УДК 351.863:342.9:338.246.87
JEL: H56; H76; K23; L98; O19
DOI: https://doi.org/10.32983/2222-4459-2025-11-6-26

ПРАВОВІ ЗАСАДИ РЕГУЛЮВАННЯ РОЗВИТКУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: МІЖНАРОДНА ПРАКТИКА ТА УКРАЇНСЬКИЙ ДОСВІД

©2025 ХАУСТОВА В. Є., ТРУШКІНА Н. В.

УДК 351.863:342.9:338.246.87
JEL: H56; H76; K23; L98; O19

Хаустова В. Є., Трушкіна Н. В. Правові засади регулювання розвитку критичної інфраструктури: міжнародна практика та український досвід

Статтю присвячено комплексному дослідженню правових засад регулювання розвитку критичної інфраструктури в Україні з урахуванням досвіду Європейського Союзу та рекомендацій міжнародних організацій. Актуальність роботи зумовлена масштабними руйнуваннями інфраструктурних секторів, зростанням фізичних, гібридних і кібернетичних загроз, а також стратегічними завданнями повоєнної відбудови й євроінтеграційних перетворень. У дослідженні підкреслюється, що сучасні умови потребують підвищення резильєнтності критичної інфраструктури як соціоекономічної та технічної системи, здатної забезпечувати безперервність життєво важливих функцій держави та суспільства в умовах багатовимірних криз. Метою статті є порівняльно-правовий аналіз підходів до регулювання критичної інфраструктури в Україні та ЄС відповідно до Директив CER і NIS2, а також визначення напрямів удосконалення національного законодавства. Методологічний інструментарій охоплює формально-юридичний, системно-структурний і порівняльно-правовий підходи, які доповнено ризик-орієнтованими та сценарними методами. Установлено, що нормативна доктрина ЄС базується на функціональному визначенні критичної інфраструктури, інтегрованому управлінні ризиками, уніфікованих вимогах до кіберстійкості та багаторівневій координації. Українське законодавство частково відповідає цим підходам, однак зберігає об'єктно-секторальну логіку, має недостатньо розроблені механізми ризик-менеджменту, нечіткі вимоги до кіберстійкості та інституційної взаємодії, а також не містить законодавчо визначеної категорії «критична послуга». Наукова новизна статті полягає в обґрунтуванні переходу до функціонально-резильєнтної моделі регулювання критичної інфраструктури та систематизації підходів CER, NIS2 та OECD для адаптації в українському контексті. Практичні результати дослідження включають рекомендації щодо запровадження категорії «критичних послуг», створення національного центру резильєнтності, стандартизації управління ризиками та аудитів стійкості, гармонізації кібербезпеки з NIS2, розвитку державно-приватного партнерства та інтеграції фізичної й кібернетичної безпеки. Отримані результати сприятимуть підвищенню інституційної та операційної спроможності держави у сфері критичної інфраструктури, удосконаленню правового забезпечення її функціонування та формуванню резильєнтної моделі розвитку, здатної забезпечити стійкість України в умовах воєнних і поствоєнних трансформацій. Дослідження також закладає підґрунтя для подальших робіт, спрямованих на розроблення концептуальної моделі резильєнтної критичної інфраструктури України.

Ключові слова: *національна економіка, критична інфраструктура, нормативно-правове регулювання, правові засади, управління ризиками, кіберстійкість, резильєнтність, інституційна координація, державно-приватне партнерство, післявоєнна відбудова, європейські директиви, закордонний досвід.*
Табл.: *5.* ***Бібл.:*** *42.*

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 науковий співробітник сектора промислової політики та інноваційного розвитку відділу промислової політики та енергетичної безпеки, Науково-дослідний центр індустріальних проблем розвитку НАН України (пров. Інженерний, 1а, 2 пов., Харків, 61166, Україна)*
E-mail: *trushkina@nas.gov.ua*
ORCID: *https://orcid.org/0000-0002-6741-7738*
Researcher ID: *https://www.webofscience.com/wos/author/record/894686*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57210808778*

UDC 351.863:342.9:338.246.87
JEL: H56; H76; K23; L98; O19

Khaustova V. Ye., Trushkina N. V. Legal Foundations for Regulating the Development of Critical Infrastructure: International Practice and Ukrainian Experience

The article is dedicated to a comprehensive study of the legal foundations for regulating the development of critical infrastructure in Ukraine, taking into account the experience of the European Union and the recommendations of international organizations. The relevance of the study is due to the large-scale destruction of infrastructure sectors, the increase in physical, hybrid, and cyber threats, as well as the strategic challenges of post-war reconstruction and European integration reforms. The study highlights that current conditions require enhancing the resilience of critical infrastructure as a socioeconomic and technical system capable of ensuring the continuity of vital functions of the State and society in the context of multidimensional crises. The aim of the article is a comparative legal analysis of approaches to regulating critical infrastructure in Ukraine and the EU according to the CER and NIS2 Directives, and to identify directions for improving national legislation. The methodological instruments include formal-legal, systemic-structural, and comparative-legal approaches, complemented

by risk-oriented and scenario-based methods. It has been found that the EU normative doctrine is based on a functional definition of critical infrastructure, integrated risk management, unified cyber resilience requirements, and multi-level coordination. Ukrainian legislation partially conforms to these approaches; however, it retains an object-sectoral logic, has underdeveloped risk management mechanisms, ambiguous requirements for cyber resilience and institutional interaction, and does not contain a legally defined category of «critical service». The scientific novelty of this article lies in substantiating the transition to a functionally resilient model for regulating critical infrastructure and in systematizing the CER, NIS2, and OECD approaches for adaptation in the Ukrainian context. The practical results of the study include recommendations for introducing the category of «critical services», establishing a national resilience center, standardizing risk management and resilience audits, harmonizing cyber security with NIS2, promoting public-private partnerships, and integrating physical and cyber security. The findings will help enhance the institutional and operational capacity of the State in the sphere of critical infrastructure, improve the legal framework for its functioning, and create a resilient development model capable of ensuring Ukraine's stability during wartime and post-wartime transformations. The study also provides a foundation for further work aimed at developing a conceptual model of resilient critical infrastructure in Ukraine.
Keywords: *national economy, critical infrastructure, regulatory and legal framework, legal principles, risk management, cyber resilience, resilience, institutional coordination, public-private partnership, post-war reconstruction, European directives, international experience.*
Tabl.*: 5.* ***Bibl.:*** *42.*

Khaustova Viktoriia Ye. *– D. Sc. (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. *– PhD (Economics), 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*

Повоєнний розвиток України відбувається в умовах безпрецедентних викликів, що істотно впливають на функціонування критичної інфраструктури (КІ) держави. Кінцева мета повоєнної трансформації полягає не лише у відновленні зруйнованих об'єктів, а й у формуванні стійкої, адаптивної, інтегрованої з європейським простором інфраструктурної системи, здатної забезпечувати безперервність життєво важливих послуг, економічну активність і національну безпеку. Система критичної інфраструктури в Україні охоплює енергетичні, транспортно-логістичні, цифрові, комунальні, соціальні, фінансові та інші сектори, які є взаємозалежними та утворюють складний багаторівневий простір безпеки та розвитку.

Російська агресія проти України спричинила масштабні руйнування інфраструктурних систем та їх супровідних сервісів. За оцінками Світового банку [1], сумарні збитки інфраструктурних секторів України за 2022–2024 рр. перевищили 150 млрд дол. США. Причому найбільших втрат зазнали енергетика, транспорт, логістика та житлово-комунальна сфера. Події 2023–2024 рр. демонструють, що атаки на інфраструктурні об'єкти мають системний характер і часто спрямовані на зниження резильєнтності держави шляхом порушення безперебійності енергосистеми, транспортних потоків, цифрових комунікацій та роботи критично важливих державних інституцій.

Соціальний вимір наслідків руйнування інфраструктури також є надзвичайно значущим. За даними KSE Institute [2], понад 72% громадян і місцевих громад визначають перебої енергопостачання, недоступність цифрових сервісів, затримки в роботі транспорту та логістики ключовими чинниками погіршення якості життя у 2023–2024 рр. Такі результати свідчать про високий рівень залежності добробуту населення від стабільності функціонування інфраструктурних систем. Особливо гостро ці питання постають у громадах, які зазнали руйнувань енергетичних вузлів, водогонів, шляхового покриття, залізничних ліній або цифрової інфраструктури – там рівень соціальної вразливості зростає в геометричній прогресії.

Економічні наслідки порушення роботи критичної інфраструктури є системними. Так, аналітика Світового банку та Міжнародного банку реконструкції та розвитку [3] свідчить, що ненадійність інфраструктури у країнах, які переживають воєнні конфлікти, може приводити до щорічних втрат на рівні 2–4% ВВП через простої виробництва, витрати на резервні джерела енергії, погіршення логістики та зниження продуктивності. В українських реаліях масштаби цих втрат можуть бути ще вищими через системний характер атак на енергетичні та цифрові об'єкти, а також сильну залежність економіки від логістичних маршрутів експорту.

Опитування Європейської Бізнес Асоціації [4] демонструють, що близько 65% компаній у 2023–2024 рр. визначають інфраструктурні ризики

(нестабільне електропостачання, порушення логістики, кіберзагрози) одним із ключових бар'єрів для нових інвестицій і масштабування діяльності. Це означає, що держава стикається не лише з прямими економічними збитками від руйнувань, а й з відкладеним ефектом у вигляді зниження привабливості інвестиційного середовища, що має довготривалі наслідки для темпів відновлення.

Окремим і надзвичайно важливим викликом стає зростання кіберзагроз. За даними Державної служби спеціального зв'язку та захисту інформації [5], у 2023–2024 рр. кількість кібератак на державні та інфраструктурні об'єкти збільшилася на 62%. Понад 70% атак спрямовано на енергетичні та цифрові системи, що підкреслює цілеспрямований характер кібернетичного тиску [5]. Зниження цифрової стійкості посилюється нерівномірністю розвитку телекомунікацій: близько 15–18% території України залишаються зонами із нестабільним або відсутнім інтернет-покриттям, а понад 30% об'єктів цифрової інфраструктури вимагають модернізації [6].

Експертні опитування, які проведено провідними аналітичними центрами України [2; 4], також підтверджують критичність ситуації. Зокрема, 60% експертів наголошують на браку інституційної координації у сфері критичної інфраструктури [2]; 55% – на необхідності синхронізації національної нормативно-правової бази з директивами CER і NIS2; 40% – на доцільності створення окремого органу для стратегічного управління розвитком критичної інфраструктури [4]. Це свідчить про системні прогалини в чинній політиці, які потребують пошуку нормативно-правових, інституційних та управлінських засад удосконалення.

У світовій практиці за останнє десятиліття сформовано комплексне нормативне поле, спрямоване на підвищення резильєнтності критичної інфраструктури. Директива (ЄС) 2022/2557 (CER Directive) визначає вимоги до управління ризиками, безперервності надання послуг та організаційної стійкості операторів у 11 секторах, включно з енергетикою, транспортом, водопостачанням, охороною здоров'я та цифровими сервісами [7]. Директива (ЄС) 2022/2555 (NIS2) охоплює питання кіберзахисту та встановлює єдині вимоги щодо інцидент-менеджменту, аудиту, кіберризиків та обов'язкової звітності для 18 секторів економіки [8]. Рекомендації OECD підкреслюють пріоритетність довгострокового інфраструктурного планування, міжвідомчої координації, прозорості та запровадження системного ризик-орієнтованого управління [9].

