затвердженої такими державними органами [40].

Таблиця 8

Сектори критичної інфраструктури України (за тематичними блоками)

Сектор / Підсектор	Секторальний орган у сфері захисту критичної інфраструктури
1	2
Економічний блок (економіка та ресурси)	
Паливно-енергетичний сектор: електроенергетика, вугільно-промисловий комплекс, торфодобування, нафтова промисловість, газова промисловість, ядерна енергетика, енергетичне машинобудування	Міністерство енергетики України
Промисловість: хімічна, металургійна, оборонна, космічна, авіаційна, суднобудівна	Міністерства з питань стратегічних галузей промисловості (ліквідовано). Міністерство оборони України
Харчова промисловість та агропромисловий комплекс	Міністерство аграрної політики та продовольства України (нині – Міністерство економіки, довкілля та сільського господарства України)
Транспорт і пошта: авіаційний, автомобільний та міський електричний, залізничний, морський та внутрішній водний транспорт, метрополітен, поштовий зв'язок	Міністерство розвитку громад та територій України
Системи життєзабезпечення	Міністерство розвитку громад та територій України
Державний матеріальний резерв	Міністерство економіки України (нині – Міністерство економіки, довкілля та сільського господарства України)
Ринки капіталу та організовані товарні ринки	Національна комісія з цінних паперів та фондового ринку
Фінансовий сектор	Міністерство фінансів України
Соціальний блок (соціальна сфера)	
Охорона здоров'я: медична допомога, громадське здоров'я, фінансове забезпечення у сфері охорони здоров'я, інформаційні технології у сфері охорони здоров'я, фармацевтична промисловість	Міністерство охорони здоров'я України
Соціальний захист: пенсійне забезпечення, соціальне страхування, соціальна допомога і соціальні послуги, інформаційна система соціальної сфери, реабілітація	Міністерство соціальної політики, сім'ї та єдності України
Вибори та референдуми	Центральна виборча комісія
Наукові дослідження та розробки	Міністерство освіти і науки України

Закінчення табл. 8

1	2
Безпековий блок (сфера національної безпеки та оборони)	
Сектор громадської безпеки	Міністерство внутрішніх справ України
Цивільний захист населення і територій	Державна служба України з надзвичайних ситуацій
Сектор оборони	Міністерство оборони України
Правосуддя	Державна судова адміністрація України
Виконання кримінальних покарань, тримання під вартою та утримання військовополонених	Міністерство юстиції України
Охорона навколишнього природного середовища: управління, використання та відтворення поверхневих водних ресурсів, розвиток водного господарства; поводження з радіоактивними відходами; охорона, раціональне використання і відтворення об'єктів природно-заповідного фонду	Міністерство захисту довкілля та природних ресурсів України (нині – Міністерство економіки, довкілля та сільського господарства України)
Управлінський блок (управління та технології)	
Цифрові технології: електронні довірчі послуги та електронна ідентифікація, електронні комунікації, електронне урядування	Міністерство цифрової трансформації України
Захист інформації	Державна служба спеціального зв'язку та захисту інформації України
Інформаційний сектор: медіа	Міністерство культури та стратегічних комунікацій України
Державна влада	Секретаріат КМУ
Державна реєстрація	Міністерство юстиції України
Фінансовий сектор: банківська система, ринок небанківських фінансових послуг (крім ринків капіталу та організованих товарних ринків), ринок платіжних послуг	Національний банк України

Джерело: побудовано авторами на основі опрацювання [40; 41].

Як видно з табл. 8, сектори критичної інфраструктури України [41] умовно систематизовано за чотирма ключовими блоками: економічним, соціальним, безпековим та управлінським. Така класифікація відображає багатовимірність підходів до забезпечення національної безпеки та сталого розвитку держави.

Економічний блок охоплює ті сектори, що забезпечують функціонування базових виробничих і ресурсних галузей. Зокрема, це паливно-енергетичний комплекс (електроенергетика, вугільна, нафтова, газова промисловість, ядерна енергетика та енергетичне машинобудування), промисловість (хімічна, металургійна, оборонна, авіаційна, суднобудівна тощо), агропромисловий сектор і харчова промисловість, транспорт і поштовий зв'язок, системи життєзабезпечення, державний матеріальний резерв, а також ринки капіталу та фінансовий сектор.

Соціальний блок відображає сектори, що безпосередньо стосуються забезпечення життєдіяльності населення. До нього включено охорону здоров'я (медична допомога, громадське здоров'я, фармацевтика), соціальний захист (пенсійне забезпечення, страхування, соціальні послуги, реабілітація), систему виборів і референдумів, а також наукові дослідження й розробки.

Безпековий блок структурований навколо секторів, які відповідають за збереження обороноздатності держави та захист суспільства від внутрішніх і зовнішніх загроз. Він включає громадську безпеку, цивільний захист населення і територій, оборону, правосуддя, систему виконання покарань і утримання військовополонених, а також сферу екологічної безпеки (водні ресурси, поводження з радіоактивними відходами, природно-заповідний фонд).

Управлінський блок зосереджений на функціях державного управління та технологічному забезпеченні. Серед підсекторів визначено цифрові технології (електронні довірчі послуги, е-урядування), захист інформації, інформаційний сектор (медіа), систему державної влади та державної реєстрації, а також фінансову систему у частині банківських і небанківських послуг. Для кожного напряму визначено відповідальні секторальні органи.

Отже, наведена класифікація секторів критичної інфраструктури України за чотирма блоками дозволяє комплексно оцінити архітектуру національної системи безпеки та стійкості. Такий підхід не лише відображає багатогранність сучасних викликів, але й дає змогу ідентифікувати ключові вразливості та пріоритети державної політики. Зокрема, економічний блок визначає основу функціонування національної економіки та енергетики; соціальний – гарантує безперервність життєво важливих послуг для населення; безпековий – фокусується на захисті та обороні. Тоді як управлінський блок забезпечує ефективність управління й розвиток цифрових технологій. У сукупності це створює системне підґрунтя для формування стратегій зміцнення національної безпеки та реалізації принципів сталого розвитку економіки України.

