МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

МАГОМЕДОВ Андрій Омарович

Кваліфікаційна наукова
праця на правах рукопису

УДК 351.86:005.21:338.24

ДИСЕРТАЦІЯ
КОНЦЕПТУАЛЬНІ ЗАСАДИ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ТРАНСФОРМАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Подається на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.02 – механізми державного управління

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ А. О. Магомедов

Харків – 2026

АНОТАЦІЯ

Магомедов А. О. Концептуальні засади публічного управління у сфері трансформації об'єктів критичної інфраструктури. – *Рукопис.*

Дисертація на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.02 – механізми державного управління. – Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, 2026.

Дисертацію присвячено розробці концептуальних засад публічного управління у сфері трансформації об'єктів критичної інфраструктури в умовах сучасних безпекових викликів, воєнних загроз та післявоєнного відновлення України.

Автором досліджено теоретико-методологічні засади публічного управління у сфері трансформації об'єктів критичної інфраструктури, проаналізовано сучасний стан наукової розробки проблематики, понятійно-категоріальний апарат, функції та особливості управління критичною інфраструктурою. Узагальнено підходи до класифікації об'єктів критичної інфраструктури, визначено їх роль у забезпеченні економічної, соціальної та національної безпеки держави.

Публічне управління об'єктами критичної інфраструктури визначено як складна, багаторівнева система впливу суб'єктів управління (органів державної влади, уповноважених регуляторних інституцій та органів місцевого самоврядування) на об'єкти критичної інфраструктури (енергетичні, транспортні, комунальні, інформаційні та інші життєзабезпечувальні системи), що реалізується через комплекс аналітичних, превентивних та організаційно-управлінських механізмів, із залученням взаємодії з операторами інфраструктури та іншими заінтересованими суб'єктами, і спрямоване на забезпечення безперервності функціонування критично важливих систем, їх стійкості до загроз та захисту життєво важливих інтересів суспільства і держави.

Проаналізовано нормативно-правове забезпечення управління критичною інфраструктурою в Україні та визначено напрями його адаптації до європейських стандартів. Удосконалено комплексний механізм публічного управління трансформацією об'єктів критичної інфраструктури, який, на відміну від наявних підходів, структуровано за принципом інтеграції функціональних, ресурсних та інформаційних контурів управління з чітким закріпленням ролей суб'єктів на кожному етапі трансформації. До структури механізму входять: нормативно-правовий, інституційний, організаційно-інформаційний, фінансово-економічний, технологічний та цифровий механізми. У межах механізму виділено взаємопов'язані блоки: а) блок стратегічного планування, б) блок координації та в) блок операційного реагування.

Проаналізовано міжнародний досвід держав-членів Європейського Союзу, США, Канади, Ізраїлю та Австралії щодо управління, захисту та забезпечення стійкості критичної інфраструктури. Визначено перспективні напрями адаптації зарубіжних практик до українських реалій, зокрема у сферах міжвідомчої координації, державно-приватного партнерства, кібербезпеки та управління ризиками. Встановлено, що інтеграція європейських підходів до захисту критичної інфраструктури сприятиме підвищенню стійкості держави до сучасних безпекових викликів.

Удосконалено науковий підхід до класифікації об'єктів критичної інфраструктури, формування мережі взаємозалежностей між різними секторами критичної інфраструктури в Україні, визначення матриці загроз критичній інфраструктурі, характеристики елементів системи управління та захисту об'єктів критичної інфраструктури.

Розроблено концептуальну модель взаємодії суб'єктів управління, побудовану на принципах синергії, вертикальної відповідальності та цільової результативності. Сформовано систему показників оцінювання ефективності управління трансформаційними процесами, що враховує рівень адаптивності, цифрової зрілості, стійкості та швидкості реагування на загрози.

Досліджено стан пошкодження та руйнування об'єктів критичної інфраструктури України внаслідок збройної агресії, визначено основні проблеми

відбудови та модернізації критичних об’єктів. Встановлено відсутність комплексної системи стратегічних документів та механізмів відновлення критичної інфраструктури. Обґрунтовано доцільність застосування проєктної методології PMBOK, елементів Agile-підходу та механізмів державно-приватного партнерства для реалізації програм повоєнної реконструкції та відновлення інфраструктурних об’єктів.

Сформовано Концепцію публічного управління змінами об’єктів критичної інфраструктури, яка на відміну від відомих, працює через поєднання стратегічно-планувального, ресурсного та інституційного контурів управління. У межах концепції управлінські дії формуються на основі сценарного планування та узгоджуються через систему індикаторів стану інфраструктури. Запроваджено механізм адаптації управлінських процесів до змін середовища, який забезпечує переналаштування функцій і процедур залежно від рівня загроз, що підвищує стабільність функціонування інфраструктурних систем. Розроблено управлінську архітектоніку інтеграції відбудови у систему державної політики та організаційно-управлінську модель функціонування системи публічного управління трансформацією об’єктів критичної інфраструктури. Сформовано інноваційний інструментарій публічного управління трансформацією об’єктів критичної інфраструктури, який функціонує через: 1) цифрові платформи моніторингу, 2) аналітичні модулі оцінювання стану об’єктів та 3) алгоритми підтримки управлінських рішень.

Набула подальшого розвитку система управлінських заходів відновлення об’єктів критичної інфраструктури у повоєнному періоді, яка функціонує через послідовну реалізацію етапів: 1) координації, 2) фінансування, 3) оцінювання стану та 4) контролю виконання робіт. Запроваджено механізм формування реєстру пошкоджених об’єктів, їх ранжування за рівнем критичності та визначення пріоритетів відбудови. Передбачено інтеграцію державних ресурсів, міжнародної допомоги та приватного сектору, а також організацію системи моніторингу якості виконання робіт, що забезпечує узгодженість відновлювальних процесів і скорочення строків відновлення інфраструктури.

Ключові слова: публічне управління, критична інфраструктура, трансформація інфраструктури, механізми державного управління, стійкість інфраструктури, безпека інфраструктурних систем, нормативно-правове забезпечення, інституційне забезпечення, кібербезпека інфраструктури, відновлення інфраструктури, цифровізація управління, міжнародний досвід управління.

ANNOTATION

Magomedov A. O. Conceptual Foundations of Public Management in the Field of Transformation of Critical Infrastructure Facilities. – *Manuscript.*

Dissertation for the degree of Doctor of Sciences in Public Administration, specialty 25.00.02 – Mechanisms of Public Administration. – National Aerospace University "Kharkiv Aviation Institute", Kharkiv, 2026.

The dissertation develops the conceptual foundations of public management in the field of transformation of critical infrastructure facilities in the context of contemporary security challenges, military threats and the post-war recovery of Ukraine.

The author examines the theoretical and methodological foundations of public management in the field of transformation of critical infrastructure facilities. The study analyses the current state of research on the topic, the conceptual and categorical framework, and the functions and specific features of critical infrastructure management. Approaches to classifying critical infrastructure facilities are generalised, and their role in ensuring the economic, social and national security of the state is defined.

Public management of critical infrastructure assets is defined as a complex, multi-level system through which management bodies (state authorities, authorised regulatory bodies and local government bodies) exert influence on critical infrastructure assets (energy, transport, utilities, information and other life-support systems), implemented through a range of analytical, preventive and organisational-management mechanisms, involving cooperation with infrastructure operators and

other stakeholders, and is aimed at ensuring the continuity of operation of critical systems, their resilience to threats and the protection of the vital interests of society and the state.

The regulatory and legal framework for critical infrastructure management in Ukraine is analysed, and directions for its adaptation to European standards are identified. A comprehensive mechanism for the public management of the transformation of critical infrastructure assets has been refined; unlike existing approaches, it is structured around the integration of functional, resource-based and information-based management frameworks, with the roles of stakeholders clearly defined at each stage of the transformation. The structure of the mechanism comprises: regulatory and legal, institutional, organisational and information, financial and economic, technological and digital mechanisms. Within the framework of the mechanism, the following interrelated blocks have been identified: (a) the strategic planning block, (b) the coordination block and (c) the operational response block. This structure enhances the coherence of decisions, reduces response times and ensures the system's adaptability to changes in the security environment.

The study analyses the international experience of EU member states, the United States, Canada, Israel and Australia in the management, protection and resilience of critical infrastructure. Promising directions for adapting foreign practices to Ukrainian realities are identified, in particular in interagency coordination, public-private partnership, cybersecurity and risk management. It is established that integrating European approaches to critical infrastructure protection will strengthen the state's resilience to contemporary security challenges.

The scientific approach to the classification of critical infrastructure assets, the mapping of interdependencies between different sectors of critical infrastructure in Ukraine, the identification of a threat matrix for critical infrastructure, and the characteristics of the elements of the management and protection system for critical infrastructure assets have been refined.

A conceptual model of interaction among management actors is developed, based on the principles of synergy, vertical accountability and target-oriented performance. The study also builds a system of indicators for assessing the

effectiveness of managing transformation processes, which covers the level of adaptability, digital maturity, resilience and speed of response to threats.

The study examines the damage and destruction of Ukraine's critical infrastructure facilities caused by armed aggression and identifies the main problems in reconstructing and modernising critical facilities. It establishes that Ukraine lacks a comprehensive system of strategic documents and mechanisms for restoring critical infrastructure. The study substantiates the use of the PMBOK project methodology, elements of the Agile approach and public-private partnership mechanisms for implementing post-war reconstruction programmes and restoring infrastructure facilities. The study formulates the Concept of Public Management of Change in Critical Infrastructure Facilities. Unlike known concepts, it combines strategic-planning, resource and institutional circuits of management. Within the Concept, management actions are formed on the basis of scenario planning and aligned through a system of infrastructure condition indicators. A mechanism for adapting management processes to environmental changes is introduced: it reconfigures functions and procedures depending on the level of threat, which makes infrastructure systems function more stably.

The study develops a managerial architectonics for integrating reconstruction into the system of state policy, as well as an organisational and managerial model of the system of public management of the transformation of critical infrastructure facilities. An innovative toolkit for public management of the transformation of critical infrastructure facilities is formed. It operates through: 1) digital monitoring platforms; 2) analytical modules for assessing the condition of facilities; and 3) algorithms supporting management decision-making.

The system of management measures for the restoration of critical infrastructure facilities in the post-war period has been further developed; it operates through the sequential implementation of the following stages: 1) coordination, 2) funding, 3) condition assessment, and 4) monitoring of work progress. A mechanism has been introduced for compiling a register of damaged facilities, ranking them by criticality and determining reconstruction priorities. Provision has been made for the integration of state resources, international aid and the private sector, as well as for the organisation

of a system to monitor the quality of work carried out, ensuring the coherence of reconstruction processes and reducing the time taken to restore infrastructure.

Keywords: public management, critical infrastructure, infrastructure transformation, mechanisms of public administration, infrastructure resilience, security of infrastructure systems, regulatory and legal framework, institutional support, infrastructure cybersecurity, infrastructure recovery, digitalisation of management, international management experience.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у фахових виданнях індексованих у міжнародній науково-метричній базі Scopus/Web of science:

1. Magomedov A., Ivanov A., Pron L., Trostianska K., Forkun I. Administrative oversight of critical infrastructure and social security protection. *AD ALTA: Journal Of Interdisciplinary Research (14/01-XLII.)* 2024, p. 16-20. URL: https://doi.org/10.5281/zenodo.11816980.