Україна вже здійснила перші стратегічні кроки в напрямі гармонізації з європейською нормативною базою. Закон України від 16.11.2021 р. № 1882-IX «Про критичну інфраструктуру» (із змінами) визначає базову термінологію, ключові принципи державної політики, функції суб'єктів КІ, моделі координації та загальні вимоги до управління безпекою [10].

Проте потреба в подальшому розвитку нормативного поля залишається нагальною: необхідно деталізувати методики оцінювання ризиків; імплементувати європейські стандарти управління стійкістю; створити інтегровану модель моніторингу стану критичної інфраструктури; забезпечити фінансові інструменти для модернізації інфраструктурних секторів і розробити механізми міжвідомчої взаємодії, що відповідають сучасним викликам.

Отже, актуальність наукового дослідження правових засад регулювання розвитку критичної інфраструктури зумовлено масштабом руйнувань, високим рівнем фізичних і кібернетичних загроз, інституційними дисфункціями та стратегічною необхідністю гармонізації українського законодавства з європейськими стандартами безпеки. Комплексний аналіз міжнародних і національних правових підходів, оцінювання їх ефективності та адаптація до умов повоєнної відбудови України є важливою передумовою формування резильєнтної моделі критичної інфраструктури, здатної забезпечувати сталий розвиток держави, її економічну спроможність і безпеку в умовах сучасних і майбутніх зовнішніх загроз.

Питання визначення сутності критичної інфраструктури та її резильєнтності займає ключове місце в сучасному міжнародному науковому дискурсі (G. Ampratwum et al. [11]; C. Brown et al. [12]; E. Brucherseifer et al. [13]; M. Hromada et al. [14]; D. Rehak et al. [15; 16]; B. Rød et al. [17]; E. Wells et al. [18]; X. Zhao et al. [19]). Значна частина робіт присвячена дослідженню здатності інфраструктурних систем протистояти багатовимірним загрозам і швидко відновлювати функціонування. Так, на думку D. Rehak, P. Senovsky та S. Slivkova [15], резильєнтність є інтегральною характеристикою, що поєднує зниження вразливості, мінімізацію наслідків дестабілізуючих впливів і забезпечення оперативного відновлення. Подібну позицію займають E. Brucherseifer et al. [13], підкреслюючи здатність системи адаптуватися на основі отриманого досвіду та накопичених знань.

У зарубіжній теорії сформувався комплекс підходів до розуміння критичної інфраструктури – функціональний, ризик-орієнтований, мережевий і резильєнтний. Вони відображають відмінності інституційних моделей різних країн і міжнародних організацій. Аналітичні звіти OECD, NATO, Євро-

пейської Комісії та CISA трактують критичну інфраструктуру через її спроможність забезпечувати життєво важливі суспільні функції, підтримувати фізичну та кібернетичну безпеку, гарантувати економічну стабільність і безперервність державного управління [7–9; 20–22]. Така багатовимірність підходів стала основою для уніфікації ключових понять у рамках міжнародних стандартів.

Значний вплив на формування сучасної європейської доктрини критичної інфраструктури мала Європейська Комісія, яка у 2022 р. ухвалила два системоутворюючі нормативні акти – Директиву (ЄС) 2022/2557 (CER Directive) [7] і Директиву (ЄС) 2022/2555 (NIS2) [8]. CER Directive закріпила функціональний підхід, відповідно до якого критична інфраструктура визначається через здатність суб'єктів забезпечувати безперервність основних послуг навіть в умовах природних, техногенних, гібридних чи воєнних загроз. Документ містить вимоги щодо обов'язкової оцінки ризиків, упровадження планів резильєнтності, багаторівневої координації та державного нагляду [7]. Своєю чергою, NIS2 встановлює уніфіковані стандарти кіберстійкості для 18 секторів критичної інфраструктури, формуючи інтегровану модель поєднання фізичної та цифрової стійкості [8; 21]. Таким чином, у ЄС критична інфраструктура розглядається як єдина соціо-технічна система, резильєнтність якої визначається взаємозалежністю мереж, процесів та цифрових компонентів.

Суттєвий науковий внесок у розвиток методології оцінювання резильєнтності зроблено в межах OECD, де запропоновано рамкову модель «infrastructure resilience governance» [9]. Організація розглядає резильєнтність як здатність інфраструктурних систем передбачати, протистояти, адаптуватися та відновлюватися після кризових подій, наголошуючи на багатосекторальних ризиках, необхідності інтегрованого управління, участі приватного сектора та громадськості [9]. У цих документах резильєнтність трактується не лише як технічна, а як комплексна управлінська характеристика, що охоплює правові, інституційні, фінансові та комунікаційні аспекти [9; 21].

Сучасна міжнародна наукова школа (G. Cáceres [23], A. Fekete et al. [24], B. Leitner et al. [25], D. Rehak et al. [15; 16], D. Vidriková, K. Boc [26]) демонструє перехід від статичної моделі – трактування критичної інфраструктури як сукупності об'єктів – до динамічного аналізу мережевих взаємозалежностей і каскадних ефектів. До ключових напрямів дослідження [27] належать розвиток методів ризик-орієнтованого аналізу, мережевого моделювання, сценарного прогнозування, оцінювання критичності вузлів і системних компонентів. Саме ці напрацювання [28] лягли в основу концепцій resilience engineering, що активно впроваджуються в ЄС, США та OECD.

Українські наукові дослідження у сфері критичної інфраструктури інтенсивно розвиваються з 2012 року, коли вчені Національного інституту стратегічних досліджень [29; 30] вперше окреслили необхідність формування державної політики у сфері її захисту. У подальших роботах (П. Підюков, О. Калиновський [31], О. Мельничук [32], Л. Арсенович [33]) сформовано методичний апарат ідентифікації критичних об'єктів з використанням ризик-орієнтованих, експертних, соціологічних і модельних підходів. Акцент робиться на багатовимірності аналізу, що враховує технічний стан, функціональну значущість, міжсекторальні залежності та потенціал каскадних наслідків.

У низці новітніх українських досліджень критична інфраструктура розглядається як багаторівнева соціо-економічна та технічна система, яка вразлива до природних, техногенних, воєнних і кібернетичних загроз [34–37]. Наголошується на переході до проактивної моделі регулювання, яка базується на превентивному управлінні ризиками, запровадженні індикаторів резильєнтності та гармонізації національних методик із вимогами CER і NIS2 [37]. Також підкреслюється потреба уніфікації критеріїв критичності та вдосконалення інституційних механізмів міжвідомчої координації [36].

У цьому контексті показовими є результати ґрунтовного аналізу інституційних засад стійкості критичної інфраструктури ЄС, НАТО та України, здійсненого в сучасних українсько-європейських наукових публікаціях. У цих роботах наголошується, що ефективність функціонування критичної інфраструктури залежить від якості нормативно-правового регулювання, узгодженості державної політики, співпраці з приватним сектором та імплементації міжнародних стандартів (CER, NIS2, NATO Resilience Guidelines).

Загальний аналіз зарубіжної та національної літератури дає підстави стверджувати, що спільною тенденцією є відхід від об'єктно-орієнтованої парадигми в напрямку системного бачення критичної інфраструктури як резильєнтного комплексу, спроможного адаптуватися до багатовимірних загроз. Міжнародні стандарти пропонують інтегровану модель, що враховує кіберфізичну природу сучасних інфраструктур, вплив каскадних ефектів та необхідність державно-приватної взаємодії.

Водночас українські дослідження демонструють активне наближення до цих підходів, однак подальший розвиток потребує поглиблення методик

ідентифікації, вдосконалення системи управління ризиками та нормативного закріплення принципу резильєнтності як ключового орієнтира розвитку критичної інфраструктури. Отже, інтеграція міжнародних стандартів з національними підходами є необхідною умовою формування стійкої, адаптивної та резильєнтної системи критичної інфраструктури України.

З огляду на сучасні виклики у сфері національної безпеки та стратегічну необхідність адаптації українського законодавства до стандартів Європейського Союзу, ***мета статті*** полягає в обґрунтуванні правових засад регулювання розвитку критичної інфраструктури шляхом порівняльного аналізу міжнародної практики, насамперед ЄС та OECD, та чинного нормативно-правового поля України, а також у формуванні науково обґрунтованих пропозицій щодо його вдосконалення в умовах повоєнної відбудови та євроінтеграційних трансформацій. Досягнення поставленої мети передбачає осмислення ключових дефініцій, ідентифікаційних підходів, механізмів управління ризиками та резильєнтністю, що визначають функціонування критичної інфраструктури в сучасних безпекових умовах.

Методологічне підґрунтя статті ґрунтується на поєднанні класичних і сучасних дослідницьких підходів, що забезпечує комплексність аналізу та можливість інтегрувати юридичні, інституційні, управлінські та міждисциплінарні аспекти. Використання формально-юридичного методу сприяло з'ясуванню змісту норм національного законодавства, актів Європейського Союзу – передусім директив CER і NIS2 – а також документів OECD, що дозволило окреслити правову еволюцію вимог до розвитку та стійкості критичної інфраструктури. Порівняльно-правовий підхід забезпечив можливість системно співвіднести міжнародні та українські моделі регулювання, виявити спільні риси та принципові розбіжності, визначити напрями їх гармонізації та адаптації до українського контексту.

Застосування системно-структурного методу дозволило розглядати критичну інфраструктуру як багаторівневу соціо-економічну та технічну систему, що включає взаємопов'язані об'єкти, мережі, процеси, послуги та інститути, а також виявити закономірності її функціонування в умовах воєнних та гібридних загроз. Методи аналізу та синтезу були використані для узагальнення наукових підходів до визначення критичної інфраструктури, резильєнтності, управління ризиками, а також для логічного структурування здобутих результатів з позицій правового регулювання.

Для оцінювання можливостей адаптації міжнародних практик до української системи управління критичною інфраструктурою застосовано ризик-орієнтований і сценарний підходи, що дали змогу інтерпретувати моделі управління ризиками терористичних, воєнних, кібернетичних і техногенних загроз у контексті українських реалій. Метод контент-аналізу забезпечив опрацювання широкого кола джерел – наукових публікацій, міжнародних стандартів, стратегічних документів, експертних звітів – що дозволило сформувати цілісну картину сучасних тенденцій у сфері розвитку та правового забезпечення критичної інфраструктури. Логіко-інтерпретаційний метод сприяв формуванню авторських висновків і практичних пропозицій щодо вдосконалення правових механізмів регулювання, а також визначенню оптимальних напрямів підвищення стійкості критичної інфраструктури України в умовах воєнних і поствоєнних трансформацій.

Таким чином, обрана методологія забезпечує не лише всебічне висвітлення правових аспектів розвитку критичної інфраструктури, але й дозволяє здійснити багатофакторний аналіз міжнародних і національних підходів, що створює підґрунтя для формування обґрунтованих рекомендацій щодо вдосконалення законодавства та практики його застосування.

У науковому дискурсі останніх років сформувався широкий спектр теоретико-правових підходів до розуміння критичної інфраструктури, що відображає як різноманітність суспільних функцій, які виконують інфраструктурні системи, так і еволюцію загроз, що впливають на їхню стійкість і безпеку. Зарубіжні дослідження фокусуються на функціональних, ризик-орієнтованих і мережевих характеристиках інфраструктур, підкреслюючи важливість взаємозалежностей між секторами та потенціалу каскадних ефектів. Водночас український науковий дискурс активно розвиває інституційно-правові засади критичної інфраструктури, приділяючи особливу увагу питанням державної координації, нормативно-правового регулювання та формування методології оцінювання критичності.

Особливої актуальності набуває резильєнтний підхід, що розглядає критичну інфраструктуру як динамічну систему, здатну адаптуватися, протистояти та швидко відновлюватися після дії комплексних, у тому числі воєнних, загроз. В умовах сучасних викликів, а саме – гібридної агресії, кібератак, руйнування логістичних і енергетичних мереж, резильєнтність стає не додатковою характеристикою, а базовою вимогою до функціонування критичної інфраструктури.

