УДК 281
DOI https://doi.org/10.32782/TNU-2663-6468/2025.5/24

***Гончарук В. Л.***
Приватне акціонерне товариство «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»

# ЗАХИСТ КРИТИЧНИХ ФУНКЦІЙ ДЕРЖАВИ: ІНТЕГРАЦІЯ ЕКОНОМІЧНОЇ, ФІНАНСОВОЇ, ЕНЕРГЕТИЧНОЇ, ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ В СИСТЕМІ НАЦБЕЗПЕКИ

*Міжнародні практики демонструють важливість інтеграційного підходу до забезпечення критичного функціоналу держави, що охоплює правові, організаційні та технологічні механізми, а також державно-приватну співпрацю для координації й розподілу ресурсів. На тлі викликів тривалої війни в Україні швидка адаптація критичної інфраструктури формує основу національного безпекового поля. Метою дослідження є аналіз потенціалу захисту критичних функцій держави в системі національної безпеки у контексті фінансово-економічної, енергетичної, інформаційної безпеки. У статті розглянуто структуру критичної інфраструктури, її місце та роль у системі загальної безпеки держави. Досліджено можливості моделювання та прогнозування потенційних кризових ситуацій та реалізації превентивних заходів для мінімізації деструкції. Обґрунтовано, що посилення стійкості можна досягнути через оптимізацію інструментів та підходів до захисту критичних функцій держави, шляхом впровадження цифрових технологій, розроблення дієвої системи кібербезпеки, інституційної підтримки та кращої координованості між державними та приватними стейкхолдерами у критично важливих галузях. Розглянуто перспективи оптимізації стану критичної інфраструктури в Україні, серед яких – диверсифікація постачання, модернізація енергетичної системи, вдосконалення законодавства згідно європейських вимог, покращення інвестиційного клімату. Запропоновано узагальнену стратегію підвищення захисту критичних функцій держави у часі підвищених ризиків війни. Дослідження актуалізує необхідність створення стійких гарантій резильєнтності критичної інфраструктури, забезпечення спроможності до її швидкого відновлення, інтеграції політики зміцнення координації, впровадження сучасних моделей управління ризиками, розвитку кібероборони та оптимізації галузевої законодавчої бази.*

***Ключові слова:*** *національна безпека, критична інфраструктура, державне управління, ризики, стійкість, міжнародний досвід, кібербезпека.*

**Постановка проблеми.** Захист критичних функцій держави необхідно розглядати як систему заходів, що наділені векторністю забезпечення стійкості та безперебійного функціонування критичної інфраструктури, що охоплює прогнозування та управління ризиками, розроблення планів реагування, державно-приватне партнерство та міжнародну взаємодію для нівелювання загроз національній безпеці.

Критична інфраструктура, що охоплює енергетичні, транспортні, фінансові, інформаційні та комунікаційні системи, безпосередньо впливає на національну безпеку, оскільки її збій або руйнування може призвести до серйозних наслідків, що загрожують суверенітету, територіальній цілісності та функціонуванню держави. При цьому, руйнування критичної інфраструктури зумовлює нерівномірність економічного розвитку, регіональний дисбаланс, відтік фінансового та інтелектуального капіталу, зростання соціальної поляризації, сповільнення інноваційної діяльності та інвестиційного процесу, посилення екологічних проблем.

Виклики війни в Україні зумовлюють необхідність розроблення нових підходів до публічного управління в сфері національної безпеки та захисту критичних функцій держави, які повинні враховувати складний характер загроз фінансово-економічного, енергетичного, інформаційного спрямування.

**Аналіз останніх досліджень і публікацій.** Проблематика активно розробляється у сучасному науковому дискурсі. Зокрема, ученими А. Ільєнко та ін. [8], С. Іванюта та ін. [10], I. Yefimenko та ін. [18] було встановлено основні напрямки впливу захищеності критичної інфраструктури на стан загальнонаціональної безпеки, зокрема – стійкість протидії загрозам (як кібератакам, так і фізичним

руйнуванням), рівень спроможності до регенерації, економічні наслідки від пошкодження інфраструктури та перерви в її функціонуванні, динаміка обороноздатності, рівень довіри суспільства до влади та підтримка соціальної стабільності.