(Особистий внесок здобувача: обґрунтовано концептуальні засади публічного управління у сфері захисту критичної інфраструктури та соціальної безпеки).

2. Bohun V., Magomedov A., Hromyka O., Kovshun N., Fedorchuk Y. Assessing the Impact of Infrastructure Damage on National Investment Attractiveness During Martial Law. *Pakistan Journal of Life and Social Sciences,* 2024, 22(2), p.100379-100385. DOI: 10.57239/PJLSS-2024-22.2.00784.

(Особистий внесок здобувача: здійснено концептуалізацію дослідження впливу руйнування інфраструктури на інвестиційну привабливість України в умовах воєнного стану; сформовано методологічні підходи до оцінювання наслідків пошкодження критичної інфраструктури; проведено систематизацію та опрацювання даних, а також підготовлено й доопрацьовано текст статті).

3. Polovenko V., Magomedov A., Kravtsev O., Krasnostanova N., Kryzhanovskyi S. Regulatory and Institutional Frameworks for Ensuring Financial Security in Ukraine's Energy Sector: Challenges and Future Outlook. *Grassroots Journal of Natural Resources,* 2024, 7(3): s313-s330. DOI: https://doi.org/10.33002/nr2581.6853.0703ukr16.

(Особистий внесок здобувача: сформовано методологічний підхід дослідження, проведено порівняльний аналіз регуляторних та інституційних засад енергетичної безпеки).

Статті у фахових виданнях України категорії Б:

4. Магомедов А. Стратегічні документи і заходи повоєнної відбудови України. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2023. № 4. С. 61–75. DOI: https://doi.org/10.31470/2786-6246-2023-4-61-75.

5. Магомедов А.О. Зарубіжний досвід економічного відновлення після війни. *Наукові перспективи,* 2023, №11(41). С.252-263. DOI: https://doi.org/10.52058/2708-7530-2023-11(41)-252-265.

6. Магомедов А. О. Державне регулювання повоєнного відновлення економіки. *Електронне наукове видання "Публічне адміністрування та національна безпека".* 2023. №10. DOI: https://doi.org/10.25313/2617-572X-2023-10-9397.

7. Магомедов А. О. Фінансове забезпечення повоєнної відбудови та відновлення економіки: теоретичні засади. *Публічне управління: концепції, парадигма, розвиток, удосконалення,* 2023, №5. С.60-76. DOI: https://doi.org/10.31470/2786-6246-2023-5-60-76.

8. Магомедов А. О. Аналіз втрат та руйнувань інфраструктури України, що підлягає відновленню. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування*. 2023. № 6. С. 62-72. DOI: https://doi.org/10.32782/tnv-pub.2023.6.9.

9. Магомедов А. О. Оцінка економічних наслідків війни та втрат економіки України. *Актуальні питання у сучасній науці*. 2024. №1(19). С. 191-206. DOI: https://doi.org/10.52058/2786-6300-2024-1(19)-191-206.

10. Магомедов А. О. Механізм публічного управління розвитком об’єктів критичної інфраструктури: законодавчі, організаційні та управлінські виміри. *Державне управління: удосконалення та розвиток*. 2024. № 5. DOI: http://doi.org/10.32702/2307-2156.2024.5.12.

11. Магомедов А. О. Відбудова об’єктів критичної інфраструктури України після війни: стратегія та перспективи. *Економіка, фінанси, управління: Актуальні питання науки та практичної діяльності.* 2024. № 1. С. 100-116. DOI: 10.37128/2411-4413-2024-1-7.

12. Магомедов А. О. Публічне управління процесами трансформації критичної інфраструктури в країнах ЄС. *Успіхи і досягнення*. 2024. № 6. С. 520-537. DOI: https://doi.org/10.52058/3041-1254-2024-6(6)-520-537.

13. Магомедов А. О. Особливості публічного управління об’єктами критичної інфраструктури. *Наукові перспективи*. 2024. No 7(49). С. 412-427. DOI: https://doi.org/10.52058/2708-7530-2024-7(49)-412-427.

14. Магомедов А. О. Інновації в публічному управлінні сферою критичної інфраструктури. *Публічне адміністрування та національна безпека*. 2024. № 7. DOI: https://doi.org/10.25313/2617-572X-2024-7-10106.

15. Магомедов А. О. Ризики та загрози для об'єктів критичної інфраструктури та шляхи їх подолання. *Інвестиції: практика та досвід*. 2024. № 15. С. 216-221. DOI: 10.32702/2306-6814.2024.15.216.

16. Магомедов А. О. Стійкість об'єктів критичної інфраструктури в контексті публічного управління. *Modern Economics*. 2024. № 46. С.69-76. DOI: https://doi.org/10.31521/modecon.V46(2024)-10.

17. Магомедов А. О. Стратегічне управління трансформацією об’єктів критичної інфраструктури: організаційні та управлінські виклики та можливості. *Публічне управління і адміністрування в Україні*. 2024. № 41. С. 84-89. DOI: https://doi.org/10.32782/ pma2663-5240-2024.41.11

18. Магомедов А. О. Стратегічне планування повоєнної відбудови критичної інфраструкури України: еволюція підходів, фінансові розриви та цифрові інструменти. *Філософія та управління*, 2026, (3(19). DOI: https://doi.org/10.70651/3041-248X/2026.3.21.

19. Магомедов А. О. Стан, проблеми публічного управління та стратегічні пріоритети відновлення критичної інфраструктури України (2022–2025). *Філософія та управління*, 2026, (4(20). DOI: https://doi.org/10.70651/3041-248X/2026.4.07.

20. Магомедов А. О. Корпоратизація державних підприємств критичної інфраструктури України: інституційні проблеми та міжнародні уроки. *Публічне управління і політика*, 2026, (4(20). DOI: https://doi.org/10.70651/3041-2498/2026.4.20.

21. Magomedov A. Legal and regulatory framework of public management of the security and transformation of critical infrastructure facilities in modern conditions. *Public Management and Policy*. 2026. № 6(22). DOI: https://doi.org/10.70651/3041-2498/2026.6.03.

22. Magomedov A. Innovative public management tools for ensuring the resilience and transformation of critical infrastructure facilities amidst modern challenges. *Philosophy and Governance*. 2026. № 6(22). DOI: https://doi.org/10.70651/3041-248X/2026.6.03.

Публікації, що засвідчують апробацію результатів дисертації:

23. Магомедов А. О. Вплив трансформації об'єктів критичної інфраструктури на економіку та соціальні процеси. *ІІ науково-практичній конференції "Комплексний підхід до модернізації міждисциплінарних наукових досліджень", м. Дніпро, 24–25 травня 2024 року.* URL: https://molodyivchenyi.ua/omp/index.php/conference/catalog/view/86/1420/2954-1.

24. Магомедов А. О. Порівняльний аналіз стратегій та політик ЄС та інших країн у сфері публічного управління об’єктами критичної інфраструктури. *Міжнародна наукова конференція «Сучасні тенденції наукових досліджень у світі» 30–31 травня 2024 року м. Рига, Латвійська Республіка.* URL: http://www.baltijapublishing.lv/omp/index.php/bp/catalog/view/478/12795/26738-1.

25. Магомедов А. О. Трансформація об'єктів критичної інфраструктури у системі публічного управління. *VI International Scientific and Theoretical Conference «Current issues of science, prospects and challenges» 17.05, Сідней, Австралія. 2024.* URL: https://previous.scientia.report/index.php/archive/issue/view/17.05.2024.

26. Магомедов А. О. Роль інформаційних технологій у підвищенні ефективності публічного управління трансформацією об'єктів критичної інфраструктури. *І Всеукраїнській науково-практичній конференції за міжнародною участю “Публічне управління та адміністрування в Україні: євроінтеграційний поступ» 31 травня 2024.* URL: https://nung.edu.ua/sites/default/files/2024-

07/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA_%D1%82%D0%B5%D0%B7_%D0%86%D0%A4%D0%9D%D0%A2%D0%A3%D0%9D%D0%93_2024.pdf.

27. Магомедов А. О. Інноваційні підходи до забезпечення безпеки та стійкості об'єктів критичної інфраструктури. *III Міжнародної наукової конференції Наукові орієнтири: теорія та практика досліджень, 17 травня 2024, Ужгород, Україна.* 2024. С. 54-56. URL: https://archive.mcnd.org.ua/index.php/conference-proceeding/issue/view/17.05.2024/65.

ЗМІСТ

ПЕРЕЛІК УМОВАНИХ СКОРОЧЕНЬ……... 17
ВСТУП……... 20
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ТРАНСФОРМАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ…… 32
1.1. Понятійно-категорійний апарат та структуризація об'єктів критичної інфраструктури……. 32
1.2. Стан наукової розробки проблематики публічного управління у сфері трансформації об'єктів критичної інфраструктури……... 44
1.3. Основні функції та особливості управління об'єктами критичної інфраструктури……. 56
1.4. Нормативно-правове забезпечення публічного управління у сфері трансформації об'єктів критичної інфраструктури……... 71
Висновки до розділу 1…….. 91
РОЗДІЛ 2. МЕХАНІЗМИ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ТРАНСФОРМАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ…… 94
2.1. Структура та види механізмів публічного управління у сфері трансформації об'єктів критичної інфраструктури..…..…… 94
2.2. Процеси та складові публічного управління захисту, безпеки, стійкості та трансформації об'єктів критичної інфраструктури в сучасних умовах…… 120
2.3. Інституційне та організаційно-інформаційне забезпечення публічного управління у сфері трансформації об'єктів критичної інфраструктури……. 133
Висновки до розділу 2…….. 154
РОЗДІЛ 3. МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ, ЗАХИСТУ ТА БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ЗАРУБІЖНИЙ ДОСВІД……. 157

3.1. Досвід держав-членів ЄС щодо публічного управління у сфері трансформації об’єктів критичної інфраструктури…….. 157
3.2. Реалізація загальної системи управління та захисту об’єктів критичної інфраструктури в ЄС…….. 170
3.3. Практика управління та захисту критичної інфраструктури США та Канади…… 179
3.4. Міжнародний досвід забезпечення кібербезпеки критичної інфраструктури……. 192
Висновки до розділу 3…….. 201
РОЗДІЛ 4. ЕФЕКТИВНІСТЬ ПУБЛІЧНОГО УПРАВЛІННЯ ТРАНСФОРМАЦІЄЮ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВІЙСЬКОВОГО СТАНУ ТА ЇЇ ВІДНОВЛЕННЯ В ПОВОЄННОМУ ПЕРІОДІ……. 204
4.1. Стан пошкодження та руйнувань об’єктів критичної інфраструктури у період війни…… 204
4.2. Ефективність публічного управління об'єктами критичної інфраструктури в Україні……. 220
4.3. Стратегічні документи щодо відбудови об’єктів критичної інфраструктури України після війни……... 231
4.4. Механізми організації відбудови об’єктів критичної інфраструктури України в повоєнному періоді……. 242
Висновки до розділу 4…… 265
РОЗДІЛ 5. УДОСКОНАЛЕННЯ КОНЦЕПТУАЛЬНИХ ЗАСАД ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ТРАНСФОРМАЦІЇ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ…… 267
5.1. Концепція публічного управління у сфері трансформації об’єктів критичної інфраструктури……... 267
5.2. Інноваційні інструменти публічного управління у сфері трансформації об’єктів критичної інфраструктури……... 300
5.3. Перспективи відновлення об’єктів критичної інфраструктури в Україні (у т. ч. на деокупованих територіях)…… 323

