Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2025. № 12.

DOI: http://doi.org/10.32702/2307-2156.2025.12.17

УДК 281

В. Л. Гончарук,
адвокат, доктор філософії в галузі права, доцент кафедри інформаційної та фінансової безпеки Інституту безпеки, ПрАТ "ВНЗ МАУП"
ORCID ID: https://orcid.org/ 0000-0002-9627-9530

АРХІТЕКТУРА ДЕРЖАВНОГО УПРАВЛІННЯ ТА ПУБЛІЧНОЇ ПОЛІТИКИ НА ПЕРЕТИНІ ЕКОНОМІЧНОЇ, ЕНЕРГЕТИЧНОЇ ТА КІБЕРБЕЗПЕКИ: МЕХАНІЗМИ СИНХРОНІЗАЦІЇ РІШЕНЬ І КРИЗОВОГО РЕАГУВАННЯ

V. Honcharuk,
PhD in Law, Associate Professor of the Department of Information and Financial Security,
Institute of Security Interregional Academy of Personnel Management (IAPM)

ARCHITECTURE OF PUBLIC ADMINISTRATION AND PUBLIC POLICY AT THE INTERSECTION OF ECONOMIC, ENERGY AND CYBERSECURITY: MECHANISMS FOR SYNCHRONIZATION OF DECISIONS AND CRISIS RESPONSE

На тлі викликів війни в Україні публічна політика у сфері економічної, енергетичної та кібербезпеки має бути спрямована на швидке відновлення та адаптацію критичної інфраструктури як основу національного безпекового поля. Метою дослідження є аналіз функціоналу державного

управління та публічної політики щодо механізмів синхронізації рішень і кризового реагування у сучасному контексті воєнних викликів для енергетичної, економічної та інформаційної безпеки. У статті розглянуто структуру критичної інфраструктури, її місце у системі загальної безпеки держави. Проаналізовано різні методи оцінки ризиків, такі як системні моделі, багаторівневі моделі та кібернетичні моделі, що допомагають прогнозувати можливі кризові ситуації та планувати заходи для запобігання або зменшення шкоди. Розглянуто перспективи покращення стану економічної та енергетичної безпеки в Україні, серед яких – модернізація енергетичної системи і диверсифікація постачання, покращення інвестиційного клімату, вдосконалення законодавства згідно європейських вимог. Запропоновано узагальнену модель архітектури державного управління та публічної політики у безпековій сфері в часі підвищених ризиків війни. Обґрунтовано, що безпекової стійкості можна досягнути за допомогою залучення цифрових технологій і систем кібербезпеки, реалізації правових реформ та забезпечення кращої координації між приватними та державними стейкхолдерами. Дослідження актуалізує критичну важливість резильєнтності критичної інфраструктури, її адаптивності та спроможності до швидкого відновлення, а також актуалізує роль державно-приватного партнерства у безпековій сфері.

Against the backdrop of the challenges of the war in Ukraine, public policy in the field of economic, energy and cybersecurity should be aimed at the rapid restoration and adaptation of critical infrastructure as the basis of the national security field. The purpose of the study is to analyze the functionality of public administration and public policy regarding mechanisms for synchronizing decisions and crisis response in the modern context of military challenges for energy, economic and information security. The article examines the structure of critical infrastructure, its place in the overall security system of the state. Various risk assessment methods are analyzed, such as system models, multi-level models and cybernetic models, which help to predict possible crisis situations and plan measures to prevent or reduce damage. Prospects for improving the state of economic and energy security in Ukraine are considered, including modernization of the energy system and diversification of supply, improvement of the investment climate, improvement of legislation in accordance with European requirements.

During the war in Ukraine, the risks of damage to critical infrastructure are taking on a threatening scale. A generalized model of the architecture of public administration and public policy in the security sector in times of increased risks of war is proposed. It is argued that security resilience can be achieved through the use of digital technologies and cybersecurity systems, the implementation of legal reforms, and ensuring better coordination between private and public stakeholders. The study highlights the critical importance of the resilience of critical infrastructure, its adaptability and ability to recover quickly, and the role of public-private partnerships in the security sector. The study proves that public administration and public policy in the field of energy, information and economic security should develop within the framework of an integration strategy that combines legal, organizational and technological mechanisms, preventive measures of protection and international standards of resilience.