Крім цього, згідно з Постановою Кабінету Міністрів України від 09.10.2020 р. № 1109 «Деякі питання об'єктів критичної інфраструктури» (у редакції Постанови Кабінету Міністрів України від 16.12.2022 р. № 1384) [39] розроблено Методику, яка визначає механізм і критерії віднесення об'єкта критичної інфраструктури до однієї з категорій критичності [42].

У Методиці зазначено, що категорія критичності об'єкта критичної інфраструктури визначається на основі аналізу рівня негативного впливу, якого особа, суспільство, навколишнє природне середовище, економіка, національна безпека та обороноздатність країни можуть зазнати внаслідок порушення або припинення функціонування об'єкта інфраструктури відповідно до критеріїв [42].

Категорія об'єкта критичної інфраструктури визначається за процедурою, яку наведено на рис. 2.

Слід зазначити, що визначення категорії критичності об'єкта критичної інфраструктури здійснюється на основі інтегральної нормованої оцінки рівня його критичності за формулою, яку наведено у Методиці категоризації об'єктів критичної інфраструктури, затвердженій Постановою Кабінету Міністрів України від 09.10.2020 р. № 1109 (із змінами та доповненнями згідно з Постановами КМУ від 16.12.2022 р. № 1384 і від 16.01.2024 р. № 48) [42], а також у Методичних рекомендаціях щодо категоризації об'єктів критичної інфраструктури, затвердженими Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 р. № 23 (у редакції Наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 26.09.2023 р. № 857) [43]. При цьому розрахунок інтегральної нормованої оцінки рівня критичності об'єктів критичної інфраструктури здійснюється відповідно до критеріїв, які перелічено у табл. 9.

Як видно, у табл. 9 представлено класифікацію об'єктів критичної інфраструктури за категоріями критичності залежно від значення інтегрального показника $РК_{ОКІ}$. Виділено чотири рівні критичності – від I (найвищий) до IV (нижчий). Об'єкти, для яких значення показника не перевищує 0,2, не відносяться до критичної інфраструктури. Запропонований підхід забезпечує можливість уніфікованої оцінки критичності об'єктів та створює підґрунтя для визначення пріоритетів у сфері їх захисту, стійкості та управління ризиками.

Оскільки електронні комунікаційні, інформаційно-комунікаційні системи, автоматизовані системи управління технологічними процесами) віднесено до критично важливих елементів інфраструктури, то у 2020 р. урядом України визначено механізм формування національного та секторальних переліків об'єктів критичної інформаційної інфраструктури. Процедуру імплементації даного механізму викладено у Порядку формування переліку об'єктів критичної інформаційної інфраструктури, який затверджено Постановою Кабінету Міністрів України 09.10.2020 р. № 943 [44].

Згідно з п. 5 цього Порядку для оцінювання рівня критичності об'єкта інформаційної інфраструктури оператор критичної інфраструктури застосовує три основні критерії [44]:

- значущість об'єкта інформаційної інфраструктури для забезпечення стійкого й безперервного функціонування об'єкта критичної інфраструктури, а також для належного надання ним життєво важливих послуг і виконання ключових функцій;
- наявність істотного впливу кіберінцидентів, кібератак або порушень інформаційної безпеки на безперервність і стійкість процесів надання об'єктом критичної інфраструктури життєво важливих послуг та функцій;
- відсутність альтернативних об'єктів або механізмів, здатних забезпечити безперервність і стійкість надання життєво важливих послуг та функцій у разі збоїв роботи об'єкта інформаційної інфраструктури.

Об'єкти інформаційної інфраструктури, які відповідають усім зазначеним критеріям, відносяться оператором критичної інфраструктури до категорії об'єктів критичної інформаційної інфраструктури. При цьому їх категорія критичності визначається відповідно до категорії критичності відповідного об'єкта критичної інфраструктури.