Дослідники C. Alcaraz, S. Zeadally [1], J. Ingvarson, H. Hassel [9] акцентують на важливості врахування каскадного ефекту загроз критичній інфраструктурі, за якого збій одного елемента чинить значний вплив на всю систему безпеки. На продовження, B. Pacek, P. Pacek [14], C. Große [3] виявили основні аспекти вимірювання впливу критичної інфраструктури на національну безпеку, серед яких – кількісна оцінка руйнувань та фінансових втрат; оцінка слабких місць, які можуть бути потенційно уражені; моніторинг; моделювання потенційних наслідків загроз для критичної інфраструктури.

Низкою дослідників, N. Li та ін. [12] детермінована необхідність підвищення обізнаності державних службовців щодо забезпечення безперебійної роботи об'єктів, запобігання несанкціонованому втручанню, прогнозування кризових ситуацій. Також, вчені переконують у необхідності налагодження співпраці між державним сектором, громадськістю та бізнесом в контексті спільних інтересів у боротьбі з кіберзагрозами, наголошуючи на необхідності міжвідомчої координації та державно-приватного партнерства для підвищення надійності систем. На розширення тематичних наративів, S. Rass та ін. [15] просувають інноваційні системи IDS для виявлення трафіку атак, переконуючи: якщо на об'єкти критичної інфраструктури інвестувати більше ресурсів захисту, здатність стійкості до вторгнень може бути значно вищою.

Актуальними вбачаються публікації науковців O. Heino та ін. [6], G. Dimitropoulos [2], де виокремлено межі відповідальності стейкхолдерів щодо захисту критичної інфраструктури: держава визначає національну політику в галузі, формує законодавчі вимоги та координує роботу національної системи захисту критичної інфраструктури; водночас, власники (оператори) несуть відповідальність за забезпечення належного рівня захищеності об'єктів, розробку та впровадження заходів із захисту, а також кіберзахист.

Не зважаючи на суттєві наукові напрацювання, проблематика переосмислення ролі критичної інфраструктури в системі національної безпеки у часі війни потребує розширеного наукового дослідження і розробки дієвих механізмів захисту.

**Постановка завдання.** Метою дослідження є аналіз потенціалу захисту критичних функцій держави в системі національної безпеки у контексті інтеграції фінансово-економічних, енергетичних, інформаційних аспектів.

Для досягнення поставленої мети було використано сукупність загальнонаукових та спеціальних методів дослідження: аналітичний метод використовувався для систематизації наукових підходів щодо функціоналу критичної інфраструктури в системі національної безпеки; метод моделювання – для оцінки кризових сценаріїв та потенційних наслідків загроз; методи синтезу та узагальнення – для розроблення концепції формування ефективних механізмів її захисту в умовах воєнного стану в Україні.

Обмеження дослідження пов'язані зі складнощами експериментальної перевірки теоретичних висновків, а також несистематичним дослідженням та потенційною регіональною упередженістю.

**Виклад основного матеріалу.** Критична інфраструктура, що включає енергетичний сектор, транспортні системи, інформаційно-комунікаційні технології, фінансовий сектор та охорону здоров'я, визначається як сукупність об'єктів, систем та мереж, порушення функціонування яких має значний вплив на безпеку та стабільність держави.

Станом на 2025 рік інтенсивність загроз для критичної інфраструктури України на тлі військових викликів продовжує зростати, при цьому особливої популярності здобувають гібридні атаки, що торкаються різних сфер. Кожен елемент системи національної безпеки виконує унікальну функцію, а вразливість одного сегмента може створювати каскадний ефект, що актуалізує багатовимірність ризиків деструкції критичної інфраструктури та актуалізує нагальну потребу у вдосконаленні механізмів її захисту [4].