Ключові слова: *публічна політика, критична інфраструктура, національна безпека, державне управління, ризики, стійкість, механізми кризового реагування.*

Keywords: *public policy, critical infrastructure, national security, public administration, risks, resilience, crisis response mechanisms.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Стратегія державного управління та публічної політики в кризових умовах має бути зосереджена на синергії захисту критичної інфраструктури енергетичних, транспортних, фінансово-економічних та інформаційно-комунікаційних систем, з метою попередження нерівномірності економічного розвитку, соціальної поляризації і регіонального дисбалансу, відтоку фінансового та інтелектуального капіталу, кібератак, сповільнення інноваційно-інвестиційної динаміки. Актуальні виклики створюють потребу в нових підходах до публічного управління в сфері безпеки, які повинні враховувати складний характер загроз критичній інфраструктурі та необхідність швидкого реагування.

Архітектура публічної політики та державного управління в таких умовах має передбачати механізми координації та взаємодії, створення стійкої

системи управління на основі публічно-приватної взаємодії, ефективне використання ресурсів, а також достатнє нормативне, інституційне і матеріальне забезпечення процесу практичного впровадження стратегічних заходів. Виникає необхідність розроблення та впровадження узагальненої моделі парадигми публічного управління у безпековій сфері в часі підвищених ризиків війни. Актуальність тематики дослідження обумовлена критичною важливістю досягнення стійкості економічної, енергетичної та інформаційної безпеки, забезпечення резильєнтності критичної інфраструктури, її адаптивності та спроможності до швидкого відновлення, а також актуалізації функціоналу державно-приватної співпраці у безпековій галузі.

Аналіз останніх досліджень і публікацій. Ученими I. Eusgeld та ін. [1], A. Ilyenko та ін. [2], S. Ivaniuta та ін. [3] було встановлено, що економічна, енергетична та інформаційна безпека формують основу для гарантій загальнонаціональної безпеки, забезпечуючи стійкість протидії загрозам (кібератакам, фізичним руйнуванням), підвищуючи здатність до регенерації, сприяючи позитивній динаміці обороноздатності та стабільності функціонування державних інституцій. Дослідники наголошують, що важливо враховувати каскадний ефект загроз, коли збій одного елемента впливає на всю систему безпеки.

Ефективність практичних інструментів публічної політики у безпековій сфері, таких як управління ризиками та стійкістю економічної системи, доводять I. Yefimenko та ін. [4], A. Adegbite та ін. [5]. Автори переконують, що державно-приватне партнерство є перспективним, а інтеграційний підхід забезпечує найвищу ефективність захисту, що, своєю чергою, потребує зміцнення інституційної підтримки. Результати досліджень C. Alcaraz, S. Zeadally [6], V. Grigalashvili, K. Abiashvili [7], G. Ampratwum та ін. [8] демонструють потенціал сучасних моделей управління ризиками на основі адаптації міжнародних стандартів та алгоритмів швидкого відновлення об’єктів критичної інфраструктури, підвищення їхньої стійкості.

Проблематика дослідження висвітлена в сучасному науковому дискурсі в публікаціях Y. Gunawan, M. Pane [9], H. Demirel та ін. [10], M. De Rosa та ін. [11], E. Guarini та ін. [12], де особлива увага зосереджена на необхідності інтеграції стандартів інформаційної безпеки для запобігання несанкціонованому втручанню, прогнозування кризових ситуацій та запобігання їхньому негативному впливу. На продовження, 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.

Актуальними вбачаються публікації O. Herasymenko, O. Siryi [13], B. Pacek, P. Pacek [14], J. Paravantis, N. Kontoulis [15], M. Roshanaei [16], де виокремлено межі відповідальності стейкхолдерів у сфері енергетичної, економічної та інформаційної безпеки: 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 державного управління та публічної політики в системі національної безпеки у часі війни потребує розширеного наукового дослідження і розробки дієвих механізмів захисту критичної інфраструктури у енергетичному, економічному та інформаційному секторах.