Узагальнення світових і вітчизняних досліджень засвідчує, що жоден з окремих підходів не відображає повною мірою комплексного характеру критичної інфраструктури. Це зумовлює поступове формування інтегрованого багаторівневого бачення, яке поєднує об'єктні, функціональні, ризикові, мережеві та інституційно-правові виміри. На основі аналізу сучасної доктрини систематизовано теоретико-правові підходи у вигляді *табл. 1*.

Запропонована табл. 1 відображає логіку еволюції наукових підходів до критичної інфраструктури та показує, як змінювався фокус досліджень у відповідь на загрози, розвиток технологій і трансформацію державної політики у сфері національної безпеки.

Об'єктний (галузево-секторальний) підхід був одним із перших у формуванні правового розуміння критичної інфраструктури. Він ґрунтується на тому, що критичною є не система загалом, а конкретні об'єкти – електростанції, мости, нафтопроводи, лікарні, вузли зв'язку тощо. Підхід широко використовувався в перших нормативних актах України та ЄС, де перелік секторів визначався на основі історичних та оборонних пріоритетів держави. Його обмеженням є недостатнє врахування взаємозалежностей між секторами та того, що збої можуть виникати не лише через фізичні ураження, але й через інформаційні, кібернетичні або управлінські порушення.

Фокус *функціонального підходу* зсувається із об'єктів на функції, які вони виконують. Критичною вважається не конкретна споруда чи система, а життєво важлива послуга – енергопостачання, транспорт, водопостачання, охорона здоров'я, цифровий зв'язок. Це дозволяє ширше та гнучкіше розглядати інфраструктуру, не обмежуючись традиційними секторами, й адаптувати нормативне регулювання до появи нових технологій і сервісів. У сучасній європейській моделі CER цей підхід є домінуючим.

Ризик-орієнтований (наслідковий) підхід визначає критичну інфраструктуру через потенційні наслідки її відмови. Основним критерієм є масштаб

Таблиця 1

Теоретико-правові підходи до розуміння критичної інфраструктури та її резильєнтності

Теоретико-правовий підхід	Сутнісна характеристика критичної інфраструктури	Акценти щодо резильєнтності
Об'єктний (галузево-секторальний)	КІ трактується як перелік об'єктів у стратегічно важливих секторах (енергетика, транспорт, ІКТ, фінанси, охорона здоров'я тощо)	Перевага фізичного захисту та охорони об'єктів; превентивні інженерні заходи
Функціональний (орієнтований на життєво важливі послуги)	КІ визначається через функції та критичні послуги (енергопостачання, водопостачання, медичні послуги, транспортні сервіси)	Забезпечення безперервності послуг, резервування, дублювання каналів
Ризик-орієнтований (наслідковий)	Ключове – масштаби негативних наслідків у разі виходу з ладу об'єкта: людські жертви, економічні збитки, шкода нацбезпеці	Управління ризиками, оцінювання критичності, сценарне моделювання
Мережевий / системний	КІ – взаємозалежна мережа інфраструктурних систем; відмова одного елементу може спричинити каскадні ефекти	Стримування каскадних збоїв, сегментація, децентралізація, «smart grid»
Інституційно-правовий	У центрі уваги – нормативна база, повноваження органів влади, державна політика, координація, ДПП	Резильєнтність як результат врядування, уніфікованих процедур і координації
Резильєнтний	КІ – динамічна система, здатна адаптуватися, протистояти та швидко відновлюватися після впливу загроз	Повний цикл: попередження → готовність → реагування → відновлення → навчання
Інтегрований багаторівневий підхід	Поєднує об'єктний, функціональний, мережевий, ризиковий та інституційно-правовий виміри. КІ – багаторівнева соціо-економіко-технічна система	Резильєнтність як синергетичний результат узгодженості правових, технічних, управлінських і фінансових механізмів

Джерело: складено авторами на основі [7–9; 28–30; 34–40].

збитків: людські жертви, значні економічні втрати, руйнування соціальних функцій, підрив обороноздатності. Такий підхід широко застосовують НІСД, провідні європейські дослідники та міжнародні організації. Він дозволяє будувати управління безпекою інфраструктури на об'єктивних індикаторах ризику та вимірюваних критеріях.

Запропонований у відповідь на зростаючу складність інфраструктурних систем *мережевий і системний підхід* підкреслює взаємозалежності між секторами. У системах енергетики, транспорту, зв'язку та фінансів збої в одному секторі можуть викликати каскадні відмови в інших. Такий підхід забезпечує розуміння критичної інфраструктури як комплексної мережі, де важливо ідентифікувати не лише об'єкти, але й зв'язки між ними, а також ризики мережевого ефекту. Він є ключовим для розвитку сучасних моделей «smart grid», кіберфізичних систем і цифрових платформ.

Інституційно-правовий підхід фокусується на ролі держави у створенні нормативної бази, визначенні повноважень, координації між суб'єктами та формуванні механізмів публічного управління. Він розглядає критичну інфраструктуру як об'єкт державної політики, що потребує чітких правових рамок, механізмів взаємодії, процедур обміну інформацією та регуляторних інструментів. Це ключовий підхід у формуванні українського законодавства та гармонізації з європейськими директивами.

У сучасних умовах війни, кіберзагроз і комплексних техногенних ризиків резильєнтність стає базовою характеристикою критичної інфраструктури. *Резильєнтний підхід* орієнтується на здатність системи витримувати удари, адаптуватися до швидких змін і відновлюватися в умовах непевності. Він включає цикли попередження, готовності, реагування, відновлення та навчання. Резильєнтність охоплює технічний, управлінський, організаційний, цифровий та соціальний виміри.

Інтегрований багаторівневий підхід є найбільш сучасним і всеохопним, який поєднує елементи всіх попередніх. Він розглядає критичну інфраструктуру як багаторівневу соціо-економіко-технічну систему, де стійкість залежить від узгодженості технічних, правових, управлінських, фінансових та організаційних інструментів. Такий підхід є характерним для новітніх європейських моделей (CER – NIS2 – OECD), а також для українських досліджень, спрямованих на адаптацію міжнародних стандартів (*табл. 2*).

Порівняння міжнародних та українських підходів демонструє, що ключові відмінності полягають у ступені системності, рівні інституційної зрілості та інтегрованості політик. У міжнародній практиці критична інфраструктура розглядається як комплекс взаємозалежних мереж і життєво важливих послуг, а резильєнтність – як стратегічний орієнтир. Українська модель активно наближається до цього бачення, проте ще зберігає риси секторальності, фрагментарності та нормативної обмеженості, що потребує розбудови механізмів управління ризиками, міжвідомчої координації, державно-приватного партнерства та законодавчого закріплення резильєнтності як ключового принципу розвитку критичної інфраструктури.

У міжнародному правовому полі питання регулювання критичної інфраструктури розвивається в межах комплексних підходів, що поєднують фізичну, кібернетичну, організаційну та інституційну стійкість. Найбільш системну нормативну архітектуру сформовано в Європейському Союзі, де у 2022 році ухвалено два ключові документи – Директиву (ЄС) 2022/2557 про резильєнтність критичних суб'єктів (CER Directive) [7] і Директиву (ЄС) 2022/2555 (NIS2) [8], які заклали сучасну правову модель забезпечення стійкості критичної інфраструктури в умовах зростання гібридних і кібернетичних загроз. Обидва документи істотно змінили підходи ЄС до управління критичними системами, сформувавши новий концептуальний перехід від охорони об'єктів до забезпечення безперервності критичних послуг.

Директива CER визначає резильєнтність як здатність критичних суб'єктів передбачати, запобігати, протистояти та відновлюватися після впливу екстремальних подій [7]. Вона охоплює 11 секторів критичної інфраструктури, передбачає обов'язок держав – членів ЄС проводити регулярні національні оцінки ризиків, затверджувати стратегії резильєнтності, здійснювати аудит спроможності операторів критичної інфраструктури та забезпечувати міжсекторальну та транскордонну координацію [7]. CER також інтегрує фізичні, соціальні, технологічні та природні загрози, що відображає багатовимірність сучасного міжнародного регулювання.

Директива NIS2, яка доповнює CER, встановлює єдині стандарти кіберстійкості для 18 секторів критичної інфраструктури, зокрема енергетики, транспорту, охорони здоров'я, цифрової інфраструктури, водопостачання, харчового забезпечення та державного управління [8]. Документ суттєво розширює сферу регулювання кібербезпеки, підвищує відповідальність керівництва суб'єктів господарювання, конкретизує вимоги до управління ризиками та встановлює суворіші механізми державного нагляду. У такий спосіб NIS2 формує нормативну основу для інтеграції кіберстійкості в загальну систему управління критичною інфраструктурою [8; 21].

Таблиця 2

Порівняльна характеристика міжнародних та українських підходів до розуміння критичної інфраструктури та її резильєнтності

Критерій порівняння	Міжнародні підходи (ЄС, НАТО, OECD, США)	Українські підходи (законодавство, наукові дослідження різних установ)
Базове розуміння критичної інфраструктури	Трактується як система життєво важливих послуг, що надаються через взаємопов'язані мережі та комплекси об'єктів. Акцент – на функціях	У перших документах – перелік об'єктів у секторах. Поступовий перехід до розуміння КІ як системи, що забезпечує ключові функції держави та суспільства
Ключові критерії критичності	Функціональність, незамінність, рівень взаємозалежностей, масштаб наслідків, потенціал каскадних ефектів	Стратегічна важливість для держави, можливість суттєвої шкоди нацбезпеці, обороноздатності, суспільству. Оцінювання мережевих залежностей поки недостатньо розвинене
Підходи до ідентифікації об'єктів КІ	Використовуються функціональні та ризик-орієнтовані критерії, сценарний аналіз, моделі взаємозалежностей	Наявні ризик-орієнтовані, експертні, модельні підходи, однак їх застосування не є загальнообов'язковим у нормативній практиці
Підходи до класифікації секторів КІ	ЄС (11 секторів CER і 18 секторів NIS2), США (16 секторів), НАТО (критичні функції та здатності). Основний принцип – гнучкість і регулярний перегляд	Секторальний перелік у Законі України «Про критичну інфраструктуру». Однак перелік секторів не завжди оновлюється відповідно до розвитку технологій та появи нових загроз
Феномен резильєнтності	Резильєнтність – центральна концепція, що включає готовність, реагування, відновлення, адаптацію, навчання. OECD визначає резильєнтність як «здоров'я» інфраструктурних систем	Резильєнтність визнається важливою, але поки недостатньо закріплена як ключова ціль державної політики. Зосередження здебільшого на фізичному та кіберзахисті
Регулювання кібербезпеки КІ	ЄС (NIS2 встановлює загальні стандарти кіберстійкості для операторів критичної інфраструктури); США (CISA моделює ризики)	Україна гармонізує підходи до NIS2, але кіберстійкість секторів є нерівномірною, інвестиційна спроможність операторів обмежена
Управління ризиками	Інтегровані системи risk-based governance; регулярні оцінки ризиків; методології CIRIX, FAIR, сценарне моделювання, stress-testing	Українські дослідження підтримують цей підхід. У законодавстві є положення про оцінювання ризиків, але методики не стандартизовані
Підходи до міжвідомчої координації	ЄС і США мають розвинені системи централізованої координації (DG Home, CISA), а також постійні механізми обміну інформацією	Визначені повноваження профільних органів, однак координаційна модель залишається фрагментарною; обмін інформацією – недостатньо регулярний і структурований
Державно-приватне партнерство	Визнано критичним елементом розвитку та стійкості КІ; приватний сектор є власником більшості об'єктів; існують стандартизовані моделі взаємодії	ДПП є задекларованим у нормативних документах, але механізми та стимули взаємодії ще перебувають у стадії формування
Участь суспільства, прозорість, інклюзивність	OECD просуває принципи good governance: прозорість, відкритість даних, інклюзивність у процесах прийняття рішень	Україна поступово рухається до цих стандартів, але рівень прозорості та участі громад у питаннях КІ залишається обмеженим через безпекові й інституційні чинники
Загальна модель розуміння КІ	КІ – багаторівнева система, що поєднує об'єкти, послуги, мережі, функції, інститути та політику	Українська модель еволюціонує до інтегрованого бачення, однак потребує посилення міжсекторальної взаємодії, резильєнтності та управлінської інтеграції

Джерело: складено авторами на основі [7–10; 20–22; 29; 30].