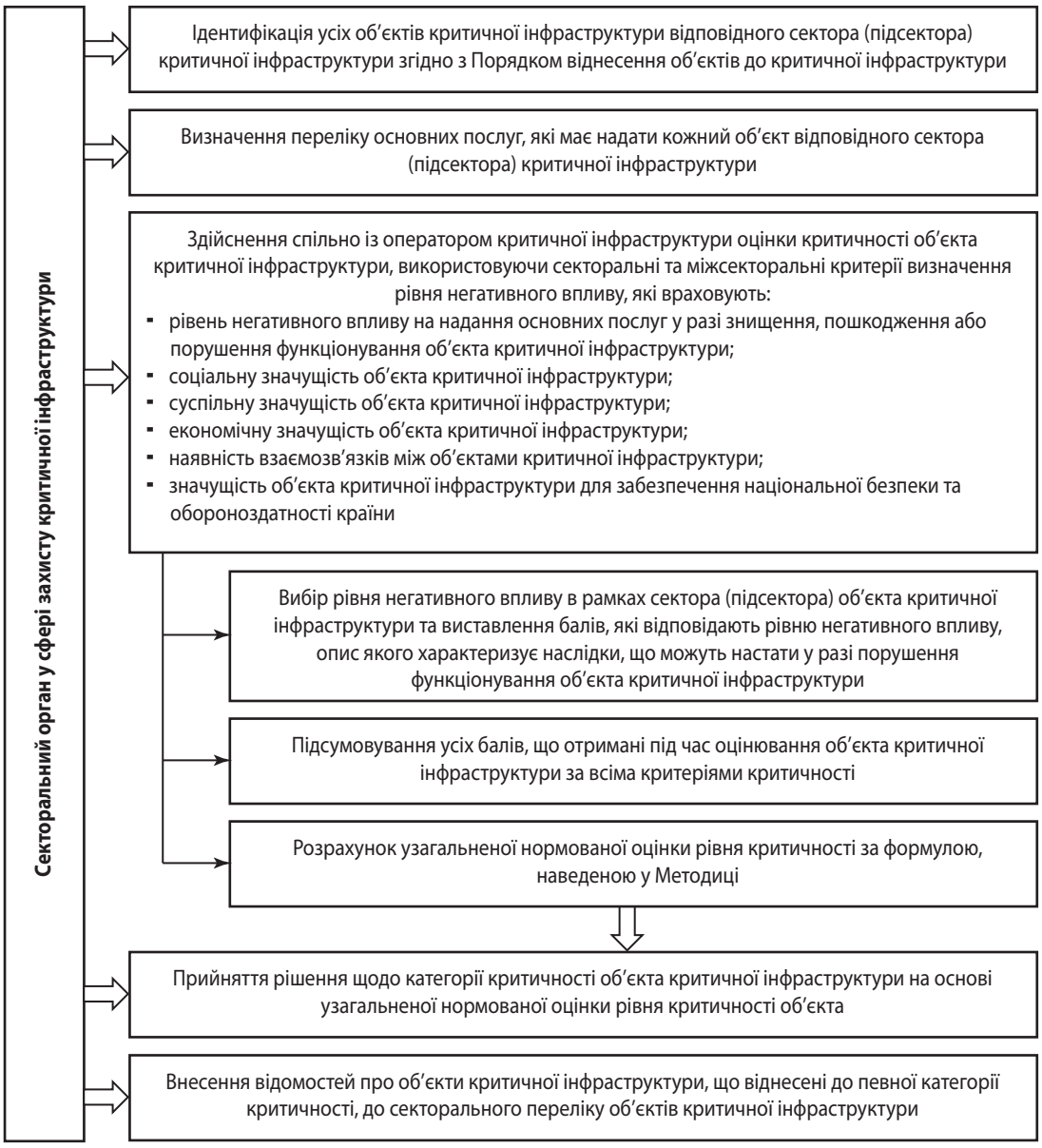

Рис. 2. Етапи визначення категорії об'єкта критичної інфраструктури

Джерело: побудовано авторами на основі опрацювання [39; 40; 42].

Таблиця 9

Категорії критичності об'єктів критичної інфраструктури залежно від рівня їх критичності

Категорії критичності	Діапазон значень рівня критичності (РКОКІ)
І категорія критичності	$0,8 < РК_{ОКІ} \leq 1$
ІІ категорія критичності	$0,63 < РК_{ОКІ} \leq 0,8$
ІІІ категорія критичності	$0,37 < РК_{ОКІ} \leq 0,63$
IV категорія критичності	$0,2 < РК_{ОКІ} \leq 0,37$
Об'єкт не є критичним	$РК_{ОКІ} \leq 0,2$

Джерело: складено авторами на основі опрацювання [42; 43].

З огляду на це, до секторального переліку включаються відомості щодо об'єктів критичної інформаційної інфраструктури, віднесених до І, ІІ, ІІІ та IV категорій критичності [44].

Необхідно зазначити, що у 2023 р. Кабінет Міністрів України затвердив Порядок ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього [45]. Реєстр критичної інфраструктури виступає ключовим інструментом у системі забезпечення національної безпеки, оскільки спрямований на координацію дій суб'єктів національної системи її захисту, організацію ефективного інформаційного обміну та проведення комплексної оцінки рівня захищеност-

ті об'єктів. Його функціональне призначення охоплює формування бази даних щодо потенційних загроз і вразливостей, підготовку науково обґрунтованих висновків і рекомендацій для власників та операторів, а також забезпечення процесів паспортизації та впровадження механізмів захисту критично важливих об'єктів [45].

Крім того, Реєстр виконує функції обробки, збереження та захисту інформації про інфраструктурні об'єкти, що мають вирішальне значення для життєдіяльності суспільства і держави. Для таких об'єктів встановлюються спеціальні вимоги безпеки й стійкості, а також здійснюється постійний моніторинг дотримання визначених стандартів. Реєстр виступає не лише інформаційно-аналітичною базою, а й інструментом підвищення стійкості критичної інфраструктури до загроз різного походження.

Таким чином, на підставі аналізу діючої нормативно-правової бази в Україні встановлено, що категоризація об'єктів критичної інфраструктури становить ключовий інструмент формування системи національної безпеки та управління ризиками у сфері захисту критичних ресурсів. Вона забезпечує диференційований підхід до організації захисних заходів залежно від рівня потенційних загроз і масштабів наслідків у разі порушення функціонування конкретного об'єкта.

При цьому встановлені правові рамки ієрархії об'єктів критичної інфраструктури ґрунтуються на принципі субординації загальнонаціональних, регіональних, місцевих та локальних інтересів. Така структура дозволяє не лише чітко визначити пріоритетність заходів із забезпечення стійкості, але й оптимізувати розподіл державних ресурсів, виходячи з імовірності та масштабів загроз. Виділення чотирьох категорій критичності створює умови для системного планування захисних заходів. Об'єкти I категорії виконують системоутворюючу роль і вимагають найвищого рівня державної уваги, тоді як об'єкти IV категорії залишаються у полі контролю здебільшого локальних суб'єктів. Така багаторівнева модель дозволяє забезпечити гнучкість і пропорційність заходів реагування, що відповідає сучасним підходам до управління національною безпекою, рекомендованим ЄС і НАТО.