Формулювання цілей статті (постановка завдання). Метою дослідження є аналіз функціоналу державного управління та публічної політики щодо механізмів синхронізації рішень і кризового реагування у сучасному контексті воєнних викликів для енергетичної, економічної та інформаційної безпеки.

Виклад основного матеріалу дослідження. Повномасштабна війна засвідчила вразливість критичної інфраструктури України та безпосередній вплив останньої на загальний безпековий контекст у національному масштабі. Лише від лютого 2022 р. до кінця 2023 р. було пошкоджено понад 63 тис. енергетичних об'єктів – загальні прямі збитки енергетики оцінюються у 8,8 млрд дол. США, а у кіберпросторі зафіксовано понад 4,3 тис. інцидентів лише у 2024 році [17, 18]. На сьогодні інтенсивність загроз продовжує зростати, при цьому особливої популярності здобувають гібридні атаки, що дестабілізують одночасно декілька різних сфер. Руйнування критичної енергетичної, виробничо-промислової та цивільної інфраструктури стало причиною підвищених ризиків для безпеки, сповільнення інвестування та зниження темпів соціально-економічного розвитку. Станом на 2024 рік, розміри прямих збитків перевищили 137 млрд дол. США (рис.1).

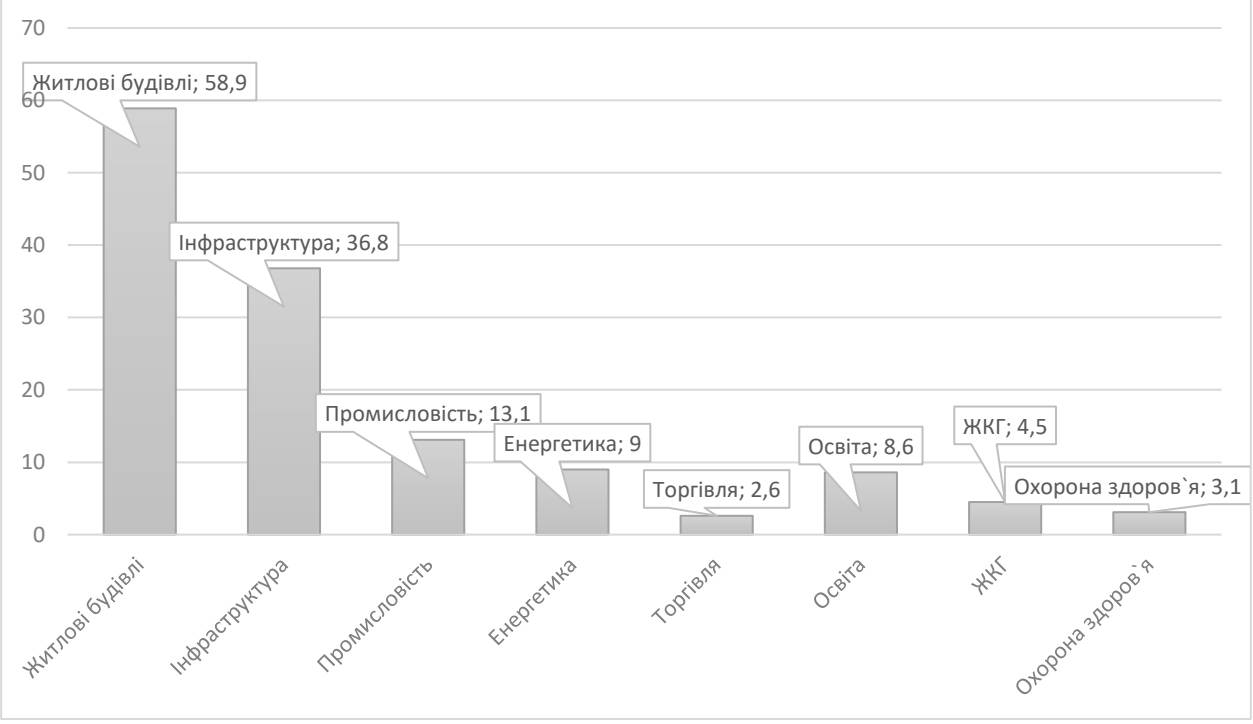

Рис. 1. Прямі збитки від руйнування інфраструктури в Україні станом на 2024 р., млрд. дол. США

Джерело: сформовано на основі [18].