Енергетична інфраструктура України позиціонується однією із найбільш постраждалих галузей, що стало причиною підвищених ризиків для безпеки, сповільнення інвестування та зниження темпів соціально-економічного розвитку. Станом на початок 2024 року розміри прямих збитків від руйнування інфраструктури агресором на території України у період від лютого 2022 р. до початку 2024 р. досягнули 137 млрд дол. США (рис. 1).

Результати статистичних підрахунків засвідчили, що найбільшого пошкодження, окрім цивільної, зазнали енергетична та промислова інфраструктура, регенерація якої потребує значних фінансових вкладень, регулярних дотацій

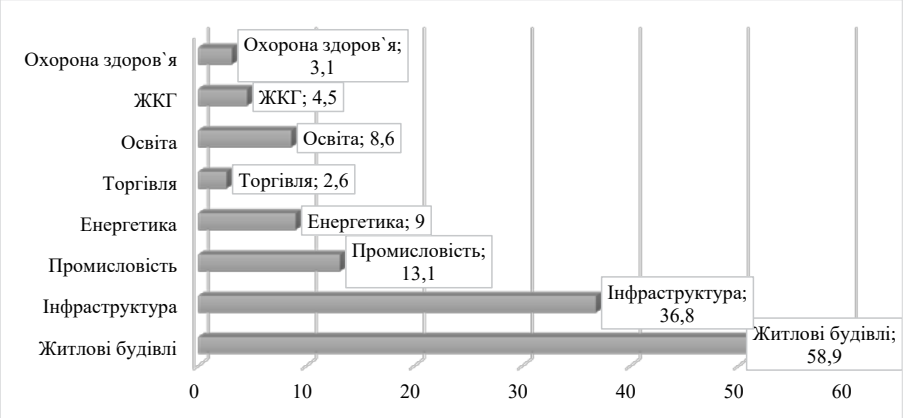


**Рис. 1. Прямі збитки від пошкодження та руйнування інфраструктури росією під час війни в Україні, млрд дол. США**

*Джерело: систематизовано на основі [17]*

та трансферів. Зростає потреба у швидкому відновленні зруйнованих об'єктів та забезпеченні їхньої стійкості.

Україна декларує прагнення гармонізувати систему захисту інфраструктури з європейськими та світовими стандартами. Основним завданням є створення комплексної стратегії захисту критичної інфраструктури має стати посилення координації між державними органами та приватним сектором для впровадження сучасних стандартів стійкості, створення національної системи кібероборони та підготовки фахівців.

Зважаючи на євроінтеграційну векторність, необхідно зауважувати практику держав Європейського Союзу, де аспекти захисту критичної інфраструктури визначаються Директивою 2008/114/ ЕС [11]. Ключовими концептами європейської стратегії захисту є визнання транснаціонального характеру загроз, централізоване управління ними, кіберзахист та інтегрований підхід, який поєднує правові, організаційні та технологічні механізми.

Важливим інструментом підвищення ефективності захисту критичних функцій держави виступає моделювання та прогнозування загроз. Розвиток кризових ситуацій у сфері критичної інфраструктури має різні сценарії залежно від масштабу та характеру загроз. Можливим є як локальне порушення функціонування окремого об'єкта з обмеженим впливом, так і каскадне поширення кризи на інші сектори інфраструктури чи навіть системний сценарій, коли порушується робота декількох секторів одночасно [13]. У таких умовах держава стикається з ризиком паралічу ключових функцій управління та життєзабезпечення. Наслідки кризових сценаріїв включають економічні збитки, соціальну нестабільність та зниження обороноздатності. Моделювання можливих сценаріїв дозволяє прогнозувати ризики та формувати превентивні заходи реагування (табл. 1).

Зауважені у (табл. 1) підходи створюють можливості для визначення як прямих, так і непрямих наслідків потенційних загроз для критичної інфраструктури. Вибір конкретної моделі залежить від специфіки сектора (енергетичний, фінансово-економічний, інформаційний) та характеру потенційних ризиків. Моделі демонструють різні рівні ефективності: системний підхід дозволяє враховувати взаємозалежність секторів, багаторівнева модель дає деталізацію на рівні об'єкта, регіону та держави, а кібермодель виявляє роль інформаційних потоків у стабільності систем.