Важливим концептуальним джерелом міжнародних підходів виступає Організація економічного співробітництва та розвитку (OECD), яка пропонує модель «інфраструктурної резильєнтності», що охоплює управління ризиками, багаторівневу координацію, державно-приватну взаємодію та принципи системного врядування [9]. У рекомендаціях OECD резильєнтність визначено як здатність інфраструктурних систем передбачати, витримувати, адаптуватися та швидко відновлюватися після дії загроз різного характеру, включно з природними, техногенними, кібернетичними та соціальними факторами [9]. Документи OECD акцентують увагу на важливості інтеграції фізичної та цифрової безпеки, удосконаленні стратегічного планування, регулярних стрес-тестах і підвищенні прозорості державної політики.

Узагальнюючи міжнародну правову базу, можна стверджувати, що CER, NIS2 та документи OECD (*табл. 3*) формують комплексну модель регулювання критичної інфраструктури, орієнтовану на стійкість її функціонування, багатовимірне управління ризиками, кіберфізичну цілісність та інституційну спроможність держав. Ці стандарти визначають цілі та інструменти, до яких поступово наближається українська система управління критичною інфраструктурою, що створює підґрунтя для подальшого аналізу її нормативно-правової еволюції та напрямів гармонізації з правом ЄС.

Отже, порівняльний аналіз директив CER і NIS2 і підходів OECD засвідчує формування в міжнародній практиці нової доктрини регулювання критичної інфраструктури, що ґрунтується на ідеї резильєнтності як базовій категорії. У центрі цієї доктрини – не просто захист окремих об'єктів, а забезпечення стійкого функціонування життєво важливих послуг у різних режимах – від повсякденного навантаження до кризових ситуацій природного, техногенного чи гібридного характеру. Така трансформація відображає глобальний перехід від реактивних моделей безпеки до превентивно-адаптивних механізмів, що охоплюють фізичний, кібернетичний та організаційний виміри.

У цій триєдиній системі CER формує основу функціонального та системного підходу, визначаючи критичну інфраструктуру через призму послуг і міжсекторальних залежностей та орієнтуючи держави на багатовимірне управління ризиками [7]. NIS2 поглиблює цей підхід у кіберсфері, встановлюючи єдині стандарти кіберстійкості для широкого спектра секторів та підвищуючи відповідальність операторів за належну організацію систем захисту [8]. OECD задає методологічну рамку належного врядування резильєнтністю, акцентуючи на інституційних спроможностях, міжвідомчій координації, державно-приватному партнерстві та стратегічному плануванні як ключових передумовах стійкого інфраструктурного розвитку [9].

Узгоджений зміст цих документів демонструє спільну логіку: критична інфраструктура розглядається як складна соціо-технічна система, що функціонує в умовах багатовимірних загроз і високої взаємозалежності секторів. Міжнародні стандарти наголошують на необхідності інтеграції фізичної та кібербезпеки, запровадження ризик-орієнтованих підходів, підвищення прозорості регулювання та інституційної спроможності держави й операторів.

Для України ці висновки мають особливе значення, оскільки окреслюють орієнтири, за якими має розвиватися національна система правового регулювання критичної інфраструктури в умовах повоєнного відновлення та євроінтеграційного курсу. Гармонізація законодавства з вимогами CER і NIS2 у поєднанні з адаптацією підходів OECD до належного врядування сприятиме переходу від фрагментарної, об'єктно орієнтованої моделі до комплексної системи, здатної забезпечувати стійкість, адаптивність і безперервність критично важливих послуг.

Таким чином, міжнародний досвід формує концептуальну основу для модернізації української нормативно-правової бази, посилення управління ризиками та розвитку резильєнтної моделі критичної інфраструктури. Це створює передумови для подальшого аналізу національного законодавства та визначення практичних напрямів його вдосконалення, що становитиме наступний етап даного дослідження.

Правове регулювання розвитку критичної інфраструктури в Україні формувалося поступово, реагуючи на трансформацію безпекового середовища, потреби модернізації державного управління та зростання міжнародних нормативних вимог. Перші системні аналітичні напрацювання сформовано Національним інститутом стратегічних досліджень, де окреслено базові концепти національної системи захисту критичної інфраструктури та доведено необхідність створення єдиної нормативної рамки, що охоплює секторальну специфіку, критерії віднесення об'єктів до критичних і принципи багаторівневого управління [29; 30]. Саме в цих розробках уперше сформульовано ідею розглядати критичну інфраструктуру як системний комплекс взаємозалежних соціо-технічних елементів, а не як набір окремих об'єктів.

Подальшим кроком став перехід від концептуальних підходів до нормативної конкретизації, який реалізовано через ухвалення Концепції створення державної системи захисту критичної

Таблиця 3

Порівняльна характеристика підходів CER, NIS2 і OECD до регулювання критичної інфраструктури та її резильєнтності

Критерій порівняння	Директива CER (ЄС 2022/2557)	Директива NIS2 (ЄС 2022/2555)	Підходи OECD до резильєнтності КІ
Об'єкт регулювання	Критичні суб'єкти, що надають життєво важливі послуги в 11 секторах (енергетика, транспорт, фінанси, водопостачання тощо)	Суб'єкти, що здійснюють діяльність у 18 секторах з підвищеними вимогами до кібербезпеки та управління інцидентами	Національні системи критичної інфраструктури в цілому, з акцентом на політику, врядування та інституційну спроможність
Основна ціль	Забезпечення резильєнтності критичних суб'єктів і безперервності надання життєво важливих послуг	Досягнення високого спільного рівня кіберстійкості та управління кіберризиками в ключових секторах економіки	Формування ефективного врядування ризиками, стійкості інфраструктурних систем і довгострокової здатності до адаптації й відновлення
Типи загроз і ризиків	Природні, техногенні, воєнні, терористичні, соціальні, окремі кіберзагрози	Кіберзагрози, інциденти, вразливості ІКТ, які пов'язані з організаційними та операційними ризиками	Комплексний multi-hazard підхід: природні, техногенні, кібернетичні, соціальні, економічні ризики
Ключові вимоги до суб'єктів	Оцінка ризиків, плани резильєнтності, заходи фізичного та організаційного захисту, готовність до кризового реагування	Системи управління кіберризиками, моніторинг і звітність про інциденти, технічні та організаційні заходи кібербезпеки, відповідальність менеджменту	Інтеграція управління ризиками в стратегії й політиці, інституційна координація, оцінка вразливостей, залучення зацікавлених сторін
Роль держави	Визначення критичних суб'єктів, затвердження нацстратегії, нагляд, координація та підтримка операторів	Регулятор і наглядовий орган у сфері кібербезпеки, координація CSIRT, застосування санкцій за недотримання вимог	Архітектор політики та системи врядування, посередник між секторами, ініціатор стандартів та «м'якого» регулювання
Інструменти координації	Нацстратегії резильєнтності, механізми обміну інформацією, транскордонна співпраця між державами-членами	Мережі компетентних органів, координаційні групи, спільні платформи обміну інформацією про інциденти	Міжнародні рекомендації, порівняльні огляди, платформи обміну досвідом, бенчмаркінг-політик
Державно-приватне партнерство	Визнається необхідним елементом забезпечення резильєнтності, але в основному в рамках нацстратегій	Підкреслюється спільна відповідальність за кіберстійкість, зокрема з боку операторів послуг	Розглядається як ключова умова стійкості, особливо з огляду на приватну власність більшості інфраструктурних активів
Орієнтація на резильєнтність	Резильєнтність є центральною категорією, що охоплює весь життєвий цикл управління загрозами	Резильєнтність розуміється насамперед як кіберстійкість, інтегрована в загальну систему безпеки КІ	Резильєнтність трактується як системна властивість інфраструктур на національному та міждержавному рівнях

Джерело: складено авторами на основі [7–9; 21].

інфраструктури (2017 р.) [41]. Документ визначив базові принципи функціонування системи, включно з інституційною координацією, формуванням секторальних переліків об'єктів, упровадженням ризик-орієнтованих підходів та налагодженням інформаційного обміну. Саме цей акт започаткував перехід від фрагментарного регулювання до розвитку цілісної державної політики у сфері критичної інфраструктури, зорієнтованої на побудову комплексної системи управління загрозами [41].

Ухвалення Концепції національної стійкості (2021 р.) [42] стало надсистемним етапом, який

формально пов'язав критичну інфраструктуру з ширшою доктриною стійкості держави. У документі закріплено інтегрований «all-of-government» та «all-of-society» підхід, у межах якого критична інфраструктура визнається ключовим елементом забезпечення життєдіяльності суспільства в умовах криз, гібридних загроз і воєнної агресії [42]. Концепція визначає здатність КІ підтримувати безперервність функцій, адаптуватися та швидко відновлюватися центральною складовою національної безпеки, що суттєво вплинуло на подальшу побудову нормативної системи [42].

Ключовим елементом сучасного регулювання став Закон України від 16.11.2021 р. № 1882-IX «Про критичну інфраструктуру» [10], який уперше створив комплексну правову основу для функціонування Національної системи захисту критичної інфраструктури. Закон визначає поняття критичної інфраструктури, вводить секторальний підхід, описує процедури ідентифікації та категоризації, встановлює вимоги до паспортів безпеки об'єктів і формує інституційний каркас багаторівневої взаємодії між державними органами та операторами критичних послуг [10]. Наявність цього Закону стала важливим кроком у формуванні системи сучасного типу, проте сама по собі нормативна база залишається багаторівневою та нерівномірною, що зберігає істотні розриви між секторами.

Сучасний етап розвитку регулювання характеризується поступовим наближенням до стандартів ЄС і НАТО, зокрема до принципів Директив CER та NIS2. Це зумовлює потребу в детальному аналізі секторального виміру регулювання. Адже реальна резильєнтність держави визначається не загальними нормами, а практичними правилами функціонування окремих секторів. Закон України від 16.11.2021 р. № 1882-IX «Про критичну інфраструктуру» [10] створює рамкову основу, але фактичне забезпечення безпеки та безперервності критичних послуг реалізується через секторальні закони у сферах енергетики, транспорту, зв'язку, фінансів, водопостачання, ЖКГ і продовольчої безпеки. Саме ці нормативні акти встановлюють вимоги до резервування потужностей, реагування на інциденти, управління ризиками, забезпечення якості послуг та захисту споживачів.