Багатовимірність ризиків деструкції критичної інфраструктури актуалізує потребу у вдосконаленні механізмів її захисту на основі

інтегрованого підходу, який поєднує правові, організаційні та технологічні механізми. Публічна політика у цій сфері в Україні має бути спрямована на прогнозування загроз, запобігання кризовим ситуаціям, зниження ризиків, що потребує гармонізації національного законодавства з міжнародними нормами, модернізації нормативно-правової бази для підвищення ефективності захисту. Ключовими компонентами стратегії ефективного державного управління у сфері безпеки енергетичного, економічного та інформаційного простору мають стати:

1) кризовий менеджмент – система заходів для попередження кризових явищ, стабілізації та ліквідації можливих наслідків;

2) стратегічне планування – формування довгострокового бачення, визначення пріоритетних цілей та завдань для ефективної реалізації державної політики в умовах кризи, нестабільності та підвищених загроз;

3) управління ресурсами, спрямоване на забезпечення стабільності енергетичного сектору та стійкого економічного зростання;

4) інституційна стійкість – забезпечення компетентного, прозорого та ефективного публічного управління, що функціонує в інтересах суспільства;

5) нормативно-правове забезпечення – затвердження положень та державних програм, що врегульовують діяльність в кризових умовах;

6) політична стабільність – підвищення довіри до влади, зниження політичної напруженості, збалансування діяльності владних інститутів.

Зважаючи на зазначене, ключові механізми синхронізації у державному управлінні в сфері економічної, енергетичної та кібербезпеки мають включати: створення єдиної правової основи для забезпечення законності та уніфікованого підходу до вирішення проблем; моделювання системи управлінських рішень на основі науково-системного підходу; інтеграцію колективних форм прийняття рішень з урахуванням позиції усіх стейкхолдерів для їх потенційного узгодження; горизонтальну (взаємодія між різними міністерствами, відомствами та місцевими органами влади) та вертикальну

(співпраця органів державного управління та органів місцевого самоврядування) координацію для різнорівневої синхронізації рішень [7, 12].

Важливим інструментом прогнозування загроз та планування захисту у сфері економічної, енергетичної та кібербезпеки позиціонуються моделі аналізу ризиків – кібернетична (розглядає інфраструктури як складної системи управління, де ключову роль відіграє обмін інформацією), системна (акцентує на взаємозалежності усіх елементів та їх вразливості до зовнішніх впливів) та багаторівнева (передбачає оцінку ризиків на різних рівнях – від окремого об'єкта до національної системи) (табл. 1).

Таблиця 1. Моделі аналізу ризиків для економічної, енергетичної та кібербезпеки

Модель	***Специфіка***	***Переваги***	***Обмеження***
Системна	Розглядає інфраструктуру як єдину 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: сформовано автором

Необхідно зауважити, що моделювання ризиків має різні сценарії: локальне порушення функціонування окремого об'єкта з обмеженим впливом, каскадне поширення кризи на інші сектори інфраструктури або ж системний сценарій, коли порушується робота декількох секторів одночасно. Останній наділений особливою небезпекою, адже у таких умовах держава стикається з ризиком паралічу ключових функцій управління. У зв'язку з цим, сучасні

підходи до управління мають бути зорієнтовані не лише на запобігання загрозам, а й на забезпечення швидкого відновлення [4]. Превентивні заходи, моніторинг, реагування на кризові ситуації та відновлення після інцидентів мають формувати комплексний підхід, що охоплює організаційний, технологічний та правовий рівні, дозволяє мінімізувати каскадні ефекти та підвищити стійкість систем.