Висновки до розділу 5…….. 340
ВИСНОВКИ…….. 344
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……. 351
ДОДАТКИ……..... 396

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ДПП – Державно-приватне партнерство

ЄКІ – Європейська критична інфраструктура

ЄС – Європейський Союз

ЗМІ – Засоби масової інформації

ЗУ – Закон України

ІКТ – Інформаційно-комунікаційні технології

ІТ – Інформаційні технології

КабМін / КМУ – Кабінет Міністрів України

КІ – Критична інфраструктура

Мінекономіки – Міністерство економіки України

Міненерго – Міністерство енергетики України

Мінінфраструктури – Міністерство розвитку громад, територій та інфраструктури України

Мінстратегпром – Міністерство з питань стратегічних галузей промисловості України

Мінфін – Міністерство фінансів України

Мінцифри – Міністерство цифрової трансформації України

МВС – Міністерство внутрішніх справ

МОЗ – Міністерство охорони здоров'я України

МСЕК – Медико-соціальна експертна комісія

НАТО – Організація Північноатлантичного договору

НКЦПФР – Національна комісія з цінних паперів та фондового ринку

НСЗУ – Національна служба здоров'я України

ОЕСР – Організація економічного співробітництва та розвитку

ОТ – Операційні технології

ППП – Публічно-приватне партнерство

РНБО – Рада національної безпеки і оборони України

США – Сполучені Штати Америки

AESCSF – Australian Energy Sector Cyber Security Framework

CFR – Code of Federal Regulations

CII Act – Critical Infrastructure Information Act

CIKR – Critical Infrastructure and Key Resources

CIRMP – The Critical Infrastructure Risk Management Program

CISA – Cybersecurity and Infrastructure Security Agency

CIWIN – Critical Infrastructure Warning Information Network

CPRs – Commonwealth Procurement Rules

CRPG – The Commonwealth Regulator Performance Guide

CSIRO – The Commonwealth Scientific and Industrial Research Organisation

DAFNI – Data & Analytics Facility for National Infrastructure

DCS – Distributed control system

DEMA – Danish Emergency Management Agency

DHS – United States Department of Homeland Security

DMZ / DZ – Demilitarized zone

EAM – Enterprise asset management

ECI – European critical infrastructure

ENISA – The European Union Agency for Cybersecurity

ENTSO-E – European Network of Transmission System Operators for Electricity

EPCIP – European Programme for Critical Infrastructure Protection

ERNCIP – European Reference Network for Critical Infrastructure Protection

Hamas – The Islamic Resistance Movement, abbreviated

HMI – Human-machine interface

IDS/IPS – Intrusion Detection System / Intrusion Prevention System

IT – Information Technology

JRC – Joint Research Centre

NCI – Securing National Critical Infrastructure

NCTV – Dutch Nationaal Coördinator Terrorismebestrijding en Veiligheid

NIPP – National Infrastructure Protection Plan and Resources

NIS – Network and Information Security

PCII – Protected Critical Infrastructure Information Program

PGPA – The Public Governance, Performance and Accountability Rule

PPL – Protection of Privacy Law

RTU – Remote terminal unit

SCADA – Supervisory Control i Data Acquisition

SERTIT – Norwegian National Security Authority

SGDSN – Secretariat-General for National Defence and Security

SOCI – Security of Critical Infrastructure Act

USA / U.S. – The United States of America

7amleh - Arab Center for Social Media Advancement

ВСТУП

Актуальність теми. Забезпечення стійкості критичної інфраструктури держави в умовах війни, макроекономічної нестабільності та технологічних загроз належить до базових пріоритетів публічного управління. Функціонування енергетичних систем, транспортних мереж, цифрових платформ і систем життєзабезпечення визначає спроможність держави виконувати основні функції та підтримувати соціально-економічну рівновагу. Трансформаційні процеси, посилені руйнуванням інфраструктурних об’єктів, спричинили загострення системних ризиків, порушення логістичних зв’язків і зниження ефективності управління. Зафіксовано дефіцит енергетичних потужностей, пошкодження транспортних вузлів, збільшення навантаження на цифрові системи та ускладнення доступу до базових ресурсів. Така ситуація вимагає оновлення підходів до публічного управління та формування нових інструментів трансформації інфраструктури. Фрагментарність нормативно-правового забезпечення, недостатній рівень координації між органами влади, обмежений аналітичний інструментарій і слабка інтеграція інформаційних систем формують комплекс проблем, що знижують результативність державної політики у сфері критичної інфраструктури. За кризових умов органи публічної влади концентрують увагу на питаннях безпеки та відновлення інфраструктурних систем. Пріоритетом виступає формування ефективних механізмів реагування на загрози та забезпечення безперервності функціонування інфраструктури. Подібна логіка актуалізує потребу теоретичного й прикладного аналізу публічного управління трансформацією критичної інфраструктури в Україні.

Наукова проблема дослідження пов’язана з концептуальною невизначеністю змісту публічного управління трансформацією об’єктів критичної інфраструктури. Відсутня інтегрована модель управління, яка враховує взаємозв’язок між секторами інфраструктури та забезпечує координацію управлінських дій. Спостерігається дефіцит системних підходів до формування механізмів трансформації, а також недостатній рівень операціоналізації інструментів управління ризиками на різних рівнях. Попри

значний обсяг наукових досліджень у сфері безпеки та інфраструктури, інтегроване публічне управління трансформаційними процесами не отримало завершеного теоретичного обґрунтування. Наявні моделі взаємодії державних інституцій не відповідають масштабам сучасних викликів. Забезпечення стійкості інфраструктури виступає ключовим завданням системи публічного управління. Показники її функціонування відображають ефективність управлінських рішень і рівень адаптації до зовнішніх впливів. Інфраструктурна безпека входить до структури державної політики безпеки та визначає здатність держави протидіяти внутрішнім і зовнішнім загрозам. Актуальність дослідження зумовлена потребою формування цілісної системи публічного управління трансформацією критичної інфраструктури, яка забезпечує контроль ризиків і стратегічну адаптивність у воєнний та повоєнний періоди.

Окреслена проблема отримала розвиток у наукових дослідженнях з державного управління, економіки та безпеки.

У межах першого напряму, що охоплює дослідження сутності та структури критичної інфраструктури, слід виділити праці О. Азаренка, А. Балана, Д. Бірюкова, С. Бєлая, Д. Бобра, Б. Богдана, Д. Бондаря, Т. Бубели, О. Возненко, А. Гаврися, О. Герасименка, Ю. Гончаренка, М. Дівізінюка, М. Домарацького, О. Єрменчука, В. Євсєєва, О. Іваницької, А. Лелеченко, М. Мельника, О. Мельникової, М. Мельниченка, В. Мирненка, О. Назаровця, Н. Нєми, А. Помази-Пономаренко, Ю. Рудика, С. Сідлярук, В. Стрільця, Н. Тур, В. Філіппової та ін. У зазначених роботах розглядаються підходи до класифікації інфраструктурних об'єктів, визначення їх функціональних характеристик і оцінювання рівня стійкості.

Другий напрям досліджень пов'язаний із аналізом механізмів публічного управління та інституційного забезпечення функціонування інфраструктури. У цій площині виокремлюються праці Р. Бердибаєва, З. Бурик, Н. Вишневської, С. Гнатюка, С. Гончара, С. Домбровської, О. Жигаревича, О. Зарицького, С. Зибіна, С. Казьмірука, Н. Карпеко, К. Клименка, В. Ковальчук, О. Корченка, В. Круглова, О. Крюкова, Ю. Кузьменка, О. Лазора, А. Лелеченко, Б. Леонова,

С. Майстра, О. Мельничука, П. Махортова, В. Мохора, О. Поступної, М. Савостьяненка, В. Сидоренка, Т. Смірнової, Н. Трушкіної, О. Омельяна, В. Шведун, І. Юник та ін. Дослідження цих авторів спрямовані на визначення структури управлінських механізмів, аналіз їх функціонування й оцінку ефективності інституційної взаємодії.

Третій напрям охоплює дослідження безпеки, стійкості та відновлення інфраструктурних систем. У цьому контексті важливими є роботи В. Баштанника, В. Косика, О. Лесика, К. Лук'янчука, Д. Мальчикової, В. Микитенка, М. Миколайчука, Н. Мороз, П. Остапенка, І. Пилипенка, І. Самарченка, Г. Ситника, а також зарубіжних дослідників L. Wansleben, W. Allen, G. Wood, C. Wenjie, M. Miko, N. Malhar, H. Eckhard, D. Detzer, N. Dodig, A. Hameeda, R. Jabeen, S. A. Shah, M. Mihut, P. Werthers, L. Guo, F. Lee, J. Wei, P. Pardo. У зазначених працях аналізуються питання кібербезпеки, управління ризиками, відновлення інфраструктури та розвитку партнерських механізмів.

Аналіз наукових джерел засвідчив фрагментарність досліджень і відсутність інтегрованого підходу до публічного управління трансформацією критичної інфраструктури. Наукові праці концентруються на окремих аспектах функціонування систем, що не дозволяє сформувати цілісну модель управління. Теоретичне обґрунтування механізмів трансформації залишається неповним. Актуальним завданням виступає комплексний аналіз публічного управління, інструментів трансформації та структури взаємодії між суб’єктами управління.

Зв’язок роботи з науковими програмами, планами, темами. Дослідження виконувалося в рамках науково-дослідних робіт: «Теоретико-методологічні засади реформування системи державного управління в Україні» (номер державної реєстрації: 0121U107430), «Цифровізація публічного управління як виклики та перспективи забезпечення національній безпеці України» (номер державної реєстрації: 0123U100291) виконані відповідно до наукових тем Університету Григорія Сковороди в Переяславі. Внесок автора полягає в обґрунтуванні теоретичних, нормативно-правових, організаційних, методичних і прикладних засад реформування та удосконалення механізмів

публічного управління у сфері трансформації об’єктів критичної інфраструктури. В науковому длслідженні використано науковий підхід до імплементації міжнародного досвіду забезпечення кібербезпеки критичної інфраструктури.

Мета і завдання дослідження. *Метою* дослідження є обґрунтування комплексу концептуальних положень та формування практичних рекомендацій щодо удосконалення публічного управління у сфері трансформації об'єктів критичної інфраструктури. Відповідно до мети визначено такі *завдання* дослідження:

– вивчити стан наукової розробки проблематики та ключові концепції публічного управління у сфері трансформації об’єктів критичної інфраструктури;

– обґрунтувати функції та вивчити загрози публічного управління у сфері трансформації об’єктів критичної інфраструктури та розкрити їх змістові особливості;

– сформувати комплексний механізм публічного управління трансформацією об’єктів критичної інфраструктури України;

– узагальнити пропозиції щодо доповнення нормативно-правового забезпечення функціонування захисту, безпеки, стійкості та трансформації об’єктів критичної інфраструктури в сучасних умовах;

– розробити організаційно-управлінську модель функціонування системи публічного управління трансформацією об’єктів критичної інфраструктури;

– дослідити та запропонувати маркери імплементації міжнародного досвіду забезпечення кібербезпеки критичної інфраструктури;

– запропонувати класифікаційні ознаки оцінювання стану пошкодження та руйнувань об’єктів критичної інфраструктури у період воєнного стану;

– розробити методичний підхід до оцінювання рівня ефективності публічного управління об’єктами критичної інфраструктури в Україні;

– обґрунтувати Концепцію публічного управління у сфері змін об’єктів критичної інфраструктури;

– розробити інноваційний інструментарій публічного управління трансформацією об’єктів критичної інфраструктури;

– обґрунтувати заходи публічного управління по відновленню об’єктів критичної інфраструктури України у повоєнному періоді.