Акцент на секторальній специфіці категоризації демонструє прагнення до уніфікації державної політики при збереженні гнучкості у різних галузях. Особливу увагу варто звернути на роль Національного банку України у банківській і фінансовій системах, що відображає пріоритетність фінансової стабільності у контексті захисту критичної інфраструктури. Це відповідає світовій практиці, де фінансова система розглядається як стратегічний сектор економіки, а її стійкість – як фактор запобігання системним кризам.

Важливим є положення щодо Методики категоризації, затверджуваної Кабінетом Міністрів України. Це свідчить про прагнення до формалізації та стандартизації процесу, що підвищує прозорість та ефективність управлінських рішень. Наявність єдиної методичної бази дозволяє уникати суб'єктивізму та забезпечує уніфікований підхід на міжгалузевому рівні. Отже, існуючі нормативно-правові документи окреслюють правові засади диференціації об'єктів критичної інфраструктури, а й формують методологічну основу для розбудови багаторівневої системи управління ризиками.

ВИСНОВКИ

Результати проведеного дослідження дозволяють зробити низку концептуально важливих узагальнень, що стосуються закордонної та української практики ідентифікації об'єктів критичної інфраструктури.

По-перше, аналіз зарубіжного досвіду свідчить про існування декількох методологічних парадигм, які визначають характер побудови систем захисту критичної інфраструктури. Французька модель робить акцент на інституційно-організаційному підході, в якому центральне місце належить життєво важливим операторам. Британська система, навпаки, ґрунтується на секторальній ієрархії та багаторівневій оцінці критичності. Нідерландська практика фокусується на процесно-орієнтованому підході, що дозволяє відмовитися від надмірної деталізації секторів та концентрувати увагу на ключових функціональних процесах. Німецька модель поєднує технічні та соціально-економічні компоненти, а ізраїльська – інтегрує культурно-символічні, функціонально-економічні та системно-структурні виміри. Таким чином, закордонна практика демонструє перехід від вузько-секторального до багаторівневого розуміння критичної інфраструктури.

По-друге, у межах Європейського Союзу відбувається процес інституціоналізації та уніфікації підходів до ідентифікації критично важливих об'єктів. Директива Ради ЄС 2008/114/ЄС та Директива (ЄС) 2022/2557 формують багаторівневу методологію, де поєднуються галузеві й міжгалузеві критерії, а також особлива увага приділяється транскордонному елементу. Делегований Регламент Комісії (ЄС) 2023/2450 окреслює базовий перелік основних послуг, який хоча і не є вичерпним, але слугує відправною точкою для національних систем. Це свідчить про поступове формування єв-

ропейського стандарту у сфері захисту критичної інфраструктури.

По-третє, теоретичний аналіз показує, що ключовими методами ідентифікації залишаються ризик-орієнтований, модельний, експертний, соціологічний та комбінований. Їх поєднання дозволяє досягти більшої точності у визначенні критичності об'єктів, врахувати як кількісні показники (частота ризиків, масштаби наслідків), так і якісні параметри (рівень взаємозалежності, символічна значущість, культурна цінність).

Слід наголосити, що український досвід у сфері ідентифікації критичної інфраструктури перебуває у процесі активного становлення. Прийняття Закону України «Про критичну інфраструктуру» (2021 р.) стало важливим кроком у формуванні нормативно-правового підґрунтя. Нормативна база передбачає секторальну диференціацію, категоризацію об'єктів за рівнями критичності (I–IV), створення державного реєстру та інституціоналізацію функцій секторальних органів.

Практичним досягненням української моделі є впровадження блочної класифікації секторів критичної інфраструктури (економічний, соціальний, безпековий, управлінський блоки), що відображає багатовимірність сучасних безпекових викликів. Такий підхід дозволяє не лише забезпечити системність управлінських рішень, а й вибудувати інтегровану архітектуру стійкості, яка спирається на принцип диференційованого ризик-менеджменту.

Водночас варто зазначити, що процес імплементації законодавчих норм залишається складним. Викликом є необхідність гармонізації секторальних методик категоризації з міжнародними стандартами, створення єдиної цифрової платформи моніторингу стану об'єктів, а також запровадження механізмів партнерства між державою і приватними операторами.

В умовах трансформації міжнародного безпекового середовища та триваючої війни в Україні питання ідентифікації та захисту критичної інфраструктури набуває не лише технічного, але й екзистенційного значення. Втрата чи порушення функціонування ключових об'єктів може спричинити не тільки економічні збитки, але й гуманітарні катастрофи, дестабілізацію політичної системи та підрив обороноздатності держави.

Отже, ідентифікація критично важливих об'єктів інфраструктури є складним, багатовимірним і динамічним процесом, який вимагає поєднання наукових підходів, правових механізмів та управлінських практик. Світовий досвід переконує, що жодна країна не може забезпечити стійкість виключно власними зусиллями – потрібна гармонізація стандартів і транскордонна координація. Для України актуальним завданням є створення стійкої системи критичної інфраструктури, здатної витримувати як внутрішні, так і зовнішні виклики. Це можливо за умови синтезу міжнародних практик, розвитку національної нормативної бази та впровадження інноваційних методів оцінки ідентифікації та категоризації об'єктів.