Узагальнений огляд таких нормативних актів наведено в *табл. 4*, яка відображає ключові секторальні законодавчі та нормативно-правові документи та їхню роль у забезпеченні резильєнтності. До них можна віднести такі:

- Закон України від 13.04.2017 р. № 2019-VIII «Про ринок електричної енергії» (із змінами); Закон України від 09.04.2015 р. № 329-VIII «Про ринок природного газу» (із змінами); Закон України від 22.06.2017 р. № 2119-VIII «Про комерційний облік теплової енергії та водопостачання» (із змінами); Закон України від 22.09.2016 р. № 1540-VIII «Про Національну комісію, що здійснює державне регулювання у сферах енергетики та комунальних послуг» (із змінами); Закон України від 04.07.1996 р. № 273/96-ВР «Про залізничний транспорт» (із змінами); Закон України від 05.04.2001 р. № 2344-III «Про автомобільний транспорт» (із змінами); Закон України від 03.12.2020 р. № 1054-IX «Про внутрішній водний транспорт» (із змінами); Закон України від 24.06.2004 р. № 1877-IV «Про засади державної аграрної політики та державної політики сільського розвитку» (із змінами); Закон України від 09.08.2023 р. № 3310-IX «Про державні резерви»; Закон України від 16.12.2020 р. № 1089-IX «Про електронні комунікації» (із змінами); Закон України від 27.07.2022 р. № 2463-IX «Про внесення змін до деяких законодавчих актів України щодо особливостей діяльності фінансового сектору у зв'язку із введенням воєнного стану в Україні» (із змінами); Закон України від 07.12.2000 р. № 2121-III «Про банки і банківську діяльність» (із змінами); Закон України від 30.06.2021 р. № 1591-IX «Про платіжні послуги» (із змінами); Закон України від 09.11.2017 р. № 2189-VIII «Про житлово-комунальні послуги» (із змінами); Закон України від 02.06.2005 р. № 2633-IV «Про теплопостачання» (із змінами); Закон України від 20.06.2022 р. № 2320-IX «Про управління відходами» (із змінами); Закон України від 10.01.2002 р. № 2918-III «Про питну воду та питне водопостачання» (із змінами);
- Розпорядження Кабінету Міністрів України від 04.08.2021 р. № 907-р «Про схвалення Стратегії енергетичної безпеки»; Розпорядження Кабінету Міністрів України від 11.07.2013 р. № 548-р (у редакції Розпорядження Кабінету Міністрів України від 23 грудня 2020 р. № 1634-р) «Про затвердження Стратегії розвитку морських портів України на період до 2038 року» (із змінами); Розпорядження Кабінету Міністрів України від 23.07.2024 р. № 684-р «Про схвалення Стратегії продовольчої безпеки України на період до 2027 року та затвердження операційного плану заходів з її реалізації»;
- Стратегія інформаційної безпеки (затверджено Указом Президента України від

28.12.2021 р. № 685/2021); Стратегія кібербезпеки України (затверджено Указом Президента України від 26.08.2021 р. № 447/2021);

- Постанова Кабінету Міністрів України від 27.12.2024 р. № 1550 «Про схвалення Національної транспортної стратегії України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025–2027 роках» (із змінами).

Аналіз табл. 4 показує, що попри різні предметні сфери, зазначені сектори мають спільні нормативні характеристики, притаманні критичній інфраструктурі: 1) забезпечення життєво важливих послуг, що визначає їх стратегічний статус; 2) наявність операторів, діяльність яких має системні наслідки для економіки та безпеки; 3) наявність вимог до безперервності, безпеки та якості послуг, що зближує їх із підходами CER;

Таблиця 4

Нормативно-правові засади функціонування стратегічних секторів економіки України в контексті критичної інфраструктури

Сектор	Ключові нормативно-правові акти	Роль у забезпеченні резильєнтності КІ
Енергетичний сектор	Закони України: «Про ринок електричної енергії», «Про ринок природного газу», «Про комерційний облік теплової енергії та водопостачання»; «Про Національну комісію, що здійснює державне регулювання у сферах енергетики та комунальних послуг»; Стратегія енергетичної безпеки України тощо	– Визначає вимоги до надійності постачання, безпеки енергосистеми, балансування та операційної стійкості; – закладає основу для визначення критичних операторів енергетики
Транспортний сектор	Закони України: «Про залізничний транспорт», «Про автомобільний транспорт», «Про внутрішній водний транспорт»; Стратегія розвитку морських портів України на період до 2038 року; Національна транспортна стратегія України на період до 2030 року тощо	– Регулюють безпеку перевезень і роботу стратегічних транспортних вузлів та об'єктів інфраструктури; – визначають критичні коридори та логістичні ланцюги
Аграрний сектор і продовольча безпека	Закони України: «Про засади державної аграрної політики та державної політики сільського розвитку», «Про державні резерви»; Стратегія продовольчої безпеки України на період до 2027 року тощо	– Гарантують стійкість виробництва та постачання продуктів харчування, функціонування елеваторів, складів тощо
Інформаційно-телекомунікаційний сектор	Закон України «Про електронні комунікації», Стратегія інформаційної безпеки, Стратегія кібербезпеки України тощо	– Встановлює вимоги до стійкості комунікаційних мереж, кіберзахисту операторів; – формує цифрову основу КІ
Фінансовий сектор	Закони України: «Про банки і банківську діяльність», «Про платіжні послуги», «Про внесення змін до деяких законодавчих актів України щодо особливостей діяльності фінансового сектору у зв'язку із введенням воєнного стану в Україні» тощо	– Забезпечує безперервність платежів, функціонування ринку капіталу та стабільність банківських операцій – критичні економічні функції держави
Житлово-комунальне господарство	Закони України «Про житлово-комунальні послуги», «Про теплопостачання», «Про управління відходами»; Національна стратегія управління відходами в Україні до 2030 року тощо	– Регулює надання базових послуг – тепло, вода, утримання мереж, що забезпечують життєздатність територіальних громад
Водопостачання та водовідведення	Закон України «Про питну воду та питне водопостачання»	– Встановлює стандарти якості води, вимоги безперервності та безпеки її постачання; – регламентує діяльність операторів водних мереж

Джерело: складено авторами на основі опрацювання законодавчої та нормативно-правової бази, яка регулює розвиток критично важливих секторів національної економіки.

4) цифрова залежність і кіберризики, що є ключовим елементом NIS2; 5) необхідність багаторівневої координації, яка в Україні лише формується.

Водночас секторальне регулювання характеризується низкою структурних проблем, серед яких: нормативи стійкості залишаються неуніфікованими; галузеві акти не містять інтегрованих індикаторів резильєнтності; механізми державно-приватної взаємодії розвинуто нерівномірно; недостатня імплементація принципу «функціональної критичності», визначального для Директиви CER; кіберстійкість секторальних операторів часто не відповідає стандартам NIS2.

Це підтверджує необхідність системної гармонізації секторального законодавства з рамкою критичної інфраструктури, що включає: введення секторальних стратегій резильєнтності; розроблення єдиних методик ризик-орієнтованого оцінювання; визначення статусу операторів критичних послуг; посилення кіберстійкості ключових суб'єктів; інтеграцію секторальних вимог до Національної системи стійкості.

Секторальний вимір є невід'ємною складовою правового регулювання критичної інфраструктури в Україні. Саме він визначає реальний рівень резильєнтності держави до фізичних, техногенних, кібернетичних і воєнних загроз. Подальший розвиток законодавства має базуватися на функціональному підході ЄС (CER), високих стандартах кіберстійкості (NIS2) і комплексній моделі національної стійкості, що дозволить сформувати цілісну, адаптивну та ефективну систему захисту критичної інфраструктури.

Попри наявність Закону та його концептуальну значущість, у науковій літературі та практичних оглядах зазначається низка обмежень, які потребують подальшого доопрацювання. Зокрема, у ряді досліджень увага звертається на недостатню інтеграцію ризик-орієнтованих підходів у процес категоризації об'єктів, відсутність уніфікованих методик оцінювання стійкості, фрагментарність підзаконної нормативної бази, яка ще перебуває в етапі формування, а також нерівномірність міжвідомчої координації. Окремі роботи підкреслюють, що чинну модель насамперед зорієнтовано на захист об'єктів, тоді як міжнародна практика впроваджує концепцію забезпечення безперервності критичних послуг і багатовимірної резильєнтності, що зумовлює необхідність переходу від статичного переліку об'єктів до функціонального підходу, узгодженого з директивами CER і NIS2.

При цьому слід наголосити, що важливою складовою правового регулювання є документи у сфері кібербезпеки, зокрема Закон України «Про основні засади забезпечення кібербезпеки України», Стратегія кібербезпеки та акти Державної служби спеціального зв'язку та захисту інформації. Вони встановлюють вимоги до кіберзахисту об'єктів критичної інфраструктури, визначають ролі державних органів, процедури реагування на інциденти та вимоги до цифрових інфраструктур. Однак чинні національні стандарти кіберстійкості все ще потребують гармонізації з вимогами NIS2, яка встановлює більш жорсткі стандарти управління вразливостями, моніторингу інцидентів та відповідальності керівництва операторів.

У контексті воєнної агресії та масштабних руйнувань інфраструктури особливої ваги набуває поступова інтеграція міжнародних норм щодо резильєнтності в національну модель управління критичною інфраструктурою. Це стосується запровадження регулярних міжсекторальних оцінок ризиків, планування безперервності діяльності, розвитку кризових центрів реагування, інституціоналізації державно-приватного партнерства та побудови механізмів прозорого обміну інформацією між державою й операторами критичної інфраструктури. Узагальнену порівняльну характеристику підходів до регулювання критичної інфраструктури в Україні та ЄС наведено в *табл. 5*.

Таким чином, варто відмітити, що правове регулювання розвитку критичної інфраструктури України перебуває у фазі глибокої трансформації. Це, своєю чергою, зумовлено необхідністю адаптації до комплексних безпекових викликів, масштабних воєнних загроз і вимог європейської інтеграції. Хоча нормативна база, яку подано Законом України «Про критичну інфраструктуру» № 1882-IX [10] та актами, які регулюють фунціонування стратегічних секторів економіки, формально закладає фундамент для функціонування національної системи критичної інфраструктури, її архітектура все ще зберігає риси об'єктно-секторального підходу. Така модель була характерною для ранніх європейських практик, однак у сучасних умовах виявила свою обмеженість.

Порівняльний аналіз засвідчує, що українська модель поки що не охоплює всі елементи сучасної європейської парадигми. Зокрема, відчутною є фрагментарність процедур управління ризиками. Національне законодавство визнає потребу в ризик-менеджменті [10], однак не містить методично уніфікованих інструментів для обов'язкових комплексних оцінок ризиків, аналізу вразливостей і регулярних аудитів резильєнтності. Це контрастує з вимогами CER щодо застосування багатофакторних моделей оцінювання загроз і стандартів OECD, які наголошують на важливості циклічного підходу «оцінка – готовність – реагування – відновлення» [9].