Таблиця 1

**Моделювання ризиків для критичної інфраструктури**

| Тип моделі | Особливості | Потенційні переваги | Основні недоліки |
|---|---|---|---|
| Системна | Інфраструктура розглядається як єдина взаємопов'язану систему | Дозволяє оцінювати каскадні ефекти | Складна для практичного застосування |
| Багаторівнева | Аналізує ризики на рівні об'єкта, регіону та держави | Забезпечує детальну оцінку загроз на різних рівнях | Потребує великої кількості даних |
| Кібернетична | Зосереджується на інформаційних потоках та управлінні системою | Враховує цифрові технології та кібербезпеку | Обмежена для нецифрових загроз |

*Джерело: складено автором*

Цифровізація захисних механізмів у сфері критичної інфраструктури підвищує ефективність управління та контролю, забезпечуючи оперативний збір даних про стан систем і можливі загрози. Концепція стійкості передбачає резильєнтність критичної інфраструктури до кризових впливів та включає превентивні заходи, моніторинг, реагування та відновлення після інцидентів. Використання моделей стійкості дозволяє мінімізувати каскадні ефекти та підвищити надійність систем [5]. У даному контексті особливої значимості набуває державно-приватна взаємодія, адже більшість об'єктів інфраструктури належить приватним операторам. Державно-приватне партнерство передбачає спільну відповідальність за управління ризиками та реалізацію заходів безпеки, обмін інформацією між суб'єктами, включаючи дані про загрози та інциденти, що підвищує ефективність реагування та оптимізує використання ресурсів.

Для швидкої регенерації критичної інфраструктури та підвищення її стійкості в кризових умовах воєнного часу державні інституції мають впроваджувати ефективні механізми інвестиційного розвитку: розвиток індустріальних парків, страхування інвестиційних ризиків у пріоритетних секторах, безвідсоткове кредитування проєктів з регенерації зруйнованої чи пошкодженої інфраструктури, фінансове стимулювання трансферу «зелених» технологій, підтримку промислово-інфраструктурних інвестиційних проєктів. Комплексний підхід дозволить оптимізувати інвестиційний клімат, успішно проводити релокацію виробництва, інтенсифікувати місцеві бюджетні вливання, що позитивно впливатиме на національне безпекове поле.

Також, важливим є залучення цифрових технологій для гарантії відкритості та прозорості процедур прийняття рішень щодо критичної інфраструктури та контролю за їх виконанням, здійснення необхідного коригувального впливу [16]. Електронні інформаційні системи дають можливість швидкого збору та консолідації необхідних даних, прийняття зважених та обґрунтованих рішень, моніторингу та контролінгу результативності [7]. Запропонована концепція сприятиме підвищенню стійкості критичної інфраструктури, оптимізує координацію дій, сприятиме укріпленню системи національної безпеки в цілому.

У контексті України, впровадження інструментів управління ризиками та стійкістю критичної інфраструктури ускладнене недостатнім фінансуванням та слабкою координацією. Державно-приватне партнерство є перспективним, але потребує зміцнення інституцій. Водночас, міжнародний досвід демонструє, що інтеграційний підхід забезпечує найвищу ефективність захисту. Українські реалії захисту критичних функцій держави потребують адаптації міжнародних стандартів та швидкого відновлення об'єктів, підвищення їхньої стійкості. Проблему необхідно розглядати в контексті правового захисту, інституційного забезпечення оцінювання збитків з винної у руйнації інфраструктури сторони, а також міжнародних гарантій, підтримки інвестиційних регенераційних проєктів.

**Висновки.** Критична інфраструктура є ключовим елементом національної безпеки, забезпечуючи стабільність життєдіяльності суспільства та функціонування державних інституцій. Будучи багаторівневою системою з взаємозалежними компонентами, критична інфраструктура України характеризується підвищеною вразливістю в умовах війни.