Перспективи подальших досліджень у даному напрямі пов'язано з розробленням інтегральних показників критичності об'єктів, що комплексно відображають економічні, соціальні та безпекові чинники; удосконаленням методик аналізу та прогнозування каскадних наслідків у разі відмови окремих елементів інфраструктури; адаптацією правової бази України до вимог європейського та міжнародного права з урахуванням викликів воєнного стану і завдань повоєнної відбудови економіки. ■

БІБЛІОГРАФІЯ

1. Cáceres G. Argentina's critical infrastructures: topics for their regulation. *International Journal of Critical Infrastructures*. 2024. Vol. 20. Iss. 2. P. 97–110. DOI: 10.1504/IJCIS.2024.137404
2. Fekete A., Lauwe P., Geier W. Risk management goals and identification of critical infrastructures. *International Journal of Critical Infrastructures*. 2012. Vol. 8. Iss. 4. P. 336–353. DOI: 10.1504/IJCIS.2012.050108
3. Galvan G., Agarwal J. Community detection in action: Identification of critical elements in infrastructure networks. *Journal of Infrastructure Systems*. 2018. Vol. 24. Iss. 1. Article 04017046. DOI: 10.1061/(ASCE)IS.1943-555X.0000400
4. Leitner B., Rehak D., Kersys R. The new procedure for identification of infrastructure elements significance in sub-sector railway transport. *Communications – Scientific Letters of the University of Žilina*. 2018. Vol. 20. Iss. 2. P. 41–48.
5. Novotny P., Janosikova M. Designating regional elements system in a critical infrastructure system in the context of the Czech Republic. *Systems*. 2020. Vol. 8. Iss. 2. P. 1–24. DOI: 10.3390/systems8020013
6. Pursiainen C., Kytömaa E. From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure*. 2022. Vol. 8 (S1). P. 85–101. DOI: https://doi.org/10.1080/23789689.2022.2128562
7. Rehak D., Senovsky P., Hromada M., Lovecek T. Complex approach to assessing resilience of critical infrastructure elements. *International Journal*

of Critical Infrastructure Protection. 2019. Vol. 25. P. 125–138.
DOI: 10.1016/j.ijcip.2019.03.003
8. Rehak D., Patrman D., Brabcová V., Dvořák Z. Identifying critical elements of road infrastructure using cascading impact assessment. *Transport*. 2020. Vol. 35. Iss. 3. P. 300–314.
DOI: 10.3846/transport.2020.12414
9. Vasylius V., Jonaitis A., Gudžius S., Kopustinskas V. Multi-period optimal power flow for identification of critical elements in a country scale high voltage power grid. *Reliability Engineering and System Safety*. 2021. Vol. 216. Article 107959.
DOI: 10.1016/j.ress.2021.107959
10. Vidriková D., Boc K. Identification of the security environment influences on renewable energy sources and critical infrastructure elements of Euroregion Beskydy. *Advanced Materials Research*. 2014. Vol. 1001. P. 80–89.
DOI: 10.4028/www.scientific.net/AMR.1001.80
11. Єрменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монографія. Дніпро : Дніпропетровський державний університет внутрішніх справ, 2018. 180 с.
12. Підюков П. П., Калиновський О. В. Система державного захисту критичної інфраструктури України: генеза, сучасний стан і перспективи оптимізування в умовах подальшого забезпечення національної безпеки країни. *Часопис Київського університету права*. 2020. № 4. С. 355–359.
DOI: 10.36695/2219-5521.4.2020.63
13. Теленик С. С. Критична інфраструктура як об'єкт адміністративно-правового регулювання. *Юридичний часопис Національної академії внутрішніх прав*. 2018. № 1. С. 179–189.
14. Яременко О. І., Страхніцький Я. О. Теоретичні підходи до визначення дефініції критичної інфраструктури як об'єкту державного управління. *Публічне управління та митне адміністрування*. 2022. № 1 (32). С. 76–82.
DOI: 10.32836/2310-9653-2022-1.13
15. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Київ : НІСД, 2012. 57 с.
16. Бобро Д. Г. Удосконалення методології ранжування об'єктів критичної інфраструктури та їх віднесення до критичної інфраструктури : аналіт. записка. Київ : НІСД, 2016. 17 с. URL: https://www.niss.gov.ua/sites/default/files/2016-06/krutuchna_infra-a7636.pdf
17. Корченко А. О., Козачок В. А., Гізун А. І. Метод оцінки рівня критичності для систем управління кризовими ситуаціями. *Захист інформації*. 2015. № 1. Т. 17. С. 86–98.
18. Мельничук О. В. Ідентифікація об'єктів критичної інфраструктури: базові методи та критерії. *Регіональна політика: історія, політико-правові засади, урбаністика, просторове планування, архітектура*. 2019. Вип. 5. Ч. 2. С. 193–197. URL: https://repositary.knuba.edu.ua/items/9ba87866-ea4b-4f32-9995-dc6c4885fe41
19. Щербак Л. Метод визначення рівня важливості об'єктів критичної інформаційної інфраструктури в галузі цивільної авіації. *Безпека інформації*. 2017. № 1. С. 27–38.
20. Бірюков Д. С., Кондратов С. І., Насвіт О. І., Суходоля О. М. Зелена книга з питань захисту критичної інфраструктури в Україні. Київ : НІСД, 2015. 35 с.
21. Арсенович Л. А. Парадигма захисту критичної інфраструктури в системі національної безпеки України. *Державне управління: удосконалення та розвиток*. 2024. № 8.
DOI: 10.32702/2307-2156.2024.8.7
22. Гора І. В. Окремі питання захисту об'єктів критичної інфраструктури: зарубіжний досвід. *Соціально-правові студії*. 2021. № 1 (11). С. 132–139.
23. Кизим М. О., Хаустова В. Є., Трушкіна Н. В. Сутність поняття «критична інфраструктура» з позицій національної безпеки України. *Бізнес Інформ*. 2022. № 12. С. 58–78.
DOI: 10.32983/2222-4459-2022-12-58-78
24. Wang D., Gryshova I., Balian A., Kyzym M., Salashenko T., Khaustova V., Davidyuk O. Assessment of Power System Sustainability and Compromises between the Development Goals. *Sustainability*. 2022. № 14. 2236.
DOI: 10.3390/su14042236
25. Bezpartochnyi M., Khaustova V., Trushkina N. Mechanism for ensuring international security in new geostrategic realities. *Prospects for sustainable development and ensuring the security of economic systems in the new geostrategic realities*: scientific monograph. Košice : Vysoká škola bezpečnostného manažérstva v Košiciach, 2023. P. 222–246.
DOI: 10.5281/zenodo.10436679
26. Хаустова В. Є., Решетняк О. І., Проноза П. В. Сучасні війни та воєнні конфлікти: сутність, класифікація, особливості та вплив на економіку. *Бізнес Інформ*. 2022. № 11. С. 6–21.
DOI: 10.32983/2222-4459-2022-11-6-21
27. Хаустова В. Є., Трушкіна Н. В. Ризики та загрози національній безпеці: сутність і класифікація. *Бізнес Інформ*. 2024. № 10. С. 6–22.
DOI: 10.32983/2222-4459-2024-10-6-22
28. Good Governance for Critical Infrastructure Resilience, OECD Reviews of Risk Management Policies. Paris : OECD, 2019. 118 p.
DOI: https://doi.org/10.1787/02f0e5a0-en
29. Luiijf E., Klaver M., Nieuwenhuijs A. RECIPE – Good Practices for CIP Policy-Makers. The CIP Report. *TNO*. 2011. June. URL: https://publications.tno.nl/publication/104061/rAzAEZ/luiijf-2011-recipe.pdf
30. 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 (Text with EEA relevance). *Official Journal of the European Union*. 2008. 23 December. URL: http://data.europa.eu/eli/dir/2008/114/oj