Формування ефективної архітектури державного управління у безпековій сфері неможливе без налагодження взаємодії держави та бізнесу, адже переважна більшість об'єктів енергетичної, інформаційної та економічної інфраструктури належить приватним операторам, що актуалізує спільну відповідальність за управління ризиками та впровадження заходів безпеки [10]. Особливої ваги у даному контексті набуває налагодження ефективного обміну інформацією між суб'єктами, що значно підвищує ефективність реагування та оптимізує використання ресурсів.

Основним завданням публічної політики в галузі стає створення комплексної стратегії захисту критичної інфраструктури, посилення координації між державними органами та приватним сектором для впровадження сучасних стандартів стійкості, створення національної системи кібероборони та підготовки фахівців. Також, важливим є подальший розвиток процесів децентралізації та дерегуляції, впровадження пріоритетних моделей державно-приватної взаємодії, залучення цифрових технологій для відкритості даних і прозорості процедур прийняття рішень, контролю за їх виконанням.

Модель архітектури державного управління та публічної політики у сфері енергетичної, економічної та кібербезпеки (рис. 2) має передбачати важливість інтеграції цифрового потенціалу для підвищення стійкості критичної інфраструктури, ефективної координації спільних дій, збору та консолідації необхідних даних для прийняття зважених та обґрунтованих рішень.

Рис. 2. Модель архітектури публічного урядування у сфері енергетичної, економічної та кібербезпеки

Джерело: сформовано автором.

Таким чином, дослідження підтверджує стратегічну роль механізмів взаємодії в системі національної безпеки. Державне управління та публічна політика у сфері енергетичної, інформаційної та економічної безпеки мають бути спрямовані на комплексну підтримку превентивних та регенеруючих заходів із залученням потенціалу публічно-приватної співпраці. Інтеграційний підхід, що охоплює правові, організаційні та технологічні механізми, дозволить швидко реагувати і відновлювати функціонування системи, ефективно впроваджувати міжнародні стандарти стійкості.

Висновки та перспективи подальших розвідок у даному напрямі. Українські реалії характеризуються підвищеною вразливістю критичної інфраструктури в умовах війни. Впровадження міжнародних стандартів в галузі енергетичної, економічної та кібербезпеки ускладнюється нормативними, інституційними та фінансовими обмеженнями, що потребує інтеграції системи управління ризиками та стійкістю, стимулювання державно-приватного партнерства для кращої координації та оптимізації ресурсів.

Пропозиції щодо вдосконалення управлінської парадигми у досліджуваній сфері включають політику зміцнення координації, впровадження сучасних моделей управління ризиками та покращення законодавчого підґрунтя, що сприятиме мінімізації ризиків каскадних ефектів та зміцнить національну безпеку. Комплексна модель публічного управління на перетині економічної, енергетичної та кібербезпеки, запропонована у дослідженні, пропонує формувати управлінську концепцію стійкості на основі нормативно-інституціональної підтримки, інноваційних рішень та партнерства держави, громадськості й бізнесу. Подальші дослідження мають бути спрямовані на розробку гнучких механізмів координації та фінансування публічної політики у досліджуваній сфері.

Ліітература

1. Eusgeld I., Nan C., Dietz S. “System-of-systems” approach for interdependent critical infrastructures. *Reliability Engineering & System Safety*. 2011. №96(6). Pp. 679-686. https://doi.org/10.1016/j.ress.2010.12.010

2. Ilyenko A., Teliushchenko V., Dubchak O. Modern Cyber Threats To Critical Infrastructure In Ukraine And The World. *Cybersecurity: Education, Science, Technique*. 2025. №3. Pp. 150-164. http://dx.doi.org/10.28925/2663-4023.2023.27.719

3. Ivanyuta, S. P., Panov, E. M., Ivanenko, O. I., & Gapon, S. IN. Assessment of risks to the critical infrastructure of Ukraine in the conditions of

Russian military aggressionю *Bulletin of NTUU "KPI named after Ihor Sikorskyi". Series: Chemical Engineering, Ecology and Resource Conservation*. 2024. №2. Pp. 47–61. https://doi.org/10.20535/2617-9741.2.2024.307360