Об’єктом дослідження є суспільно-владні відносини, що виникають у процесі функціонування та трансформації об’єктів критичної інфраструктури.

Предметом дослідження є процеси публічного управління трансформацією об’єктів критичної інфраструктури, їх механізми, інструменти та організаційно-економічні засади функціонування.

Методи дослідження. Для досягнення поставленої мети у дисертаційній роботі використано сукупність сучасних загальнонаукових, спеціальних та прикладних методів, що забезпечили комплексне дослідження механізмів публічного управління у сфері трансформації об’єктів критичної інфраструктури та створили підґрунтя для формування обґрунтованих управлінських рішень. Добір методичного інструментарію здійснено з урахуванням багаторівневості інфраструктурних систем, міжсекторального характеру їх функціонування та зростання ризиків у воєнний і повоєнний періоди. *Комплексний аналіз* забезпечив виявлення системних дисфункцій у функціонуванні механізмів публічного управління трансформацією критичної інфраструктури. У межах цього підходу досліджено нормативно-правові, організаційні, фінансово-економічні та інформаційні компоненти діяльності органів публічної влади. *Системний аналіз* використано для розгляду критичної інфраструктури як інтегрованої багаторівневої системи, що поєднує функціональні, інституційні та технологічні елементи. У межах цього підходу визначено взаємозалежності між секторами інфраструктури, встановлено критичні точки вразливості та ідентифіковано фактори впливу на їх стійкість. На цій основі сформовано функціональну модель публічного управління трансформацією інфраструктурних об’єктів, яка враховує багаторівневу структуру управлінських процесів. *Концептуальний аналіз* спрямовано на формування нових теоретичних положень щодо публічного управління трансформацією критичної інфраструктури. У межах цього підходу обґрунтовано авторське бачення концепції управління, визначено її принципи,

функції та стратегічні орієнтири. *Структурно-функціональний метод* забезпечив побудову моделі механізмів публічного управління трансформацією об’єктів критичної інфраструктури з урахуванням функціонального навантаження кожного суб’єкта. У процесі аналізу визначено ефективність діяльності органів державної влади, уточнено розподіл повноважень та обґрунтовано напрями оптимізації інституційної структури управління. *Методи узагальнення та систематизації* застосовано для формування понятійно-категорійного апарату дослідження. Уточнено зміст базових дефініцій, проведено класифікацію об’єктів критичної інфраструктури та систематизовано підходи до їх оцінювання. У межах цього підходу визначено структурні компоненти інфраструктури та їх функціональні характеристики. *Порівняльний метод* використано для аналізу міжнародного досвіду управління критичною інфраструктурою. Досліджено підходи країн Європейського Союзу, США та Канади до організації управлінських процесів, визначено ефективні інструменти та моделі, придатні для адаптації в Україні. Зіставлення різних моделей дозволило виявити спільні закономірності та визначити напрями вдосконалення національної системи управління. *Економіко-математичні методи* застосовано для оцінювання ефективності публічного управління трансформацією інфраструктурних систем. *Контент-аналіз і формально-логічний аналіз* застосовано для дослідження нормативно-правових актів, стратегічних документів та міжнародних стандартів у сфері критичної інфраструктури. У межах цього підходу виявлено колізії, прогалини та напрями вдосконалення регуляторного середовища. *Методи прогнозування та сценарного аналізу* застосовано для моделювання розвитку інфраструктурних систем у повоєнний період. Побудовано альтернативні сценарії трансформації інфраструктури з урахуванням різних рівнів ресурсного забезпечення, безпекових ризиків та управлінських рішень.

Наукова новизна одержаних результатів полягає в розв’язанні важливої наукової проблеми в галузі державного управління, а саме – обґрунтування комплексу концептуальних положень та формування практичних рекомендацій щодо удосконалення публічного управління у сфері трансформації об'єктів критичної інфраструктури. Наукова новизна визначається такими положеннями:

уперше:

– сформовано концепцію публічного управління змінами об’єктів критичної інфраструктури, яка на відміну від відомих, працює через поєднання стратегічно-планувального, ресурсного та інституційного контурів управління. У межах концепції управлінські дії формуються на основі сценарного планування та узгоджуються через систему індикаторів стану інфраструктури, через механізм адаптації управлінських процесів до змін середовища, який забезпечує переналаштування функцій і процедур залежно від рівня загроз, що підвищує стабільність функціонування інфраструктурних систем;

– розроблено управлінську архітектоніку інтеграції відбудови у систему державної політики та організаційно-управлінську модель функціонування системи публічного управління трансформацією об’єктів критичної інфраструктури через поетапне проходження управлінських процесів від стратегічного планування до операційного реагування, що забезпечує узгоджене функціонування системи та підвищує її стійкість до дестабілізуючих впливів, що на противагу до існуючих моделей може функціонувати, як інтегрована система багатоаспектної взаємодії органів державної влади з поєднанням вертикальної і горизонтальної координації, розподілу функцій та спільного використання ресурсів;

– сформовано інноваційний інструментарій публічного управління трансформацією об’єктів критичної інфраструктури, що функціонує через 1) цифрові платформи моніторингу, 2) аналітичні модулі оцінювання стану об’єктів та 3) алгоритми підтримки управлінських рішень та за допомогою якого забезпечується збір і обробка інформації про стан інфраструктури, формування аналітичних сигналів та передачу їх суб’єктам управління та застосування якого передбачає використання прогнозних моделей для визначення сценаріїв розвитку і вибору оптимальних управлінських дій, що знижує ризики прийняття неузгоджених рішень;

удосконалено:

– науковий підхід до класифікації об’єктів критичної інфраструктури, формування мережі взаємозалежностей між різними секторами критичної

інфраструктури в Україні, визначення матриці загроз критичній інфраструктурі, характеристики елементів системи управління та захисту об’єктів критичної інфраструктури, та визначення функцій публічного управління в питанні перетворень об’єктів критичної інфраструктури, який, на відміну від відомих, структурований через виокремлення стратегічного, адаптивного, координаційного та безпекового функціональних блоків;

– комплексний механізм публічного управління трансформацією об’єктів критичної інфраструктури, який, на відміну від наявних підходів, структуровано за принципом інтеграції функціональних, ресурсних та інформаційних контурів управління з чітким закріпленням ролей суб’єктів на кожному етапі трансформації і до структури якого належать: нормативно-правовий, інституційний, організаційно-інформаційний, фінансово-економічний, технологічний та цифровий механізми через виділення взаємопов’язаних блоків: а) стратегічного планування, б) координації та в) операційного реагування, що підвищує узгодженість рішень, скорочує втрати часу на реагування та забезпечує адаптацію системи до змін безпекового середовища;

– організаційний підхід до класифікації стану пошкодження та руйнувань об’єктів критичної інфраструктури у період воєнного стану, що враховує функціональні втрати, глибину структурних пошкоджень та час, який необхідний для відновлення об’єкта КІ, шляхом запропонованої диференціації об’єктів за ступенем критичності, порушень і масштабом впливу на суміжні сектори через визначену логіку оцінювання з урахуванням каскадних ефектів і просторових особливостей руйнувань, що забезпечує підвищення обґрунтованості державних рішень для очікуваного відновлення критичної інфраструктури України;

– методичний підхід до оцінювання рівня ефективності публічного управління об’єктами критичної інфраструктури, у межах якого введено оцінювання узгодженості управлінських рішень, швидкості реагування на загрози та здатності системи до відновлення функціонування, передбачено формування інтегрального показника на основі нормованих даних та вагових

коефіцієнтів, що дозволяє визначати вплив окремих управлінських компонентів на кінцевий результат; який, на противагу до вже реалізованих, побудований на поєднанні результативних, процесних та інституційних індикаторів із їх диференціацією за рівнями управління;

– формування правового базису забезпечення захисту, безпеки, стійкості та трансформації об'єктів критичної інфраструктури та визначення пріоритетних напрямків удосконалення правового забезпечення публічного управління об'єктами критичної інфраструктури шляхом оновлення оцінок ризиків з урахуванням поточних загроз для об'єктів КІ, проведення стрес-тестів у ключових секторах, розробки національного плану реагування на значні інциденти в критичній інфраструктурі, посилення міжнародного співробітництва з питань безпеки критичної інфраструктури, залучення до європейських дослідницьких програм із безпеки критичної інфраструктури, формування єдиного управлінського механізму щодо захисту критичної інфраструктури;

набули подальшого розвитку:

– категоріально-понятійний апарат теорії публічного управління у частині фундаментальних дефініцій «*критична інфраструктура», «трансформація об'єктів критичної інфраструктури», «публічне управління у сфері трансформації критичної інфраструктури»*, шляхом систематизації та переосмислення існуючих наукових підходів, уточнення змістових характеристик і логіко-структурної побудови відповідних категорій, подальшого розвитку набули: а) відмежування поняття «критична інфраструктура» від суміжних категорій базової інфраструктури, стратегічних активів та систем життєзабезпечення; б) структуризація взаємозв'язків між секторами інфраструктури з урахуванням міжсекторальних залежностей і каскадних ефектів; в) концептуальне розкриття взаємодії державних інституцій, операторів інфраструктури та суспільства у процесі функціонування та трансформації інфраструктурних систем;

– науковий підхід до імплементації міжнародного досвіду забезпечення кібербезпеки критичної інфраструктури, шляхом виділення системи маркерів

імплементації, що охоплюють інституційні, технологічні та процедурні параметри адаптації, запропоновано їх структуру, яка включає рівень готовності нормативного середовища, ступінь інтеграції цифрових платформ, наявність механізмів обміну інформацією та швидкості реагування на кіберзагрози, здійснено прив'язку маркерів до етапів впровадження міжнародних практик і до рівнів управління, що підвищує точність оцінювання результативності імплементаційних процесів та узгодженість управлінських дій;

– система управлінських заходів відновлення об'єктів критичної інфраструктури у повоєнному періоді, яка функціонує через послідовну реалізацію етапів: 1) координації, 2) фінансування, 3) оцінювання стану та 4) контролю виконання робіт шляхом запровадження механізму формування реєстру пошкоджених об'єктів, їх ранжування за рівнем критичності та визначення пріоритетів відбудови та передбачення інтеграції державних ресурсів, міжнародної допомоги та приватного сектору, а також організацію системи моніторингу якості виконання робіт, що забезпечує узгодженість відновлювальних процесів і скорочення строків відновлення об'єктів КІ.