31. European critical infrastructure: Revision of Directive 2008/114/EC. *European Parliament*. 2021. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf
32. Commission Delegated Regulation (EU) 2023/2450 of 25 July 2023 supplementing Directive (EU) 2022/2557 of the European Parliament and of the Council by establishing a list of essential services. *Official Journal of the European Union*. 2023. 30 October. URL: http://data.europa.eu/eli/reg_del/2023/2450/oj
33. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance). *Official Journal of the European Union*. 2022. 27 December. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng
34. Factsheet Critical Infrastructure. The Netherlands: National Coordinator for Security and Counterterrorism Ministry of Justice and Security, 2018. 02 February. URL: https://english.nctv.nl/documents/publications/2018/02/01/factsheet-critical-infrastructure
35. The protection of critical infrastructures against terrorist attacks: compendium of good practices. New York: United Nations Office of Counter-Terrorism, United Nations Security Council Counter-Terrorism Committee Executive Directorate, 2021. 170 p. URL: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf
36. Instruction générale interministérielle relative la sécurité des activités d'importance vitale N 6600/SGDSN/PSE/PSN du 7 janvier 2014. URL: https://www.legifrance.gouv.fr/download/pdf/circ?id=37828
37. Концепція забезпечення національної системи стійкості : Указ Президента України від 27.09.2021 № 479/2021. URL: https://zakon.rada.gov.ua/laws/show/479/2021#n11
38. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX (із змінами, у редакції від 21.09.2024 р.). URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text
39. Деякі питання об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 № 1109 (із змінами, у редакції від 13.03.2025 р.). URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n45
40. Порядок віднесення об'єктів до критичної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 № 1109 (у редакції Постанови Кабінету Міністрів України від 16.12.2022 р. № 1384). URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n45
41. Перелік секторів критичної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 № 1109 (у редакції Постанови Кабінету Міністрів України від 16.01.2024 р. № 48). URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n45
42. Методика категоризації об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 № 1109 (із змінами та доповненнями згідно з Постановами КМУ від 16.12.2022 р. № 1384 і від 16.01.2024 р. № 48). URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n45
43. Методичні рекомендації щодо категоризації об'єктів критичної інфраструктури : Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 № 23 (із змінами, у редакції Наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 26.09.2023 р. № 857). URL: https://zakon.rada.gov.ua/rada/show/v0023519-21#Text
44. Порядок формування переліку об'єктів критичної інформаційної інфраструктури : Постанова Кабінету Міністрів України 09.10.2020 № 943 (із змінами, внесеними згідно з Постановою Кабінету Міністрів України від 28.03.2025 р. № 447). URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#n61
45. Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього : Постанова Кабінету Міністрів України від 28.04.2023 № 415. URL: https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#n15

REFERENCES

Arsenovych, L. A. (2024). Paradyhma zakhystu krytychnoi infrastruktury v systemi natsionalnoi bezpeky Ukrainy [The paradigm of critical infrastructure protection in the national security system of Ukraine]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok, (8)*. https://doi.org/10.32702/2307-2156.2024.8.7

Bezpartochnyi, M., Khaustova, V., & Trushkina, N. (2023). Mechanism for ensuring international security in new geostrategic realities. In *Prospects for sustainable development and ensuring the security of economic systems in the new geostrategic realities: scientific monograph* (pp. 222–246). Vysoká škola bezpečnostného manažérstva v Košiciach. Košice. https://doi.org/10.5281/zenodo.10436679

Biriukov, D. S., & Kondratov, S. I. (2012). *Zakhyst krytychnoi infrastruktury: problemy ta perspektyvy vprovadzhennia v Ukraini* [Protection of critical infrastructure: Problems and prospects of implementation in Ukraine]. NISD. Kyiv.

Biriukov, D. S., Kondratov, S. I., Nasvit, O. I., & Sukhodolia, O. M. (2015). *Zelena knyha z pytan zakhystu krytychnoi infrastruktury v Ukraini* [Green Paper on the Protection of Critical Infrastructure in Ukraine]. NISD. Kyiv.