4. 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

5. Adegbite A., Akinwolemiwa D., Uwaoma P., Kaggwa S., Akindote O., Dawodu S. Review of cybersecurity strategies in protecting national infrastructure: perspectives from the USA. *Computer Science & IT Research Journal*. 2023. №4. Pp. 200-219. http://dx.doi.org/10.51594/csitrj.v4i3.658

6. 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

7. Grigalashvili V., Abiashvili K. Conceptual review of the european union critical infrastructure architecture: policy, law and administration. *Social and Economic Aspects of Education in Modern Society.* 2021. Pp. 10-17. http://dx.doi.org/10.31435/rsglobal_conf/25052021/7562

8. Ampratwum G., Robert O.-K., Tam P. Exploring the Concept of Public-Private Partnership in Building Critical Infrastructure Resilience Against Unexpected Events: A systematic Review. *International Journal of Critical Infrastructure Protection.* 2022. №39, P. 100556. https://doi.org/10.1016/j.ijcip.2022.100556

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

10. Demirel H. C., Leendertse W., Volker L. Mechanisms for protecting returns on private investments in public infrastructure projects. International Journal

of Project Management. 2022. №40(3). Pp. 155-166. https://doi.org/10.1016/j.ijproman.2021.11.008

11. De Rosa M., Gainsford K., Pallonetto F., Finn D. P. Diversification, concentration and renewability of the energy supply in the European Union. *Energy*. 2022. №253. https://doi.org/10.1016/j.energy.2022.124097

12. 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. https://www.emerald.com/insight/content/doi/10.1108/JPBAFM-02-2021-0031/full/html

13. Herasymenko O., Siryi O. Regulatory and legal support for international cooperation of the Security service of Ukraine during the fight against criminal offenses at critical infrastructure facilities. *Analytical and Comparative Jurisprudence*. 2025. №3. Pp. 451-464. http://dx.doi.org/10.24144/2788-6018.2025.03.3.70

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. https://www.ceeol.com/search/article-detail?id=1169528

15. Paravantis J. A., Kontoulis N. Energy security and renewable energy: a geopolitical perspective. In *Renewable energy-resources, challenges and applications*. IntechOpen, 2020. DOI: 10.5772/intechopen.91848 https://www.researchgate.net/publication/344733640_Energy_Security_and_Renewable_Energy_A_Geopolitical_Perspective

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. НКРЕКП. Державні сайти України. 2024. https://www.nerc.gov.ua/

18. Державна служба статистики України. 2024. https://www.ukrstat.gov.ua

References

1. Eusgeld, I., Nan, C., & Dietz, S. (2011), “System-of-systems” approach for interdependent critical infrastructures”, *Reliability Engineering & System Safety, vol. 96*(6), pp. 679-686. https://doi.org/10.1016/j.ress.2010.12.010

2. Ilyenko, A., Teliushchenko, V., & Dubchak, O. (2025), “Modern Cyber Threats To Critical Infrastructure In Ukraine And The World”, *Cybersecurity: Education, Science, Technique, vol. 3*, pp. 150-164. http://dx.doi.org/10.28925/2663-4023.2023.27.719.

3. Ivanyuta, S. P., Panov, E. M., Ivanenko, O. I., & Gapon, S. IN. (2024), “Assessment of risks to the critical infrastructure of Ukraine in the conditions of Russian military aggression”, *Bulletin of NTUU “KPI named after Ihor Sikorskyi”. Series: Chemical Engineering, Ecology and Resource Conservation*, vol. 2, pp. 47–61. http://dx.doi.org/10.20535/2617-9741.2.2024.307360.

4. Yefimenko, I., Sakovskyi, A., & Bilozorov, Y. (2023). “Protection of critical infrastructure as a component of Ukraine’s national security”, *Ûridičnij časopis Nacìonal'noï akademìï vnutrìšnìh sprav,* vol. 13. http://dx.doi.org/10.56215/naia-chasopis/2.2023.74.