Практичне значення дослідження. Практична цінність отриманих результатів полягає у поглибленні теоретико-методичних засад аналізу системи публічного управління трансформацією об'єктів критичної інфраструктури та у розробленні прикладних інструментів її вдосконалення. У роботі сформовано рекомендації, спрямовані на підвищення ефективності рішень влади у процесі відновлення, модернізації та забезпечення стійкості інфраструктурних систем. Запропоновані підходи орієнтовані на оптимізацію взаємодії між органами державної влади, суб'єктами господарювання та інституціями, відповідальними за функціонування критичної інфраструктури. Результати дослідження можуть застосовуватися у практичній діяльності органів публічної влади під час формування державної політики у сфері відбудови інфраструктури, розроблення стратегічних програм розвитку та впровадження механізмів управління ризиками. Сформовані у роботі моделі та інструменти направлені на підвищення рівня обґрунтованості державних рішень, та забезпечення узгодженості дій суб'єктів публічного управління були використані у діяльності:

Департаменту житлово-комунального господарства та енергоефективності Київської обласної військової адміністрації – під час підготовки пропозицій щодо концептуальної логіки становлення інтегрованої системи публічного управління трансформацією критичної інфраструктури. (довідка про впровадження від 16.06.2026 р. № 7327/35/2026);

Бориспільської районної державної (військової) адміністрації Київської області – для вдосконалення організаційно-управлінського забезпечення трансформаційних процесів у сфері відновлення критичної інфраструктури. У діяльності адміністрації застосовано напрацювання дисертанта щодо функціональних блоків такого забезпечення: інфраструктурно-облікового, міжвідомчо-координаційного, аналітично-прогностичного, ресурсно-забезпечувального та інформаційно-аналітичного (довідка про впровадження від 21.04.2026 р. № 12-10/21-д);

Університету Григорія Сковороди в Переяславі – впроваджені в освітній процес і науково-методичну діяльність кафедри публічного управління та адміністрування Університету Григорія Сковороди в Переяславі й використовуються під час викладання дисциплін: «Теорія і практика реформ» та «Управлінський контроль в публічній сфері», а також під час оновлення робочих програм навчальних дисциплін і навчально-методичних комплексів. (довідка про впровадження від 08.06.2026 р. № 647);

Громадської організації «Східно-Європейська спілка науковців» – під час обговорення громадських ініціатив щодо соціально-економічних трансформацій в умовах війни та в повоєнний період, використано обґрунтовані дисертантом принципи механізму публічного управління відновленням критичної інфраструктури (довідка про впровадження від 04.04.2026 р. № 08/2026).

Особистий внесок здобувача полягає у самостійному формуванні теоретичних положень, розробленні методичних підходів та обґрунтуванні практичних рекомендацій щодо вдосконалення публічного управління трансформацією об’єктів критичної інфраструктури. Усі результати дослідження отримано автором самостійно та мають наукову новизну і прикладну

спрямованість. Запропоновані рішення базуються на власних аналітичних напрацюваннях і логічно інтегровані у структуру дисертаційної роботи.

Апробація результатів дисертації. Основні положення і результати дисертаційного дослідження розглянуто та схвалено на міжнародних та всеукраїнських науково-практичних конференціях, серед яких, зокрема: VI International Scientific and Theoretical Conference «Current Issues of Science, Prospects and Challenges» (17 травня 2024 р., м. Сідней, Австралія); III Міжнародна наукова конференція «Наукові орієнтири: теорія та практика досліджень» (17 травня 2024 р., м. Ужгород); II науково-практична конференція «Комплексний підхід до модернізації міждисциплінарних наукових досліджень» (24–25 травня 2024 р., м. Дніпро); Міжнародна наукова конференція «Сучасні тенденції наукових досліджень у світі» (30–31 травня 2024 р., м. Рига, Латвійська Республіка); I Всеукраїнська науково-практична конференція за міжнародною участю «Публічне управління та адміністрування в Україні: євроінтеграційний поступ» (31 травня 2024 р., м. Івано-Франківськ). Також апробація результатів дослідження здійснювалася шляхом їх представлення на фахових семінарах та наукових форумах. Обговорення отриманих результатів у професійному середовищі забезпечило їх наукову верифікацію, підтвердило практичну значущість і сприяло уточненню окремих положень дослідження.

Публікації. За темою дисертації опубліковано 27 наукових праць, зокрема: 19 статей у фахових наукових виданнях з державного управління, 3 статті у наукових періодичних виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus, а також 5 тез доповідей на наукових конференціях за участю дисертанта.

Структура та обсяг роботи. Дисертація викладена на 415 стор. друкарського тексту, з них обсяг основного тексту 350 стор.; містить 32 таблиці, 44 рисунки, 5 додатків. Текст складається із вступу, п’яти розділів, висновків, списку використаних джерел. Бібліографія включає 376 джерел, із них: зарубіжних – 251 джерело.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ТРАНСФОРМАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Понятійно-категорійний апарат та структуризація об'єктів критичної інфраструктури

В умовах зростаючих глобальних загроз та складної економічної ситуації питання захисту та управління критичною інфраструктурою стає все більш актуальним для національної безпеки кожної держави. Критична інфраструктура охоплює системи та об'єкти, порушення роботи яких може призвести до значних економічних, соціальних та екологічних наслідків, включаючи загрози життю і здоров'ю громадян. Р. Вудкевич (R. Wódkiewicz) [368] на прикладі президентської адміністрації США наголошує на тому, що певні компоненти національної інфраструктури мають настільки фундаментальне значення, що їхня деградація або знищення здатні поставити під загрозу оборонний потенціал і економічну стабільність країни. Натомість Б. Т. Бенет (B. T. Bennett) [127] підходить до питання захисту критичної інфраструктури з різних перспектив, зазначаючи, що ще в античності значення мали не лише захисні функції, а й безперервне покращення та зміцнення таких елементів реальності, які зараз розглядаються як критично важливі для держави. У даному контексті Р. Врубель (R. Wróbel) [369] акцентує увагу на тому, що надійне функціонування критичної інфраструктури забезпечує суспільству не лише задоволення базових потреб у безпеці, але й створює передумови для сталого розвитку та забезпечення високого рівня життєвого комфорту як для окремих громадян, так і для суспільних груп.

Більш сучасні автори, зокрема В. МакОлі (W. McAuley), Е. Аксельсдоттір, Р. Джонасон Бйоренстам (E. Axelsdóttir, R. Jonason Bjärenstam) [264; 141] та інші, відзначають критичну інфраструктуру як комплекс важливих об'єктів та систем, що забезпечують основні суспільні функції (VSF), які є життєво необхідними для стабільності та безпеки держави. На думку Г. Пескаролі та Д. Александер

(G. Pescaroli, D. Alexander) [292] вона має особливе значення через підвищену вразливість до численних загроз і каскадних ефектів, що можуть порушити функціонування взаємопов'язаних інфраструктурних елементів. У даному контексті К. Барке, М. Енглунд, К. Інга, К. Андре та Л. Сегнестам (K. Barquet, M. Englund, K. Inga, K. André, L. Segnestam) [125] досліджуються підходи до оцінки та управління ризиками для КІ як в академічній літературі, так і на практиці, зокрема у випадку Швеції, яка розглядається як приклад для аналізу та узагальнення ефективних методів забезпечення стабільності таких об'єктів на загальнонаціональному рівні.

І. Жукова, Н. Трушкіна, В. В. Мохор, С. Ф. Гончар та Д. С. Бірюков [6; 31; 63] зазначають, що надзвичайно актуальним для об’єктів критичної інфраструктури, особливо в енергетичному секторі, є забезпечення стійкості та готовності до протидії множинним загрозам; а процес її захисту вирізняється необхідністю координації між різними секторами та запровадженням ефективних систем управління ризиками.

Якщо говорити про трактування даного поняття у різних країнах або географічних регіонах, то воно є варіативним з огляду на різні геополітичні, сейсмічні або кліматичні умови, а також техногенні, кібернетичні та природні ризики. Дефініційна різноманітність у підходах до формування категорій критичної інфраструктури зумовлена необхідністю всебічного врахування ключових аспектів суспільного функціонування, зокрема енергетичної стабільності, безперервності транспортних мереж, кібербезпеки, захисту водних і продовольчих ресурсів. Так, згідно Закону України «Про критичну інфраструктуру» № 1882-IX від 21 вересня 2024 р. [83], об’єктами критичної інфраструктури є об’єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам. Згідно до ст. 6 іншого Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 28 червня 2024 р. [84] об'єкти критичної інфраструктури включають підприємства, установи та організації всіх форм власності, які забезпечують населення життєво

необхідними послугами, що передусім стосується таких галузей, як централізоване водопостачання, водовідведення, постачання електроенергії та природного газу, виробництво продуктів харчування, аграрний сектор, а також охорона здоров’я.

Натомість у польському законодавстві [358] до критичної інфраструктури відносять системи та функціонально пов'язані з ними об'єкти, у тому числі будівлі, пристрої, споруди, послуги, що мають вирішальне значення для безпеки держави та її громадян і слугують для забезпечення ефективного функціонування органів державної влади, а також установ та суб'єктів підприємницької діяльності. Також згідно до зазначеного документу до критичної інфраструктури належать підприємства, що забезпечують енергопостачання, безперебійне функціонування громадського транспорту, а також ті, чия діяльність, пов'язана з виробництвом, зберіганням і використанням хімічних та радіоактивних матеріалів, включаючи трубопроводи для транспортування небезпечних речовин.

Згідно до USA PATRIOT Act [355] поняття критичної інфраструктури визначається як системи та активи, фізичні або віртуальні, настільки життєво-важливі для Сполучених Штатів, що непрацездатність або руйнування таких систем та активів матиме виснажливий вплив на безпеку, національну економічну безпеку, здоров'я та безпеку населення, або будь-яку комбінацію цих питань. У сучасній Національній стратегії безпеки США до 2022 року [276; 326], прийнятій вперше у 2002 році з метою консолідації та мобілізації нації для захисту території штатів від терористичних загроз, захист критичної інфраструктури було визначено як один із шести пріоритетних напрямів. У даному контексті коментарі Ентоні Х. Кордесмана (A. H. Cordesman) [183] щодо вищезазначеного документу підкреслюють необхідність удосконалення правового забезпечення захисту критичної інфраструктури як одного з пріоритетних напрямків убезпечення територій в рамках огляду ядерної ситуації на 2020 рік і протиракетної оборони на 2022 рік. Отже, завдання національної безпеки, що включають заходи для захисту критичних об’єктів, реалізуються через Національні плани захисту інфраструктури (NIPP) [278], які регулярно оновлюються, враховуючи зміни у сфері безпеки.

Німецький підхід до трактування поняття критичної інфраструктури значною мірою збігається з визначенням, наведеним у законодавстві США, за винятком особливого акценту на важливості сталого постачання продукції, товарів та послуг і, крім того, відображає вплив стану критичної інфраструктури на громадську безпеку, яка, вочевидь є однією з найголовніших складових державної безпеки Німеччини. У CIP Strategy [279] зазначається, що критична інфраструктура – це організаційні та фізичні структури та об'єкти, що мають таке життєво важливе значення для суспільства та економіки країни, що їх вихід з ладу або деградація призведе до стійкого дефіциту постачання, значного порушення громадського порядку та безпеки або інших драматичних наслідків.

Згідно з Директивою Ради Європи від 8 грудня 2008 року, термін «критична інфраструктура» охоплює об'єкт, систему або їх елементи, що розташовані в межах держав-членів і мають вирішальне значення для забезпечення життєво важливих суспільних функцій, збереження здоров'я, безпеки, захисту, а також економічного та соціального добробуту населення; а пошкодження або знищення такої інфраструктури може спричинити значні наслідки для держави-члена через неможливість виконання вказаних функцій [19]. Натомість визначення поняття «критична інфраструктура» ЄС означає фізичних засобів та ІТ, мереж, послуг, активів, яка має важливе значення для підтримки життєво важливих суспільних функцій, здоров’я, безпеки, безпеки, економіки чи добробуту людей, і порушення або знищення якої призведе до мати значний вплив принаймні на дві держави-члени внаслідок неспроможності підтримувати зазначених функцій [116].