Bobro, D. H. (2016). *Udoskonalennia metodolohii ranzhuvannia obiektiv krytychnoi infrastruktury ta yikh vidnesennia do krytychnoi infrastruktury : analit. zapyska* [Improving the methodology for ranking critical infrastructure objects and classifying them as critical infrastructure: Analytical note]. NISD. Kyiv. https://www.niss.gov.ua/sites/default/files/2016-06/krutuchna_infra-a7636.pdf

Cáceres, G. (2024). Argentina's critical infrastructures: topics for their regulation. *International Journal of Critical Infrastructures*, *20*(2), 97–110. https://doi.org/10.1504/IJCIS.2024.137404

Commission Delegated Regulation (EU) 2023/2450 of 25 July 2023 supplementing Directive (EU) 2022/2557 of the European Parliament and of the Council by establishing a list of essential services. (2023, October 30). *Official Journal of the European Union*. http://data.europa.eu/eli/reg_del/2023/2450/oj

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 (Text with EEA relevance). (2008, December 23). *Official Journal of the European Union*. http://data.europa.eu/eli/dir/2008/114/oj

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance). (2022, December 27). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

European Parliament. (2021). *European critical infrastructure: Revision of Directive 2008/114/EC*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf

Fekete, A., Lauwe, P., & Geier, W. (2012). Risk management goals and identification of critical infrastructures. *International Journal of Critical Infrastructures*, *8*(4), 336–353. https://doi.org/10.1504/IJCIS.2012.050108

Galvan, G., & Agarwal, J. (2018). Community detection in action: Identification of critical elements in infrastructure networks. *Journal of Infrastructure Systems*, *24*(1), Article 04017046. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000400

Hora, I. V. (2021). Okremi pytannia zakhystu obiektiv krytychnoi infrastruktury: zarubizhnyi dosvid [Some issues of protection of critical infrastructure facilities: Foreign experience]. *Sotsialno-pravovi studii*, *(1(11))*, 132–139.

Instruction générale interministérielle relative la sécurité des activités d'importance vitale N 6600/SGDSN/PSE/PSN du 7 janvier 2014. https://www.legifrance.gouv.fr/download/pdf/circ?id=37828

Khaustova, V. Ye., Reshetniak, O. I., & Pronoza, P. V. (2022). Cuchasni viiny ta voienni konflikty: sutnist, klasyfikatsiia, osoblyvosti ta vplyv na ekonomiku [Modern wars and military conflicts: Essence, classification, features and impact on the economy]. *Biznes Inform*, *(11)*, 6–21. https://doi.org/10.32983/2222-4459-2022-11-6-21

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

Korchenko, A. O., Kozachok, V. A., & Hizun, A. I. (2015). Metod otsinky rivnia krytychnosti dlia system upravlinnia kryzovymy sytuatsiiamy [Method of assessing the level of criticality for crisis management systems]. *Zakhyst informatsii*, *17*(1), 86–98.

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

Leitner, B., Rehak, D., & Kersys, R. (2018). The new procedure for identification of infrastructure elements significance in sub-sector railway transport. *Communications – Scientific Letters of the University of Žilina*, *20*(2), 41–48.

Luiijf, E., Klaver, M., & Nieuwenhuijs, A. (2011). *RECIPE – Good practices for CIP policy-makers. The CIP report*. TNO. https://publications.tno.nl/publication/104061/rAzAEZ/luiijf-2011-recipe.pdf

Melnychuk, O. V. (2019). Identyfikatsiia obiektiv krytychnoi infrastruktury: bazovi metody ta kryterii [Identification of critical infrastructure objects: Basic methods and criteria]. *Rehionalna polityka: istoriia, polityko-pravovi zasady, urbanistyka, prostorove planuvannia, arkhitektura*, *(5, Ch. 2)*, 193–197. https://repositary.knuba.edu.ua/items/9ba87866-ea4b-4f32-9995-dc6c4885fe41

Nakaz Administratsii Derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii Ukrainy vid 15.01.2021 № 23 (iz zminamy, u redaktsii Nakazu Administratsii Derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii Ukrainy vid 26.09.2023 r. № 857). *Metodychni rekomendatsii shchodo kategoryzatsii obiektiv krytychnoi infrastruktury* [Methodological recommendations for categorizing critical infrastructure objects]. https://zakon.rada.gov.ua/rada/show/v0023519-21#Text

National Coordinator for Security and Counterterrorism Ministry of Justice and Security. (2018, February 2). *Factsheet critical infrastructure*. The Netherlands. https://english.nctv.nl/documents/publications/2018/02/01/factsheet-critical-infrastructure

Novotny, P., & Janosikova, M. (2020). Designating regional elements system in a critical infrastructure system

in the context of the Czech Republic. *Systems*, *8*(2), 1–24. https://doi.org/10.3390/systems8020013

OECD. (2019). *Good governance for critical infrastructure resilience, OECD reviews of risk management policies*. Paris. https://doi.org/10.1787/02f0e5a0-en

Pidiukov, P. P., & Kalynovskyi, O. V. (2020). Systema derzhavnoho zakhystu krytychnoi infrastruktury Ukrainy: heneza, suchasnyi stan i perspektyvy optymizuvannia v umovakh podalshoho zabezpechennia natsionalnoi bezpeky krainy [The system of state protection of critical infrastructure of Ukraine: Genesis, current state and prospects for optimization in the context of further ensuring the national security of the country]. *Chasopys Kyivskoho universytetu prava*, *(4)*, 355–359. https://doi.org/10.36695/2219-5521.4.2020.63

Postanova Kabinetu Ministriv Ukrainy 09.10.2020 № 943 (iz zminamy, vnesenymy zhidno z Postanovoiu Kabinetu Ministriv Ukrainy vid 28.03.2025 r. № 447). *Poriadok formuvannia pereliku obiektiv krytychnoi informatsiinoi infrastruktury* [Procedure for forming a list of critical information infrastructure objects]. https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#n61