5. Adegbite, A., Akinwolemiwa, D., Uwaoma, P., Kaggwa, S., Akindote, O., & Dawodu, S. (2023), “Review of cybersecurity strategies in protecting national infrastructure: perspectives from the USA”, *Computer Science & IT Research Journal,* vol. 4, pp. 200-219. http://dx.doi.org/10.51594/csitrj.v4i3.658.

6. Alcaraz, C., & Zeadally, S. (2015), “Critical infrastructure protection: Requirements and challenges for the 21st century”, *International Journal of Critical Infrastructure Protection,* vol. 8, pp. 53-66. https://doi.org/10.1016/j.ijcip.2014.12.002.

7. Grigalashvili, V., & Abiashvili, K. (2021), “Conceptual review of the european union critical infrastructure architecture: policy, law and administration”, *Social and Economic Aspects of Education in Modern Society,* pp. 10-17. http://dx.doi.org/10.31435/rsglobal_conf/25052021/7562.

8. Ampratwum, G., Robert, O.-K., & Tam, P. (2022), “Exploring the Concept of Public-Private Partnership in Building Critical Infrastructure Resilience Against Unexpected Events: A systematic Review”, *International Journal of Critical Infrastructure Protection, vol. 39*, pp. 100556. https://doi.org/10.1016/j.ijcip.2022.100556.

9. Gunawan, Y., & Pane, M. (2024), “Responsibility for Excessive Infrastructure Damage in Attacks: Analysing Russia's Attack in Ukraine”, *PETITA,* vol. 9, pp. 212, available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/petita9&div=18&id=&page (Accessed 10 Nov 2025).

10. Demirel, H. C., Leendertse, W., & Volker, L. (2022), “Mechanisms for protecting returns on private investments in public infrastructure projects”, *International Journal of Project Management,* vol. 40(3), pp. 155-166. https://doi.org/10.1016/j.ijproman.2021.11.008.

11. De Rosa, M., Gainsford, K., Pallonetto, F., & Finn, D. P. (2022), “Diversification, concentration and renewability of the energy supply in the European Union”, *Energy*, vol. 253, P. 124097. https://doi.org/10.1016/j.energy.2022.124097.

12. Guarini, E., Mori, E., & Zuffada, E. (2021), “New development: embedding the SDGs into city strategic planning”, *Public Money and Management*, vol. *41*(6), pp. 494–497, available at: https://www.emerald.com/insight/content/doi/10.1108/JPBAFM-02-2021-0031/full/html (Accessed 12 Nov 2025).

13. Herasymenko, O., & Siryi, O. (2025), “Regulatory and legal support for international cooperation of the Security service of Ukraine during the fight against criminal offenses at critical infrastructure facilities”, *Analytical and Comparative Jurisprudence,* vol. 3, pp. 451-464. http://dx.doi.org/10.24144/2788-6018.2025.03.3.70.

14. Pacek, B., & Pacek, P. (2023), “Russia's devastating impact on critical infrastructure during the hybrid war in Ukraine”, *Bezpieczeństwo. Teoria i Praktyka,*

vol. 2, pp. 11-27, available at: https://www.ceeol.com/search/article-detail?id=1169528 (Accessed 12 Nov 2025).

15. Paravantis, J. A., & Kontoulis, N. (2020), “Energy security and renewable energy: a geopolitical perspective”, In *Renewable energy-resources, challenges and applications.* IntechOpen, available at: https://www.researchgate.net/publication/344733640_Energy_Security_and_Renewable_Energy_A_Geopolitical_Perspective (Accessed 12 Nov 2025). DOI: 10.5772/intechopen.91848

16. Roshanaei, M. (2021), “Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies”, *Journal of Computer and Communications, vol. 09*, pp. 80-102. http://dx.doi.org/10.4236/jcc.2021.98006.

17. NKREKP, (2024), available at: https://www.nerc.gov.ua/ (Accessed 10 Nov 2025).

18. State Statistics Service of Ukraine (2024), available at: https://www.ukrstat.gov.ua (Accessed 10 Nov 2025).

Стаття надійшла до редакції 14.11.2025 р.