На нашу думку, критична інфраструктура – це система матеріальних і нематеріальних активів держави, що складається з об’єктів, які мають визначальне та ключове значення для забезпечення життєдіяльності, економіки та національної безпеки держави. Трансформація об’єктів критичної інфраструктури – це зміна, модернізація, покращення, відновлення об’єкта критичної інфраструктури.

У процесі визначення елементів критичної інфраструктури, що передбачає класифікацію конкретних об'єктів за категоріями (Рис. 1.1), формуються багаторівневі критерії, які складають ієрархічну структуру, до якої входить:

економічна безпека, яка охоплює фінансову стабільність і сприяння сталому розвитку; безпека життєдіяльності та здоров'я населення, що забезпечує належні умови для фізичного і психічного благополуччя громадян; а також недопущення техногенних катастроф регіонального або національного масштабів; державна безпека та оборона; та імідж держави.

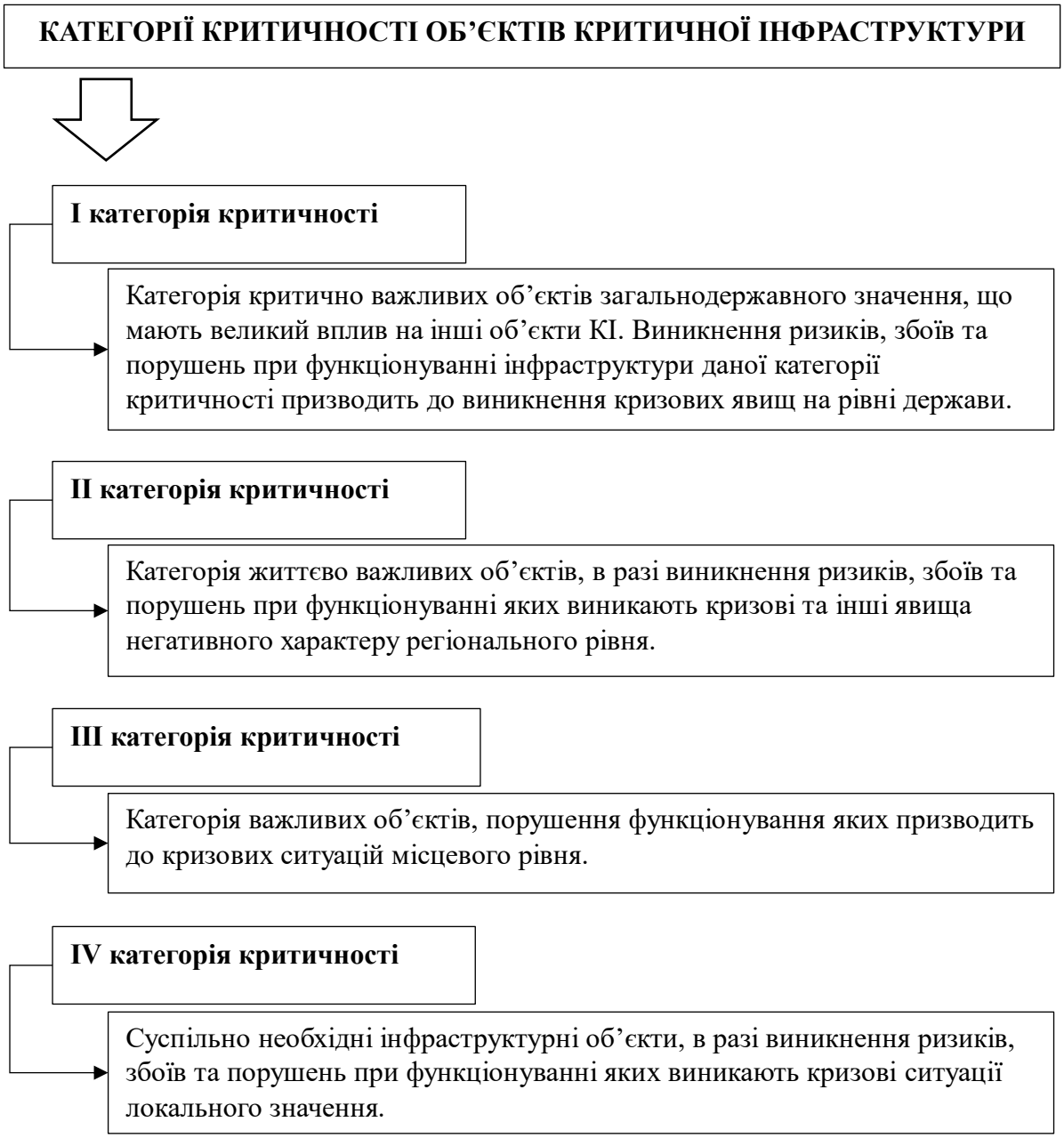


Рис. 1.1. Категорії критичності об'єктів критичної інфраструктури

Джерело: власна розробка автора

Відповідно до ст. 10 Закону України «Про критичну інфраструктуру» № 1882-IX від 21 вересня 2024 р. [83], для встановлення рівня вимог щодо забезпечення захисту об'єктів критичної інфраструктури, що ґрунтується на їх

важливості для реалізації окремих життєво важливих функцій у рамках секторів критичної інфраструктури, проводиться категоризація цих об'єктів. В результаті категоризації об’єктів критичної інфраструктури уповноваженими органами за секторами спільно з операторами критичної інфраструктури призначається категорія критичності об’єкта, які зображені на Рис. 1.1, що шляхом застосування форми відповідає як галузевим, так і міжгалузевим критеріям, які викладені в Методичних рекомендаціях, що стосуються категоризації об'єктів критичної інфраструктури [77]. Слід зазначити, що дані рекомендації враховують важливість кожного об’єкта, спираючись на аналіз вибраних збитків, які можуть виникнути при порушенні або припинення функціонування даного інфраструктурного об’єкта.

Реєстр об'єктів критичної інфраструктури є важливим офіційним документом, що відображає перелік ключових об'єктів, значущих для забезпечення стабільного функціонування суспільства, економіки та національної безпеки. До таких об'єктів належать ті, що є невід’ємною частиною енергетичної системи, транспортної інфраструктури, інформаційно-комунікаційних технологій, фінансових та банківських структур, а також інші стратегічні сфери.

Відповідно до Закону України «Про критичну інфраструктуру» № 1882-IX від 21 вересня 2024 р. [83], процес збору, узагальнення та попереднього аналізу інформації про об'єкти критичної інфраструктури здійснюється секторальними органами, які відповідають за визначені сектори. Дані органи також подають пропозиції щодо внесення об'єктів до Реєстру об'єктів критичної інфраструктури. Серед основних життєво важливих функцій та послуг, пов’язаних з об'єктами критичної інфраструктури, виділяють забезпечення адміністративних функцій та послуг, постачання електроенергії та тепла, водопостачання і водовідведення, забезпечення продовольством, діяльність у сфері охорони здоров’я, як державного, так і приватного, а також функціонування фармацевтичної промисловості тощо.

Згідно Законом України «Про критичну інфраструктуру» № 1882-IX від 21 вересня 2024 р. [83] визначено ряд секторів критичної інфраструктури (Рис. 1.2),

що включають: паливно-енергетичний сектор, цифрові технології, а також захист інформації. Також закон охоплює харчову промисловість, агропромисловий комплекс, охорону здоров’я, державний матеріальний резерв, ринки капіталу та організовані товарні ринки. Серед інших критичних елементів вказано фінансовий сектор, транспорт, поштові послуги, промисловість, а також системи життєзабезпечення. Не менш важливими є сектор громадської безпеки та цивільний захист населення і територій. Крім того, слід відзначити, охорону навколишнього середовища, сектор оборони, правосуддя та інформаційний сектор, що також входять до даної класифікації. Слід зазначити, що подібну класифікацію об’єктів критичної інфраструктури визначає Агентство з кібербезпеки та безпеки інфраструктури (CISA), згідно якої сектори енергетики, водопостачання, транспорту та хімічної промисловості мають загальнодоступні набори даних, які використовуються для розробки підходів на основі машинного навчання для виявлення кібератак системою управління інцидентами (ICS) [190].

Як комплекс різноманітних об'єктів і систем критична інфраструктура відіграє стратегічну роль у забезпеченні функціонування суспільства та стабільності економіки. Критична інфраструктура містить значну кількість об’єктів, що групуються за секторами, кожен з яких має свої специфічні об'єкти, що забезпечують виконання життєво важливих функцій.

Енергетичний сектор охоплює ключові об'єкти, такі як електростанції, що забезпечують виробництво електричної енергії; магістральні газопроводи і нафтопроводи, які відповідають за транспортування енергоресурсів; атомні станції, що є важливими для енергетичної безпеки; трансформаторні підстанції, які забезпечують стабільність електропостачання, а також інші об'єкти, що забезпечують функціонування енергетичної системи. Транспортний сектор включає критично важливі інфраструктурні об'єкти, такі як аеропорти, які забезпечують повітряне сполучення; залізничні вузли, що забезпечують транспортування вантажів і пасажирів; морські та річкові порти, які є важливими для міжнародної торгівлі; автомагістралі, тунелі, мости та інші елементи дорожньої інфраструктури, що забезпечують рух автомобільного транспорту.