Таблиця 5

Порівняльна характеристика підходів до регулювання критичної інфраструктури в Україні, CER та NIS2

Критерій порівняння	Україна (Закон України від 16.11.2021 р. № 1882-IX, інші акти)	CER Directive (ЄС 2022/2557)	NIS2 Directive (ЄС 2022/2555)
Об'єкт регулювання	Об'єкти, системи та ресурси, стратегічно важливі для держави; секторальний перелік (10 секторів)	Критичні суб'єкти, що надають життєво важливі послуги в 11 секторах; акцент на функціях	Суб'єкти, що здійснюють діяльність у 18 секторах; акцент на цифровій інфраструктурі та ІКТ-ланцюгах
Підхід до критичності	Переважно об'єктний; критерії визначаються секторами та загальною важливістю для держави	Функціональний; критичність визначається безперервністю надання послуг і масштабом потенційних наслідків	Ризик-орієнтований; критичність визначається вразливістю цифрових систем і значенням кіберпроцесів
Типи загроз	Фізичні, техногенні, воєнні, кібернетичні; рівень деталізації різниться між секторами	Природні, техногенні, соціальні, терористичні, гібридні, частково кіберзагрози	Кіберзагрози, інциденти, уразливості ІКТ, атаки на ланцюги постачання
Стандарти управління ризиками	У загальних рисах визначено; методики залишаються фрагментованими; малоформалізовані вимоги	Обов'язкові оцінки ризиків, плани резильєнтності, аудит спроможності	Стандартизовані системи кіберризиків, обов'язковий моніторинг, звітність, управління інцидентами
Вимоги до резильєнт-ності	Резильєнтність визначається, але не є правовою категорією з чіткими індикаторами	Резильєнтність – центральна категорія; вимоги до попередження, готовності, реагування та відновлення	Кіберстійкість інтегрується в загальну модель резильєнтності; вимоги до операційних і технічних заходів
Ідентифікація та категоризація	Передбачена, але методично частково деталізована; паспортизація об'єктів	Встановлені чіткі процедури визначення критичних суб'єктів на нацрівні	Детальна класифікація операторів основних послуг і цифрових постачальників
Інституційна координація	Міжвідомча взаємодія існує, але залишається фрагментарною; потребує уніфікації	Координація держав-членів, спільні механізми реагування, транскордонна взаємодія	Мережа CSIRT і EU-CyCLONe; чітка координація компетентних органів ЄС
Кібербезпека	Визначена законом про кібербезпеку; рівень зрілості секторів нерівномірний	Кіберскладова врахована, але не домінує	Кіберскладова – ядро регулювання; підвищена відповідальність керівництва
Нагляд і відповідальність	Державний контроль переважно секторальний; обмежена кількість механізмів впливу	Державний нагляд, аудит, обов'язкові нацстратегії	Суворіші механізми контролю, санкції за невиконання вимог
Державно-приватне партнерство	Визнане необхідним, проте механізми лише формуються	Передбачає співпрацю з приватним сектором у межах резильєнтності	Значна частина заходів реалізується через операторів і постачальників послуг
Рівень гармонізації з міжнародними стандартами	Частково гармонізовано, але потребує суттєвого доопрацювання	Європейський зразок для нацсистем держав-членів	Стандарт кіберстійкості ЄС, обов'язковий до виконання

Джерело: складено авторами на основі [7–9; 42].

Концептуально важливими є й відмінності у визначенні критичності. Українське законодавство оперує переважно переліками об'єктів, що часто є статичними та не враховують динаміку інфраструктурних потоків, трансформацію технологій та еволюцію загроз. Натомість CER передбачає визначення критичних суб'єктів на основі оцінки наслідковості та системної важливості послуг [7]. Відсутність у національному законодавстві поняття «критична послуга» не дозволяє повною мірою ідентифікувати реальні точки вразливості інфраструктурної системи.

Суттєві диспропорції виявляються у сфері кіберстійкості. NIS2 встановлює жорсткі вимоги до управління кіберризиками, моніторингу загроз, процедур повідомлення про інциденти, інтеграції механізмів управління уразливостями та персональної відповідальності керівництва [8]. В Україні ж нормативні акти у сфері кібербезпеки застосовуються нерівномірно, а відсутність уніфікованої системи кіберризиків призводить до різного рівня кіберзахищеності в різних секторах, що суперечить вимогам NIS2.

Організаційно-інституційний вимір також потребує суттєвого посилення. CER передбачає створення компетентних органів, національних стратегій резильєнтності, регулярного звітування та міждержавної координації [7]. В Україні інституційні механізми формально окреслені, однак залишаються роз'єднаними та часто дублюють функції різних відомств. OECD наголошує, що ефективна система управління критичною інфраструктурою потребує наявності координаційного центру, який забезпечує інтегроване стратегічне планування та об'єднує фізичну та кібербезпеку в єдиний управлінський контур [9].

Узагальнюючи, можна констатувати, що українське законодавство рухається в напрямі гармонізації з європейськими нормами, але ще не відповідає критичним елементам сучасної міжнародної моделі регулювання критичної інфраструктури. Це зумовлює потребу в цілеспрямованому вдосконаленні нормативно-правового забезпечення з урахуванням кращих зарубіжних практик. На підставі проведеного порівняльного аналізу пропозиції щодо вдосконалення українського законодавства можуть бути згруповані за кількома стратегічними напрямами.

По-перше, потребує перегляду підхід до визначення критичної інфраструктури. Секторальна модель, закріплена в чинному законодавстві, має бути доповнена функціональним підходом, орієнтованим на визначення «критичних послуг», безперервність яких забезпечує життєдіяльність держави та суспільства. Запровадження в законодавстві категорії «критична послуга» та механізмів її правової інтерпретації, за аналогією з CER, дозволить уникнути надмірної фрагментації, підвищити гнучкість системи ідентифікації критичних суб'єктів та краще враховувати міжсекторальні залежності.

По-друге, необхідно суттєво посилити механізми управління ризиками. Доцільно нормативно закріпити обов'язкові, стандартизовані процедури оцінювання ризиків і вразливостей для всіх секторів критичної інфраструктури, включно з аналізом природних, техногенних, кібернетичних і соціальних загроз. Важливим інструментом можуть стати регулярні аудити резильєнтності за зразком практик ЄС, із чітко визначеними показниками, періодичністю, відповідальними суб'єктами та механізмами реагування на виявлені недоліки.

По-третє, у межах гармонізації з NIS2 доцільно встановити єдині вимоги до кіберстійкості для всіх операторів критичної інфраструктури. Це передбачає уніфікацію стандартів управління інцидентами, запровадження чітких процедур повідомлення про кіберінциденти, посилення вимог до управління вразливостями та технічних засобів захисту. Важливим кроком є також закріплення механізмів персональної відповідальності керівництва підприємств за невиконання вимог кібербезпеки, що відповідає логіці NIS2 і стимулює більш відповідальне ставлення менеджменту до питань кіберстійкості.

По-четверте, на інституційному рівні доцільно створити центральний координаційний орган або центр резильєнтності, відповідальний за стратегічне планування, міжсекторальну координацію, методичне забезпечення оцінювання ризиків, комунікацію з операторами критичної інфраструктури та взаємодію з міжнародними структурами. Такий орган має стати ядром інтегрованої системи управління, що поєднує фізичну та кібернетичну безпеку, забезпечує єдиний інформаційний простір і координацію кризового реагування.

По-п'яте, важливо системно розвивати державно-приватне партнерство, оскільки значна частина критичної інфраструктури перебуває у приватній власності. Необхідно закріпити в законодавстві інструменти та стимули для участі бізнесу в забезпеченні стійкості: спільне фінансування модернізації об'єктів, участь у програмах кіберзахисту, регулярних навчаннях і стрес-тестах, розбудова механізмів захищеного обміну інформацією про загрози та інциденти. Такий підхід відповідає рекомендаціям OECD, де узгоджена взаємодія держави та приватного сектора розглядається як один із ключових факторів ефективності системи критичної інфраструктури.

По-шосте, перспективним напрямом є запровадження індикаторів та метрик резильєнтності – кількісних і якісних показників, які дозволяють оцінювати рівень стійкості інфраструктурних систем, ефективність заходів безпеки та готовність суб'єктів до кризових ситуацій. Вони мають бути інтегровані в національні стандарти, методичні рекомендації та процедури аудиту, що узгоджується з практиками ЄС і OECD.

Подальший розвиток нормативної бази має включати оновлення секторальних стандартів для енергетики, транспорту, зв'язку, охорони здоров'я, водопостачання та інших критичних секторів із урахуванням вимог CER, NIS2 та принципів багаторівневої інфраструктурної стійкості. Це передбачає посилення вимог до управління активами, резервування потужностей, децентралізації, захисту ланцюгів постачання та цифрової трансформації.

Таким чином, удосконалення нормативно-правової бази критичної інфраструктури України має розгортатися одночасно в законодавчому, інституційному, кібернетичному та управлінському вимірах. Гармонізація з директивами CER і NIS2 та впровадження рекомендацій OECD не лише забезпечать формальну відповідність європейським стандартам, а й створять підґрунтя для побудови резильєнтної моделі розвитку критичної інфраструктури, здатної ефективно функціонувати в умовах воєнних та гібридних загроз і забезпечувати довгострокову стійкість держави.

ВИСНОВКИ

Проведене дослідження дозволило комплексно охарактеризувати сучасні теоретико-правові підходи до визначення критичної інфраструктури, узагальнити міжнародні стандарти її регулювання та оцінити рівень відповідності українського законодавства вимогам директив CER і NIS2 та рекомендаціям OECD. Установлено, що в умовах воєнної агресії, масштабних руйнувань, ескалації гібридних і кібернетичних загроз питання забезпечення резильєнтності критичної інфраструктури перетворюється на ключову складову національної безпеки, стабільності державного управління та повоєнного відновлення економіки.

Аналіз міжнародних документів засвідчив, що сучасна європейська та глобальна практика розглядає критичну інфраструктуру як складну соціотехнічну систему, стійкість якої досягається завдяки інтеграції функціонального підходу до визначення критичних послуг, багаторівневого управління ризиками, уніфікованих вимог до кіберстійкості, ефективної міжвідомчої координації та активної участі приватного сектору. Директиви CER та NIS2 формують високі стандарти оцінювання ризиків, категоризації критичних суб'єктів, розроблення стратегій забезпечення стійкості, реагування на інциденти та управління цифровими вразливостями. Рекомендації OECD доповнюють ці вимоги управлінськими, стратегічними та інституційними інструментами, необхідними для розбудови довгострокової адаптивності інфраструктурних систем.

Встановлено, що українське законодавство загалом відображає основні тенденції розвитку міжнародної практики, однак залишається структурно незавершеним і потребує суттєвої модернізації. Домінування об'єктно-секторальної логіки, недостатня деталізація вимог до ризик-менеджменту, відсутність законодавчо закріпленої категорії «критичної послуги», нерозвиненість механізмів кіберстійкості та інституційної координації свідчать про необхідність переходу до інтегрованої, функціонально орієнтованої системи, узгодженої зі стандартами CER і NIS2. Разом із тим, наявні нормативні напрацювання створюють підґрунтя для ефективного реформування та подальшої гармонізації з європейським законодавством.

Узагальнюючи результати дослідження, можна стверджувати, що розвиток системи критичної інфраструктури України має спиратися на комплексну модель, яка поєднує правові, інституційні, технічні, цифрові та управлінські елементи, забезпечуючи здатність суспільства та держави до адаптації, відновлення і функціонування в умовах багатовимірних загроз.

Задля досягнення цієї мети запропоновано такі практичні рекомендації. Для *центральних органів державної влади* визначальними є:

- перехід від об'єктно-секторального до функціонального підходу через запровадження у законодавство категорії «критична послуга» та критеріїв її резильєнтності;
- створення національного координаційного органу або центру резильєнтності, відповідального за інтеграцію фізичної та кібернетичної безпеки, стандартизацію ризик-менеджменту, проведення аудитів стійкості та розроблення стратегічних документів відповідно до вимог CER і NIS2;
- удосконалення правових механізмів державно-приватного партнерства, що повинно стати ключовим інструментом розвитку стійких інфраструктурних мереж.

Операторам критичної інфраструктури рекомендовано впроваджувати розширені системи управління ризиками, які охоплюють оцінювання фізичних, технологічних, кібернетичних та операційних загроз, застосування стрес-тестування,

формування планів безперервності діяльності та адаптивних процедур. Особлива увага має приділятися виконанню вимог NIS2, включно з моніторингом кіберризиків, обов'язковим звітуванням про інциденти, підвищенням відповідальності керівництва та розвитком внутрішніх компетенцій у сфері кібербезпеки.