Postanova Kabinetu Ministriv Ukrainy vid 09.10.2020 № 1109 (iz zminamy ta dopovnenniamy zhidno z Postanovamy KMU vid 16.12.2022 r. № 1384 i vid 16.01.2024 r. № 48). *Metodyka katehoryzatsii obiektiv krytychnoi infrastruktury* [Methodology for categorizing critical infrastructure objects]. https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n45

Postanova Kabinetu Ministriv Ukrainy vid 09.10.2020 № 1109 (iz zminamy, u redaktsii vid 13.03.2025 r.). *Deiaki pytannia obiektiv krytychnoi infrastruktury* [Decree of the Cabinet of Ministers of Ukraine dated October 9, 2020 No. 1109 (as amended, in the edition of March 13, 2025)]. https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n45

Postanova Kabinetu Ministriv Ukrainy vid 09.10.2020 № 1109 (u redaktsii Postanovy Kabinetu Ministriv Ukrainy vid 16.01.2024 r. № 48). *Perelik sektoriv krytychnoi infrastruktury* [List of critical infrastructure sectors]. https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n45

Postanova Kabinetu Ministriv Ukrainy vid 09.10.2020 № 1109 (u redaktsii Postanovy Kabinetu Ministriv Ukrainy vid 16.12.2022 r. № 1384). *Poriadok vidnesennia obiektiv do krytychnoi infrastruktury* [Procedure for classifying objects as critical infrastructure]. https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n45

Postanova Kabinetu Ministriv Ukrainy vid 28.04.2023 № 415. *Pro zatverdzhennia Poriadku vedennia Reiestru obiektiv krytychnoi infrastruktury, vkliuchennia takykh obiektiv do Reiestru, dostupu ta nadannia informatsii z noho* [On approval of the Procedure for maintaining the Register of Critical Infrastructure Objects, including such objects in the Register, accessing and providing information from it]. https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#n15

Pursiainen, C., & Kytömaa, E. (2022). From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure*, *8*(S1), 85–101. https://doi.org/10.1080/23789689.2022.2128562

Rehak, D., Patrman, D., Brabcová, V., & Dvořák, Z. (2020). Identifying critical elements of road infrastructure using cascading impact assessment. *Transport*, *35*(3), 300–314. https://doi.org/10.3846/transport.2020.12414

Rehak, D., Senovsky, P., Hromada, M., & Lovecek, T. (2019). Complex approach to assessing resilience of critical infrastructure elements. *International Journal of Critical Infrastructure Protection*, *25*, 125–138. https://doi.org/10.1016/j.ijcip.2019.03.003

Shcherbak, L. (2017). Metod vyznachennia rivnia vazhlyvosti obiektiv krytychnoi informatsiinoi infrastruktury v haluzi tsyvilnoi aviatsii [Method for determining the level of importance of critical information infrastructure facilities in the field of civil aviation]. *Bezpeka informatsii*, *(1)*, 27–38.

Telenyk, S. S. (2018). Krytychna infrastruktura yak obiekt administratyvno-pravovoho rehuliuvannia [Critical infrastructure as an object of administrative and legal regulation]. *Yurydychnyi chasopys Natsionalnoi akademii vnutrishnikh prav*, *(1)*, 179–189.

Ukaz Prezydenta Ukrainy vid 27.09.2021 № 479/2021. *Kontseptsiia zabezpechennia natsionalnoi systemy stiikosti* [Decree of the President of Ukraine dated September 27, 2021 No. 479/2021. Concept for ensuring the national resilience system]. https://zakon.rada.gov.ua/laws/show/479/2021#n11

United Nations Office of Counter-Terrorism, United Nations Security Council Counter-Terrorism Committee Executive Directorate. (2021). *The protection of critical infrastructures against terrorist attacks: Compendium of good practices*. New York. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf

Vasylius, V., Jonaitis, A., Gudžius, S., & Kopustinskas, V. (2021). Multi-period optimal power flow for identification of critical elements in a country scale high voltage power grid. *Reliability Engineering and System Safety*, *216*, Article 107959. https://doi.org/10.1016/j.ress.2021.107959

Vidriková, D., & Boc, K. (2014). Identification of the security environment influences on renewable energy sources and critical infrastructure elements of Euroregion Beskydy. *Advanced Materials Research*, *1001*, 80–89. https://doi.org/10.4028/www.scientific.net/AMR.1001.80

Wang, D., Gryshova, I., Balian, A., Kyzym, M., Salashenko, T., Khaustova, V., & Davidyuk, O. (2022). Assessment of power system sustainability and compromises between the development goals. *Sustainability*, *(14)*, 2236. https://doi.org/10.3390/su14042236

Yaremenko, O. I., & Strakhnitskyi, Ya. O. (2022). Teoretychni pidkhody do vyznachennia definitsii krytychnoi infrastruktury yak obiektu derzhavnoho upravlinnia [Theoretical approaches to defining the definition of critical infrastructure as an object of public administration]. *Publichne upravlinnia ta mytne administruvannia*, *(1(32))*, 76–82. https://doi.org/10.32836/2310-9653-2022-1.13

Yermenchuk, O. P. (2018). *Osnovni pidkhody do orhanizatsii zakhystu krytychnoi infrastruktury v krainakh Yevropy: dosvid dlia Ukrainy* [Basic approaches to organizing the protection of critical infrastructure in European countries: Experience for Ukraine]. Dnipropetrovskyi derzhavnyi universytet vnutrishnikh sprav. Dnipro.

Zakon Ukrainy vid 16.11.2021 № 1882-IX (iz zminamy, u redaktsii vid 21.09.2024 r.). *Pro krytychnu infrastrukturu* [Law of Ukraine dated November 16, 2021 No. 1882-IX (as amended, in the edition of September 21, 2024)]. https://zakon.rada.gov.ua/laws/show/1882-20#Text