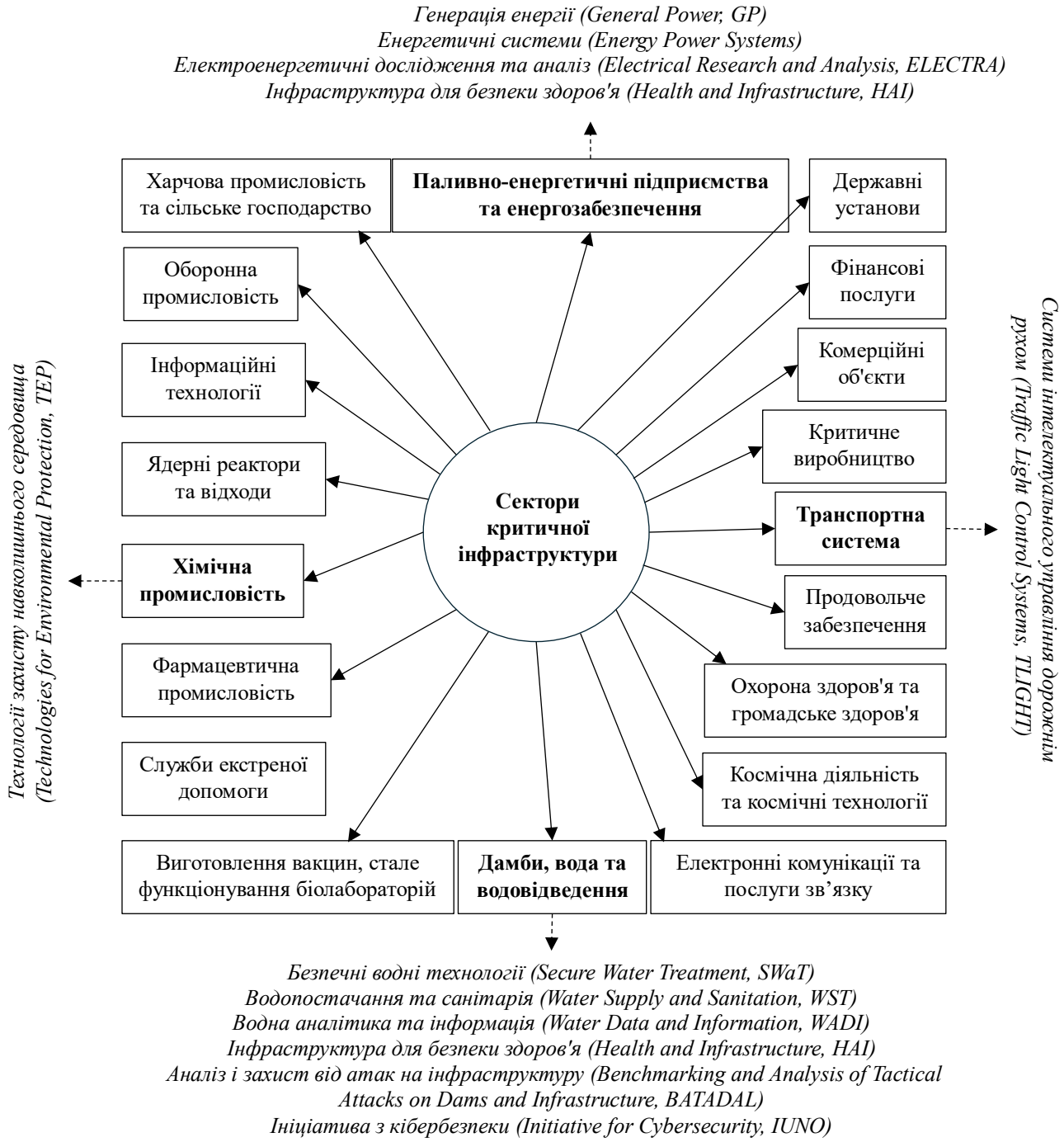


Рис. 1.2. Класифікація об’єктів критичної інфраструктури

Джерело: власна розробка автора

Сектор телекомунікацій охоплює різноманітні системи зв'язку, зокрема мережі мобільного зв'язку, супутникові системи та елементи кіберзахисту. Цифрова інфраструктура, яка включає в себе інтернет-інфраструктуру, також є важливою складовою, оскільки забезпечує комунікаційні можливості та інформаційний обмін.

Водопостачання та водовідведення є критично важливими для життєдіяльності населення, включаючи водозабори, водопроводи, каналізаційні мережі та водоочисні споруди, які забезпечують доступ до чистої води та ефективне відведення стічних вод.

Харчова промисловість включає об'єкти, що займаються виробництвом, зберіганням та розподілом харчових продуктів. До даного сектора входять також системи постачання води та енергії, необхідні для функціонування виробничих потужностей, які забезпечують продовольчу безпеку.

Фінансова система складається з банків, фінансових установ, бірж і платіжних систем, які забезпечують функціонування економіки, управління фінансами та електронних платежів. Інфраструктура електронних платежів стає дедалі важливішою у сучасних умовах.

Сфера охорони здоров'я охоплює лікарні, клініки, медичні лабораторії, аптеки, а також системи електронного здоров'я, що забезпечують доступ до медичних послуг і підтримують здоров'я населення.

Інформаційна інфраструктура включає в себе IT-мережі, центри обробки даних, сервери, електронні платформи та системи збереження даних, що забезпечують надійне зберігання та обробку інформації, критично важливої для функціонування всіх інших секторів критичної інфраструктури.

Слід також зазначити, що у сучасній науковій літературі [21; 29] пропонується категоризувати критичні об’єкти, що підлягають державному управлінню, за такими ознаками: об’єкти, що реалізують важливі функції державного управління; об’єкти безпеки життєдіяльності населення, призначені для транспорту; потенційно небезпечні об’єкти; об’єкти оборонного призначення; об’єкти, що забезпечують постійне або періодичне масове зібрання людей; а також об’єкти, що мають історичну та культурну значущість. Проте така категоризація, хоча і здатна забезпечити чітку систематизацію, полегшити управлінські процеси та посприяти підвищенню ефективності заходів з безпеки, має низку недоліків, зокрема, вона не враховує специфічні локальні умови, складність взаємозалежностей між різними типами об'єктів, а також можливу

динамічність загроз залежно від контексту соціально-економічних та політичних процесів.

Зосередившись саме на питанні складності взаємозалежностей між різними типами об'єктів, слід зазначити, що у науковій літературі [293] існує диференціація даного процесу на односторонню залежність та міжоб'єктну взаємозалежність. Одностороння залежність передбачає вплив функціонування одного об’єкта на інший, як, наприклад, у випадку, коли стабільна робота водоочисної станції детермінується доступністю систем зв’язку для підтримки механізмів моніторингу, диспетчерського контролю та збору даних (наприклад, SCADA чи GEOSimple); натомість взаємозалежність є складною двосторонньою конструкцією, що охоплює дві односторонні залежності, для розуміння якої потрібен детальний аналіз кожного напряму впливу з метою ефективного управління ризиками в межах критичної інфраструктури.

На основі вищезазначеного було сформовано схему взаємозалежностей різних секторів критичної інфраструктури в Україні, що має на меті підкреслити складність і багатогранність зв'язків, що існують між ключовими елементами критичної інфраструктури. Схема, представлена на рис. 1.3, відображає концепцію системної єдності, де окремі системи критичної інфраструктури залежать та функціонально пов’язані одна від одною, таким чином, створюючи мережу взаємозалежностей, що функціонують в умовах динамічного зовнішнього середовища. Тому збій або тимчасова зупинка в роботі однієї з систем критичної інфраструктури спричиняє значні негативні наслідки для інших залежних від неї систем та загалом для економічного розвитку держави. Зокрема, така ситуація спостерігалася на початку повномасштабного вторгнення, коли масові ракетні обстріли енергетичної інфраструктури з боку росії паралізували енергетичну систему України, що вплинуло на водопостачання, транспорт та екстрені і медичні служби, оскільки відсутність електрики ускладнила роботу насосних станцій, систем зв’язку та інших життєво важливих установ. Отже, руйнування багатьох стратегічно важливих інфраструктурних систем в Україні призвело до порушення загальної мережі зв’язків і залежностей, що призвело до ослаблення безпеки усієї держави.

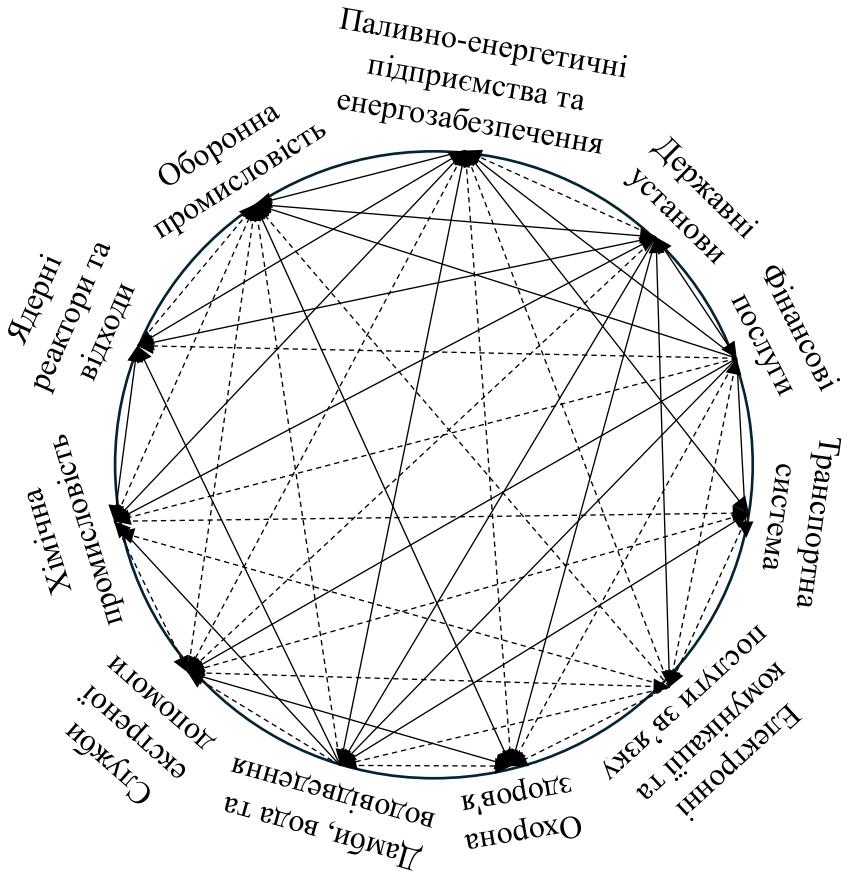


Рис. 1.3. Мережа взаємозалежностей між різними секторами критичної інфраструктури в Україні

Джерело: власна розробка автора

З огляду на це, у наведеній нижче схемі суцільні лінії зображують прямі зв'язки між секторами і свідчать про безпосередні взаємозалежності, які можуть вказувати на важливі потоки ресурсів, що забезпечують функціонування кожного сектора. Наприклад, енергетичний сектор може безпосередньо постачати електроенергію для систем водопостачання або транспортних мереж, що є критично важливим для їхньої роботи. Натомість штрихові лінії відображають непрямі залежності і, таким чином, підкреслюють необхідність врахування множинних аспектів взаємодії між секторами, які можуть не бути одразу очевидними. У даному випадку непрямі зв’язки вказують на те, як інформаційні технології можуть впливати на управлінські процеси в оборонному секторі, сфері фінансів тощо.

Слід також зазначити, що кожен з видів взаємозалежностей між інфраструктурними системами має свою специфіку, що зумовлює унікальні механізми впливу на стабільність функціонування цих систем. Так, існують фізична залежність, що передбачає функціонування однієї інфраструктури на базі матеріальних продуктів чи послуг, отриманих від іншої інфраструктури, що визначає їх взаємозв'язок; кіберзалежність, що виникає тоді, коли інфраструктура залежить від обміну інформацією через цифрові та інформаційні канали, а вирішальними для підтримки їх функціональності є дані, що циркулюють між системами; географічна залежність, що спостерігається у випадках, коли інфраструктурні елементи розташовані в одній географічній зоні, а умови даного регіону можуть одночасно впливати на всі розташовані в ньому системи; а також логічна залежність, що зумовлена не фізичними або інформаційними зв'язками, а людськими рішеннями та діями, що визначають роботу однієї системи залежно від стану іншої.

Таким чином, взаємозалежності між різними секторами критичної інфраструктури України складають основу її стійкості, стабільності та функціональної надійності, оскільки одні її компоненти прямим чином пов’язані з іншими через багатовимірні зв'язки, що ускладнюють функціонування держави та суспільства в умовах сучасних загроз. Забезпечення ефективності роботи інфраструктурних систем, яка базується на таких принципах, як надійність, економічність, раціональність і безпека, залежить від глибокого розуміння і адекватного управління взаємозалежностями. Проте, враховуючи вразливість окремих секторів до зовнішніх і внутрішніх ризиків, пріоритетом держави передусім є розвиток напрямків та окремих заходів для зниження негативного впливу таких залежностей, що вимагає розширеної співпраці на національному та міжнародному рівнях. Інтеграція відповідних рішень між державною адміністрацією, операторами критичної інфраструктури, а також партнерськими організаціями на регіональному та глобальному рівнях є необхідною для забезпечення стійкості, що сприяє ефективному функціонуванню держави в умовах наслідків війни та інших потенційних загроз.