З боку *міжнародних партнерів* (ЄС, OECD, UNIDO, НАТО, структур міжнародної технічної допомоги) Україні є доцільною та важливою підтримка у площині формування нормативних, інституційних та технічних засад резильєнтності, сприяння обміну передовим досвідом, модернізації цифрової та енергетичної інфраструктури, впровадження індикаторів стійкості та комплексних систем управління ризиками.

Суб'єктам місцевого самоврядування (територіальні громади, органи місцевого самоврядування) варто розширити роботу зі створення регіональних паспортів ризиків, підвищення стійкості локальних інфраструктурних об'єктів, розвитку енергетичної децентралізації, удосконалення систем оповіщення та цивільного захисту, а також з активізації взаємодії з операторами та громадськістю.

Перспективи подальших наукових досліджень пов'язано зі створенням методології багаторівневого оцінювання резильєнтності; моделюванням сценаріїв впливу комплексних загроз; розробленням секторальних індикаторів стійкості; вивченням цифрових, організаційних і поведінкових механізмів підвищення здатності держави до кризового реагування.

Важливим пріоритетом досліджень є формування концептуальної моделі резильєнтної системи критичної інфраструктури України, що інтегруватиме положення CER і NIS2, методологічні принципи OECD та національні безпекові потреби. Це забезпечить наукове підґрунтя для побудови сучасної, стійкої та адаптивної критичної інфраструктури, здатної підтримувати життєздатність держави в умовах довготривалих криз і майбутніх викликів. ■

БІБЛІОГРАФІЯ

1. Ukraine. Rapid damage and needs assessment (RDNA4). February 2022 – December 2024. Washington, DC : World Bank, 2025. 195 p. URL: https://openknowledge.worldbank.org/server/api/core/bitstreams/96bd9c94-c327-49b4-8aff-fe125686f04e/content
2. Report on damages to infrastructure from the destruction caused by Russia's military aggression against Ukraine as of November 2024 / D. Andrienko, D. Goriunov, V. Grudova et al. Kyiv: KSE Institute, 2025. 26 p. URL: https://kse.ua/wp-content/uploads/2025/02/KSE_Damages_Report-November-2024---ENG.pdf.
3. Hallegatte S., Rentschler J., Rozenberg Ju. Lifelines: The Resilient Infrastructure Opportunity. Washington, DC: The World Bank, International Bank for Reconstruction and Development, 2019. 224 p. URL: https://documents1.worldbank.org/curated/en/111181560974989791/pdf/Lifelines-The-Resilient-Infrastructure-Opportunity.pdf
4. Business Climate Survey 2023–2024. Kyiv : European Business Association (EBA), 2024. URL: https://eba.com.ua/en/research/doslidzhennya-ta-analityka/
5. Річний звіт системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Київ : Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України, 2024. 24 с. URL: https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006
6. Індекс цифрової трансформації регіонів України (підсумки 2024 року). Київ : Міністерство цифрової трансформації України, 2024. 28 с. URL: https://storage.thedigital.gov.ua/files/a/5a/7be6e4e930076257945a29847c6035a9.pdf
7. Directive (EU) 2022/2557 of the European Parliałment 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. P. 164–198. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng
8. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). *Official Journal of the European Union*. 2022. 27 December. P. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
9. Good Governance for Critical Infrastructure Resilience. OECD Reviews of Risk Management Policies. Paris : OECD Publishing, 2019. 118 p. DOI: https://doi.org/10.1787/02f0e5a0-en
10. Закон України «Про критичну інфраструктуру» від 16.11.2021 р. № 1882-IX (із змінами, у редакції від 21.09.2024 р.). URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text
11. Ampratwum G., Osei-Kyei R., Tam V. W. Y. Developeing a performance assessment tool for building critical infrastructure resilience through Public-Private Partnership in Ghana. *International Journal of Critical Infrastructure Protection*. 2025. Vol. 50. Art. 100784. DOI: https://doi.org/10.1016/j.ijcip.2025.100784
12. Brown C., Seville E., Vargo J. Measuring the organizational resilience of critical infrastructure providers: A New Zealand case study. *International Journal of Critical Infrastructure Protection*. 2017. Vol. 18. P. 37–49. DOI: https://doi.org/10.1016/j.ijcip.2017.05.002

13. Brucherseifer E., Winter H., Mentges A., Mühlhäuser M., Hellmann M. Digital Twin conceptual framework for improving critical infrastructure resilience. *At-Automatisierungstechnik*. 2021. Vol. 69. Iss. 12. P. 1062–1080.
DOI: https://doi.org/10.1515/auto-2021-0104
14. Hromada M., Rehak D., Kontogeorgos M., Walker N. External Resilience Assessment of Energy Critical Infrastructures. Energy System Resilience and Distributed Generation. *Power Systems*. 2024. Part F3518. P. 109–142.
DOI: https://doi.org/10.1007/978-3-031-67754-0_4
15. Rehak D., Senovsky P., Slivkova S. Resilience of Critical Infrastructure Elements and Its Main Factors. *Systems*. 2018. Vol. 6. Iss. 2. Art. 21.
DOI: https://doi.org/10.3390/systems6020021
16. Rehak D., Slivkova S., Janeckova H., Stuberova D., Hromada M. Strengthening Resilience in the Energy Critical Infrastructure: Methodological Overview. *Energies*. 2022. Vol. 15. Iss. 14. Art. 5276.
DOI: https://doi.org/10.3390/en15145276
17. Rød B., Lange D., Theocharidou M., Pursiainen Ch. From Risk Management to Resilience Management in Critical Infrastructure. *Journal of Management in Engineering*. 2020. Vol. 36. No. 4. Art. 04020039.
DOI: https://doi.org/10.1061/(ASCE)ME.1943-5479.0000795
18. Wells E. M., Boden M., Tseytlin I., Linkov I. Modeling critical infrastructure resilience under compounding threats: A systematic literature review. *Progress in Disaster Science*. 2022. Vol. 15. Art. 100244.
DOI: https://doi.org/10.1016/j.pdisas.2022.100244
19. Zhao X., Chen Z., Gong H., Li Q. Review on the study of disaster resilience of critical infrastructure systems. *China Civil Engineering Journal*. 2017. Vol. 50. Iss. 12. P. 62–71.
20. Hall J., Sandeman H. NATO's Resilience: The first and last line of defence. London : LSE IDEAS, 2022. 18 p. URL: https://www.lse.ac.uk/ideas/Assets/Documents/updates/2022-SU-NATO-HallSandeman.pdf
21. CER and NIS-2 Directives enter into force to strengthen EU's Resilience. *European Commission*. 2022. 26 October. URL: https://ec.europa.eu/newsroom/cipr/items/764849/en
22. Скалецький Ю. М., Бірюков Д. С., Кондратов С. І. Європейський досвід розбудови системи захисту критичної інфраструктури: уроки для України: аналіт. записка. Київ : Національний інститут стратегічних досліджень, 2013. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/evropeyskiy-dosvid-rozbudovi-sistemi-zakhistu-kritichnoi
23. Cáceres G. Argentina's critical infrastructures: topics for their regulation. *International Journal of Critical Infrastructures*. 2024. Vol. 20. Iss. 2. P. 97–110.
DOI: https://doi.org/10.1504/IJCIS.2024.137404
24. 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: https://doi.org/10.1504/IJCIS.2012.050108
25. 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.
DOI: https://doi.org/10.26552/com.C.2018.2.41.48
26. 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: https://doi.org/10.4028/www.scientific.net/AMR.1001.80
27. Lagutin V., Boiko A., Shkuropadska D. Institutional Conditions for Ensuring Resilience of National Economy: On the Example of Ukraine. *Baltic Journal of Economic Studies*. 2020. Vol. 6. No. 3. P. 76–86.
DOI: https://doi.org/10.30525/2256-0742/2020-6-3-76-86
28. Shkuropadska D., Lebedeva L., Gonçalves J. Institutional Framework for the Resilience of Critical Infrastructure of EU, NATO Countries and Ukraine. *Scientia Fructuosa*. 2025. No. 1. P. 45–60.
DOI: https://doi.org/10.31617/1.2025(159)03
29. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні: аналітична доповідь. Київ : Національний інститут стратегічних досліджень, 2012. 96 с.
30. Бірюков Д. С., Кондратов С. І., Насвіт О. І., Суходоля О. М. Зелена книга з питань захисту критичної інфраструктури в Україні: аналітична доповідь. Київ : Національний інститут стратегічних досліджень, 2015. 35 с.
31. 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: https://doi.org/10.36695/2219-5521.4.2020.63
32. Мельничук О. В. Ідентифікація об'єктів критичної інфраструктури: базові методи та критерії. *Регіональна політика: історія, політико-правові засади, урбаністика, просторове планування, архітектура* : зб. наук. праць : у 2 ч. Вип. 5. Ч. 2. С. 193–197. URL: https://repositary.knuba.edu.ua/server/api/core/bitstreams/0cd4bcd4-894c-49a7-944a-53ab22d911ae/content
33. Арсенович Л. А. Парадигма захисту критичної інфраструктури в системі національної безпеки України. *Державне управління: удосконалення та розвиток*. 2024. № 8.
DOI: https://doi.org/10.32702/2307-2156.2024.8.7
34. Кизим М. О., Хаустова В. Є., Трушкіна Н. В. Сутність поняття «критична інфраструктура» з позицій національної безпеки України. *Бізнес Інформ*. 2022. № 12. С. 58–78.
DOI: https://doi.org/10.32983/2222-4459-2022-12-58-78

35. Хаустова В., Трушкіна Н., Зінченко В. Ключові виклики відновлення критичної інфраструктури України в умовах повоєнної розбудови економіки. *Повоєнне відновлення економіки України: проблеми та напрямки вирішення* : кол. моногр. / за ред. В. Є. Хаустової. Харків : ФОП Лібуркіна Л. М., 2023. С. 7–33.
36. Хаустова В. Є., Трушкіна Н. В., Проноза П. В. Ідентифікація елементів критичної інфраструктури: закордонний і вітчизняний досвід. *Бізнес Інформ*. 2025. № 8. С. 47–71. DOI: https://doi.org/10.32983/2222-4459-2025-8-47-71
37. Хаустова В. Є., Трушкіна Н. В. Загрози розвитку критичної інфраструктури: сутність і класифікація. *Проблеми економіки*. 2025. № 3. С. 89–104. DOI: https://doi.org/10.32983/2222-0712-2025-3-89-104
38. Хаустова В. Є., Решетняк О. І. Резильєнтність економіки: сутність і виклики для України. *Бізнес Інформ*. 2023. № 7. С. 30–41. DOI: https://doi.org/10.32983/2222-4459-2023-7-30-41
39. 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. С. 76–82. DOI: https://doi.org/10.32836/2310-9653-2022-1.13
40. Єрменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монографія. Дніпро : ДДУВС, 2018. 180 с.
41. Розпорядження Кабінету Міністрів України «Про схвалення Концепції створення державної системи захисту критичної інфраструктури» від 06.12.2017 р. № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-р#Text
42. Концепція забезпечення національної системи стійкості : затверджено Указом Президента України від 27.09.2021 р. № 479/2021. URL: https://zakon.rada.gov.ua/laws/show/479/2021#Text

REFERENCES

Ampratwum G., Osei-Kyei R. & Tam V. W. Y. (2025). Developing a performance assessment tool for building critical infrastructure resilience through Public-Private Partnership in Ghana. *International Journal of Critical Infrastructure Protection*, 50, Art. 100784. https://doi.org/10.1016/j.ijcip.2025.100784

Andrienko D., Goriunov D. & Grudova V. (2025). *Report on damages to infrastructure from the destruction caused by Russia's military aggression against Ukraine as of November 2024*. Kyiv: KSE Institute. https://kse.ua/wp-content/uploads/2025/02/KSE_Damages_Report-November-2024---ENG.pdf

Arsenovych L. A. (2024). Paradyhma zakhystu krytychnoi infrastruktury v systemi natsionalnoi bezpeky Ukrainy [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

Biriukov D. S. & Kondratov S. I. (2012). *Zakhyst krytychnoi infrastruktury: problemy ta perspektyvy vprovadzhennia v Ukraini* [Critical infrastructure protection: problems and prospects for implementation in Ukraine]. Kyiv: Natsionalnyi instytut stratehichnykh doslidzhen.