Міжнародний досвід підтверджує важливість комплексного підходу до її захисту та впровадження стандартів стійкості. Моделювання ризиків дозволяє прогнозувати наслідки та розробляти превентивні заходи, що значно підвищить ефективність галузевого публічного управління. Кращі міжнародні практики демонструють важливість інтеграційного підходу, що охоплює правові, організаційні та технологічні механізми, де державно-приватне партнерство виступає інструментом координації та оптимізації ресурсів. Разом із тим, в українських реаліях впровадження міжнародних стандартів ускладнюється нормативними, інституційними та фінансовими обмеженнями.

Посилення стійкості національної безпеки можна досягнути через оптимізацію інструментів та підходів до захисту критичних функцій держави, шляхом впровадження цифрових технологій, розроблення дієвої системи кібербезпеки, інституційної підтримки та кращої координованості між державними та приватними стейкхолдерами у критично важливих галузях.

Таким чином, дослідження підтверджує стратегічну роль критичної інфраструктури в системі національної безпеки. Водночас воно виявляє розрив між міжнародними практиками та українською реальністю. Подальші дослідження мають бути спрямовані на розробку гнучких механізмів координації та фінансування.

**Список літератури:**

1. Alcaraz C., Zeadally S. Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection.* 2015. №8. Pp. 53–66. https://doi.org/10.1016/j.ijcip.2014.12.002

2. Dimitropoulos G. National security: The role of investment screening mechanisms. In: *Handbook of international investment law and policy* (pp. 1-37). Springer, 2020. https://doi.org/10.1007/978-981-13-5744-2_59-1

3. Große C. Multi-Level Planning for Enhancing Critical Infrastructure Resilience against Power Shortages–An Analysis of the Swedish System of Styrel. *Infrastructures*. 2021. №6(5), 71. https://doi.org/10.3390/infrastructures6050071

4. Guarini E., Mori E., Zuffada E. New development: embedding the SDGs into city strategic planning. *Public Money and Management*. 2021. №41(6). Pp. 494–497. URL: https://www.emerald.com/insight/content/doi/10.1108/JPBAFM-02-2021-0031/full/html

5. Gunawan Y., Pane M. Responsibility for Excessive Infrastructure Damage in Attacks: Analysing Russia's Attack in Ukraine. *PETITA*. 2024. №9, 212. URL: https://heinonline.org/HOL/LandingPage?handle=hein.journals/petita9&div=18&id=&page=

6. Heino O., Takala A., Jukarainen P., Kalalahti J., Kekki T., Verho P. Critical Infrastructures: The Operational Environment in Cases of Severe Disruption. *Sustainability*. 2019. №11(3). P. 838. https://doi.org/10.3390/su11030838

7. Герасименко О., Сірий О. (2025). Нормативно-правове забезпечення міжнародного співробітництва Служби безпеки України під час протидії кримінальним правопорушенням на об'єктах критичної інфраструктури. *Аналітичне та порівняльне правознавство.* № 3. С. 451–464. http://dx.doi.org/10.24144/2788-6018.2025.03.3.70

8. Ільєнко А., Телющенко В., Дубчак О. Сучасні кіберзагрози критичної інфраструктури України та світу. Електронне фахове наукове видання *«Кібербезпека: освіта, наука, техніка»*. 2025. №3 (27). С. 150–164. http://dx.doi.org/10.28925/2663-4023.2023.27.719

9. Ingvarson J., Hassel H. On the strength of arguments related to standardization in risk management regulations. Safety Science. 2023. №158, 105998. https://doi.org/10.1016/j.ssci.2022.105998

10. Іванюта С. П., Панов Є. М., Іваненко О. І., Гапон С. В. Оцінка ризиків критичній інфраструктурі України в умовах російської військової агресії. *Вісник НТУУ «КПІ імені Ігоря Сікорського». Серія: Хімічна інженерія, екологія та ресурсозбереження*. 2024. № 2. С. 47–61. http://dx.doi.org/10.20535/2617-9741.2.2024.307360

11. Kalapodis N., Sakkas, G., Kazantzidou-Firtinidou D., Alcasena F., Cardarilli M., Eftychidis G., Schultz A. Towards Resilient Critical Infrastructure in the Face of Extreme Wildfire Events: Lessons and Policy Pathways from the US and EU. *Infrastructures*. 2025. №10(9), 246. https://doi.org/10.3390/infrastructures10090246

12. Li N., Wang F., Magoua J. J., Fang D. Interdependent effects of critical infrastructure systems under different types of disruptions. *International Journal of Disaster Risk Reduction.* 2022. №81, 103266. https://doi.org/10.1016/j.ijdrr.2022.103266

13. Novotny P., Janosikova M. Designating Regional Elements System in a Critical Infrastructure System in the Context of the Czech Republic. *Systems*. 2020. №8(2), 13. https://doi.org/10.3390/systems8020013

14. Pacek B., Pacek P. Russia's devastating impact on critical infrastructure during the hybrid war in Ukraine. *Bezpieczeństwo*. *Teoria i Praktyka.* 2023. №2. Pp. 11–27. URL: https://www.ceeol.com/search/article-detail?id=1169528

15. Rass S., Schauer S., König S., Zhu Q. Cyber-Security in Critical Infrastructures. *Springer International Publishing,* 2020. https://doi.org/10.1007/978-3-030-46908-5

16. Roshanaei M. Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. *Journal of Computer and Communications.* 2021. №09. Pp. 80–102. http://dx.doi.org/10.4236/jcc.2021.98006

17. State Statistics Service of Ukraine, 2024. URL: https://www.ukrstat.gov.ua

18. Yefimenko I., Sakovskyi A., Bilozorov Y. Protection of critical infrastructure as a component of Ukraine's national security. *Ûridičnij časopis Nacìonal'noï akademìï vnutrìšnìh sprav.* 2023. №13. http://dx.doi.org/10.56215/naia-chasopis/2.2023.74

**Goncharuk V. L. PROTECTION OF CRITICAL STATE FUNCTIONS: INTEGRATION OF ECONOMIC, FINANCIAL, ENERGY, INFORMATION AND CYBER SECURITY INTO THE NATIONAL SECURITY SYSTEM**

*International practices demonstrate the importance of an integrated approach to ensuring the critical functionality of the state, which includes legal, organizational and technological mechanisms, as well as public-private cooperation for the coordination and distribution of resources. Against the backdrop of the challenges of the protracted war in Ukraine, the rapid adaptation of critical infrastructure forms the basis of the national security field. The purpose of the study is to analyze the potential for protecting critical functions of the state in the national security system in the context of financial and economic, energy, and information security. The article examines the structure of critical infrastructure, its place and role in the overall security system of the state. The possibilities of modeling and forecasting potential crisis situations and implementing preventive measures to minimize destruction are investigated. It is substantiated that increased resilience can be achieved through optimization of tools and approaches to protecting critical functions of the state, through the introduction of digital technologies, the development of an effective cybersecurity system, institutional support, and better coordination between public and private stakeholders in critical industries. The prospects for optimizing the state of critical infrastructure in Ukraine are considered, including diversification of supply, modernization of the energy system, improvement of legislation in accordance with European requirements, and improvement of the investment climate. A generalized model for increasing the protection of critical functions of the state in times of increased risks of war is proposed. The study highlights the need to create sustainable guarantees of resilience of critical infrastructure, ensure the ability to quickly restore it, integrate policies to strengthen coordination, implement modern risk management models, develop cyber defense, and optimize the sectoral legislative framework.*

***Key words:*** *national security, critical infrastructure, public administration, risks, resilience, international experience, cybersecurity.*

Дата надходження статті: 31.10.2025
Дата прийняття статті: 20.11.2025
Опубліковано: 29.12.2025