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 critical infrastructure protection in Ukraine]. Kyiv: Natsionalnyi instytut stratehichnykh doslidzhen.

Brown C., Seville E. & Vargo J. (2017). Measuring the organizational resilience of critical infrastructure providers: A New Zealand case study. *International Journal of Critical Infrastructure Protection, 18*, 37–49. https://doi.org/10.1016/j.ijcip.2017.05.002

Brucherseifer E., Winter H., Mentges A., Mühlhäuser M. & Hellmann M. (2021). Digital Twin conceptual framework for improving critical infrastructure resilience. *At-Automatisierungstechnik, 12*(69), 1062–1080. https://doi.org/10.1515/auto-2021-0104

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

European Business Association (EBA). (2024). *Business Climate Survey 2023–2024*. Kyiv : European Business Association (EBA). https://eba.com.ua/en/research/doslidzhennya-ta-analityka/

European Commission. (2022, October 26). CER and NIS-2 Directives enter into force to strengthen EU's Resilience. *European Commission*. https://ec.europa.eu/newsroom/cipr/items/764849/en

European Parliament & Council of the European Union. (2022, December 27). Directive (EU) 2022/2557 on the resilience of critical entities. *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

European Parliament & Council of the European Union. (2022, December 27). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

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

Hall J. & Sandeman H. (2022). *NATO's Resilience: The first and last line of defence*. London: LSE IDEAS. https://www.lse.ac.uk/ideas/Assets/Documents/updates/2022-SU-NATO-HallSandeman.pdf

Hallegatte S., Rentschler J. & Rozenberg Ju. (2019). *Lifelines: The Resilient Infrastructure Opportunity*. Washington, DC: The World Bank, International Bank for Reconstruction and Development.

https://documents1.worldbank.org/curated/en/111181560974989791/pdf/Lifelines-The-Resilient-Infrastructure-Opportunity.pdf

Hromada M., Rehak D., Kontogeorgos M. & Walker N. (2024). External Resilience Assessment of Energy Critical Infrastructures. *Energy System Resilience and Distributed Generation*. *Power Systems,* 109–142. https://doi.org/10.1007/978-3-031-67754-0_4

Kabinet Ministriv Ukrainy. (2017, December 6). Rozporiadzhennia «Pro skhvalennia Kontseptsii stvorennia derzhavnoi systemy zakhystu krytychnoi infrastruktury» [Order 'On Approval of the Concept of Creating a State Critical Infrastructure Protection System']. https://zakon.rada.gov.ua/laws/show/1009-2017-r#Text

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

Khaustova V., Trushkina N. & Zinchenko V. (2023). *Kliuchovi vyklyky vidnovlennia krytychnoi infrastruktury Ukrainy v umovakh povoiennoi rozbudovy ekonomiky* [Key challenges for the restoration of Ukraine's critical infrastructure in the conditions of post-war economic development]. Kharkiv: FOP Liburkina L. M.

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

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

Kyiv : Operatyvnyi tsentr reahuvannia na kiberintsydenty Derzhavnoho tsentru kiberzakhystu. (2024). *Richnyi zvit systemy vyiavlennia vrazlyvostei i reahuvannia na kiberintsydenty ta kiberataky* [Annual report of the vulnerability detection and response system for cyber incidents and cyber attacks]. https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006

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

Lagutin V., Boiko A. & Shkuropadska D. (2020). Institutional Conditions for Ensuring Resilience of National Economy: On the Example of Ukraine. *Baltic Journal of Economic Studies, 3*(6), 76–86. https://doi.org/10.30525/2256-0742/2020-6-3-76-86

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, 2*(20), 41–48. https://doi.org/10.26552/com.C.2018.2.41.48

Melnychuk O. V. Identyfikatsiia obiektiv krytychnoi infrastruktury: bazovi metody ta kryterii [Identification of critical infrastructure objects: basic methods and criteria]. *Rehionalna polityka: istoriia, politykopravovi zasady, urbanistyka, prostorove planuvannia, arkhitektura.* https://repositary.knuba.edu.ua/server/api/core/bitstreams/0cd4bcd4-894c-49a7-944a-53ab22d911ae/content

Ministerstvo tsyfrovoi transformatsii Ukrainy. (2024). *Indeks tsyfrovoi transformatsii rehioniv Ukrainy* (pidsumky 2024 roku) [Digital transformation index of the regions of Ukraine (results of 2024)]. Kyiv : Ministerstvo tsyfrovoi transformatsii Ukrainy. https://storage.thedigital.gov.ua/files/a/5a/7be6e4e930076257945a29847c6035a9.pdf

OECD (2019). *Good Governance for Critical Infrastructure Resilience*. Paris: OECD Publishing. 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 [The system of state protection of critical infrastructure of Ukraine: genesis, current state and prospects for optimization]. *Chasopys Kyivskoho universytetu prava, 4*, 355–359. https://doi.org/10.36695/2219-5521.4.2020.63

Prezydent Ukrainy. (2021, September 27). Kontseptsiia zabezpechennia natsionalnoi systemy stiikosti [Concept for Ensuring the National Resilience System]. https://zakon.rada.gov.ua/laws/show/479/2021#Text

Rød B., Lange D., Theocharidou M. & Pursiainen Ch. (2020). From Risk Management to Resilience Management in Critical Infrastructure. *Journal of Management in Engineering, 4*(36), Art. 04020039. https://doi.org/10.1061/(ASCE)ME.1943-5479.0000795

Rehak D., Slivkova S., Janeckova H., Stuberova D. & Hromada M. (2022). Strengthening Resilience in the Energy Critical Infrastructure: Methodological Overview. *Energies, 14*(15), Art. 5276. https://doi.org/10.3390/en15145276

Rehak D., Senovsky P. & Slivkova S. (2018). Resilience of Critical Infrastructure Elements and Its Main Factors. *Systems, 2*(6), Art. 21. https://doi.org/10.3390/systems6020021

Shkuropadska D., Lebedeva L. & Gonçalves J. (2025). Institutional Framework for the Resilience of Critical Infrastructure of EU, NATO Countries and Ukraine. *Scientia Fructuosa, 1*, 45–60. https://doi.org/10.31617/1.2025(159)03

Skaletskyi Yu. M., Biriukov D. S. & Kondratov S. I. (2013). *Yevropeiskyi dosvid rozbudovy systemy zakhystu krytychnoi infrastruktury: uroky dlia Ukrainy* [European experience of building a critical infrastructure pro-

tection system: lessons for Ukraine]. Kyiv : Natsionalnyi instytut stratehichnykh doslidzhen. https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/evropeyskiy-dosvid-rozbudovi-sistemi-zakhistu-kritichnoi

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

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

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

Yaremenko O. I. & Strakhnitskyi Ya. O. (2022). Teoretychni pidkhody do vyznachennia definitsii krytychnoi infrastruktury yak obiektu derzhavnoho upravlinnia [Theoretical approaches to determining the definition of critical infrastructure as an object of state management]. *Publichne upravlinnia ta mytne administruvannia, 1*, 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 critical infrastructure protection in European countries: experience for Ukraine]. Dnipro: DDUVS.

Zakon Ukrainy «Pro krytychnu infrastrukturu» vid 16.11.2021 r. № 1882-IX [Law of Ukraine 'On Critical Infrastructure'] (2024, September 21). https://zakon.rada.gov.ua/laws/show/1882-20#Text

Zhao X., Chen Z., Gong H. & Li Q. (2017). Review on the study of disaster resilience of critical infrastructure systems. *China Civil Engineering Journal, 12*(50), 62–71.

УДК 330.522:316.46
JEL: D63; H53; H55; I38
DOI: https://doi.org/10.32983/2222-4459-2025-11-26-34

ВПЛИВ ЕКОНОМІЧНОЇ НЕРІВНОСТІ НА СОЦІАЛЬНУ БЕЗПЕКУ: ВИКЛИКИ ДЛЯ УКРАЇНИ

©2025 **БОНДАРЕВСЬКА К. В., САГАЧ А. І.**

УДК 330.522:316.46
JEL: D63; H53; H55; I38

Бондаревська К. В., Сагач А. І. Вплив економічної нерівності на соціальну безпеку: виклики для України

У статті досліджується вплив економічної нерівності на соціальну безпеку України, зокрема на її соціально-економічну стабільність та життєвий рівень населення. В умовах глобалізації та сучасних викликів, таких як пандемія COVID-19, війна та економічні кризи, рівень економічної нерівності в Україні став одним із основних факторів, що впливають на соціальну безпеку та рівень добробуту громадян. Актуальність дослідження зумовлена необхідністю виявлення та вирішення соціальних проблем, що постають перед Україною в умовах глобальних викликів, а також пошуком шляхів зменшення економічної нерівності через удосконалення державної політики та розробку соціальних ініціатив. Метою статті є вивчення економічної нерівності в Україні як чинника, що має прямий вплив на соціальну безпеку країни. Для цього проаналізовано теоретичні аспекти нерівності та її прояви на прикладі українського суспільства. Автори звертають увагу на важливість вивчення економічної нерівності через існуючі дослідження, статистичні дані та звіти міжнародних організацій, а також національних інституцій, що оцінюють рівень нерівності в Україні. Одним із ключових аспектів є виявлення соціальних груп, найбільш вразливих до економічної нерівності: люди з інвалідністю, малозабезпечені категорії населення, пенсіонери, внутрішньо переміщені особи. Їхній доступ до медичної допомоги, освіти та можливості для економічної активності обмежені через нерівний доступ до ресурсів, що створює додаткові соціальні ризики. Особлива увага приділяється аналізу причин виникнення економічної нерівності в Україні, серед яких можна виділити низький рівень доходів для більшості населення, високий рівень безробіття. Дослідження продемонструвало, що зменшення економічної нерівності може покращити соціальну безпеку. Стаття має значення для розуміння взаємозв'язку між економічною нерівністю та соціальною безпекою і розробки рекомендацій щодо покращення соціально-економічної ситуації в Україні. Проблеми та пропозиції можуть стати основою для подальших досліджень і розробки стратегій державної політики для забезпечення стабільності в суспільстві.

Ключові слова: *економічна нерівність, соціальна безпека, соціальний захист, ринок праці, вразливі верстви населення.*
Рис.: *2.* ***Табл.:*** *3.* ***Бібл.:*** *15.*

Бондаревська Ксенія Валентинівна *– доктор економічних наук, професор, професор кафедри соціального забезпечення та податкової політики, Університет митної справи та фінансів (вул. Володимира Вернадського, 2/4, Дніпро, 49000, Україна)*
E-mail: *Kseny-8888@i.ua*
ORCID: *https://orcid.org/0000-0001-8683-6834*
Researcher ID: *https://www.webofscience.com/wos/author/record/1243656*
Сагач Анастасія Ігорівна *– магістрантка, Університет митної справи та фінансів (вул. Володимира Вернадського, 2/4, Дніпро, 49000, Україна)*
E-mail: *nastya.sagach16@gmail.com*