1.2. Стан наукової розробки проблематики публічного управління у сфері трансформації об’єктів критичної інфраструктури

Стан наукової розробки проблематики публічного управління у сфері трансформації об’єктів критичної інфраструктури є актуальним напрямком дослідження, оскільки він також впливає на забезпечення стабільності суспільства та його розвитку. З метою аналізу поняття «критична інфраструктура» було досліджено велику кількість наукової літератури, зокрема на думку В. І. Мельникова, О. П. Мельникова, Т. В. Сідлярук, І. Ю. Тур, Г. М. Шведова [64] критична інфраструктура є сукупністю матеріальних та нематеріальних систем і об'єктів, що забезпечують життєдіяльність суспільства та економіки, а також підтримують національну безпеку, економічну стабільність і соціальний добробут. У своїй науковій праці Я. Рудюк, Р. Русин-Гриник, О. Федорчак [91] відзначає, що критична інфраструктура включає в себе основні компоненти, які є необхідними для функціонування суспільства, зокрема енергетичні системи, транспортні мережі, системи водопостачання, охорони здоров’я та інформаційні технології, які повинні бути захищені від різноманітних загроз. Схожу думку висунув В. І. Ящук [106], які вважають, що критична інфраструктура є системами, спорудами або технологіями, що забезпечують основні функції держави та суспільства, включаючи економічні, соціальні та екологічні аспекти, а також здатні пізнати негативний вплив у випадках кризових або надзвичайних ситуацій.

Серед зарубіжних трактувань даного поняття пропонуємо зазначити висновок А. Цзі, Р. Хе, В. Чень та Л. Чжан (A. Ji, R. He, W. Chen, L. Zhang) [243], які зазначають, що критична інфраструктура визначається як сукупність життєво важливих національних стратегічних ресурсів та об’єктів, що забезпечують надання фундаментальних послуг для економічної стабільності та соціального добробуту, включаючи водопостачання, транспорт, зв’язок, енергетику, атомну галузь, державне управління, охорону здоров'я та фінанси. Таку думку поділяють Ю. Ван, О. Чжао та Л. Чжан (Y. Wang, O. Zhao, L. Zhang) [361], які стверджують, що критична інфраструктура охоплює ключові системи, зокрема водопостачання,

енергетику, утилізацію відходів та транспорт, які задовольняють базові потреби суспільства і забезпечують умови для соціально-економічного розвитку, включаючи комерційну діяльність, медичне обслуговування та освіту. Натомість Х. Енрікес, Ф. Калдейра, Т. Круз, П. Сімоенс (J. Henriques, F. Caldeira, T. Cruz, P. Simões) [232] зазначають, що критична інфраструктура охоплює ключові системи, від яких залежить сучасне суспільство для отримання основних продуктів і послуг, що функціонують на основі систем промислової автоматизації та управління, які потребують комплексного захисту і вдосконалених стратегій управління для забезпечення їх безпеки та надійності.

Слід також зазначити, що під об’єктом критичної інфраструктури А. Р. Берклі, М. Уоллес, Ч. А. Ку (A. R. Berkeley, M. Wallace, C. A. Coo) [129], Г. Пескаролі, Д. Александер (G. Pescaroli, D. Alexander) [292] тощо розуміють конкретну фізичну чи інформаційну структуру, яка має вирішальне значення для функціонування критичної інфраструктури та забезпечення її стабільності, зокрема електростанції, лікарні, транспортних вузлів або мережі зв’язку. Натомість А. С. Джордж, Т. Баскар, П. Б. Шрікант (A. S. George, T. Baskar, P. B. Srikaanth) [221] вважають, що об’єкт критичної інфраструктури охоплює спеціалізовані компоненти, які вважаються важливими функціями в рамках критичної інфраструктури, і які можуть бути піддані ризикам або атакам, які можуть призвести до серйозних наслідків для національної безпеки та суспільної безпеки.

Також, варто звернути увагу на висновки В. МакОлі (W. McAuley), Е. Аксельсдоттір, Р. Джонасон Бйоренстам (E. Axelsdóttir, R. Jonason Bjärenstam) [264; 122] та інших, що характеризують критичну інфраструктуру як комплекс важливих об'єктів і систем, які виконують основні суспільні функції (VSF) і є життєво важливими для підтримки стабільності та безпеки держави. Автори наголошують на тому, що об’єкти КІ забезпечують основні потреби суспільства, від транспорту і енергетики до охорони здоров’я та інформаційних технологій, а їх безперервне функціонування є основою для нормального життя та розвитку. На думку Г. Пескаролі та Д. Александер (G. Pescaroli, D. Alexander) [292] критична інфраструктура має особливе значення в умовах масштабування загроз

та ризиків, наприклад, природні катастрофи, терористичні акти та техногенні аварії. Зазначені загрози часто викликають каскадні ефекти, що порушують роботу взаємопов’язаних елементів інфраструктури, що, у свою чергу, призводить до значних соціальних і економічних наслідків. У даному контексті К. Барке, М. Енглунд, К. Інга, К. Андре та Л. Сегнестам (K. Barquet, M. Englund, K. Inga, K. André, L. Segnestam) [125] досліджують різноманітні підходи до оцінки та управління ризиками, пов'язаними з критичною інфраструктурою. Завдяки детальному вивченню шведського досвіду, автори виявляють ключові методи та інструменти, які можуть бути застосовані в інших країнах для покращення управління ризиками в сфері критичної інфраструктури, зокрема пропонується: інтегрувати міжвідомчу співпрацю; розширити систему навчання і підготовки кадрів; а також впровадити нові технології для моніторингу і оцінки ризиків, що в подальшому дозволить створити стійку та адаптивну інфраструктурну систему України в умовах підвищеного рівня ризику та невизначеності.

Відповідно до Директиви Ради Європи [19], дане поняття охоплює об’єкти, системи та їхні елементи, які мають ключове значення для забезпечення життєво важливих функцій суспільства. Крім того, критична інфраструктура лише включає фізичні об'єкти, але й інформаційні технології, мережі та послуги, які формують основні складові функціонування держави. Вона виконує важливу роль у підтримці здоров’я, безпеки, економічного та соціального добробуту населення. Натомість критична інфраструктура ЄС як похідне поняття відзначається впливом на життєво важливі функції. Важливою рисою цього терміну є те, що будь-яке пошкодження або знищення таких об’єктів може призвести до серйозних наслідків лише для однієї країни, а й для небагатьох держав-членів, що підкреслює необхідність співпраці між країнами в управлінні та захисті критичної інфраструктури [116].

Важливо також зазначити думку М. Нейкової (M. Neikova) [269] щодо нової Директиви Ради Європи від 5 квітня 2022 року [186], що як і її попередня версія не обмежує компетенцію держав-членів та їхніх органів у питаннях адміністративної автономії, відповідальності за забезпечення національної

безпеки та оборони, а також їхньої здатності захищати інші важливі функції держави, особливо в контексті громадської безпеки, територіальної цілісності та підтримання правопорядку. На його думку виключення органів державного управління з дії цієї директиви має стосуватися суб'єктів, чия діяльність переважно пов'язана з національною безпекою, громадською безпекою, обороною або правоохоронною діяльністю, включаючи розслідування, виявлення та переслідування кримінальних правопорушень.

У сучасній науковій літературі, зокрема у роботах С. М. Домбровська [5], В. О. Шведун, М. Б. Домарацький [21], О. Єрменчук [28] та інших, пропонується категоризувати критичні об'єкти, які підлягають державному управлінню, відповідно до їх функціональної значимості. Вони включають об’єкти, які забезпечують ключові функції державного управління, підтримують безпеку населення, об’єкти транспорту, показані небезпечні виробництва, об’єкти оборонного призначення, місця масового скупчення людей, а також ті, що мають культурну чи історичну цінність. перевірити на те, що така класифікація допоможе систематизувати управлінські процеси, ефективність заходів безпеки та робить управління більш прозорим, її обмеження полягають у недостатньому врахуванні специфічних регіональних умов, складності взаємозв’язків між великими типами об’єктів, а також динамічного характеру загроз, які змінено залежно від політичних і соціально-економічних процесів.

Функції публічного управління критичною інфраструктурою варто розглядати як цілеспрямований вплив державних інституцій на суспільні та природні процеси через управлінські дії. Згідно до висновків М. Б. Домарацького [21] такі дії спричиняють зміни в управлінських об'єктах, впливаючи на поведінку та діяльність громадян. Основними напрямками функцій публічного управління є: політико-адміністративна, що координує роботу державних органів для захисту критичних об’єктів, економічна, що забезпечує функціонування важливих інфраструктурних систем, соціальна, що забезпечує доступ населення до базових послуг, та оборонна, спрямована на захист стратегічно важливих. об'єктів у контексті державної безпеки.

Наразі трансформація об'єктів критичної інфраструктури, що є важливою складовою національної безпеки, неодноразово привертала увагу дослідників. Проблематика національної критичної інфраструктури розглядається як ключовий елемент безпеки, оскільки її захист залежить від ефективності стратегій та технологій, спрямованих на протидію різноманітним загрозам.

Серед основних аспектів дослідження виділяється увага на визначення критичної інфраструктури в контексті різних секторів, включаючи енергетику, транспорт, фінансову сферу, телекомунікації, охорону здоров’я та інші. О. О. Верголяс [12] підкреслює, що ці сектори є стратегічно важливими для забезпечення функціонування економіки та державної безпеки. Дослідження акцентує на необхідності проведення глибоких реформ у системі захисту критичної інфраструктури України, зокрема через впровадження новітніх технологій і підходів, що є актуальним в умовах зростаючих гібридних загроз.

Натомість І. В. Уряднікова, В. М. Заплатинський [98] розглядають критичну інфраструктуру як сукупність фізичних і віртуальних систем, руйнування яких може завдати суттєвої шкоди національній безпеці та здоров’ю населення. Д. Г. Бобро [9] акцентує на техногенних аваріях, людських помилках, стихійних лихах і зловмисних діях як основних загрозах, тоді як О. М. Суходоля [22] виділяє надзвичайні ситуації, терористичні акти, диверсії та кіберзагрози, які вимагають комплексного підходу до їхнього запобігання.

Як стверджують вчені [293], критична інфраструктура перебуває у постійній взаємодії з навколишнім середовищем, використовуючи і трансформуючи вхідні дані з навколишнього середовища для надання вихідних даних тому ж самому середовищу. Взаємодію між критичною інфраструктурою та її оточенням можна охарактеризувати трьома категоріями:

І. Висхідні залежності. Продукти або послуги, що надаються одній інфраструктурі іншою зовнішньою інфраструктурою, які необхідні для підтримки її діяльності та функцій.

ІІ. Внутрішні залежності. Взаємодія між внутрішніми операціями, функціями та місіями інфраструктури. Внутрішні залежності - це внутрішні

зв’язки між активами, що складають критичну інфраструктуру (наприклад, електростанція, яка залежить від охолоджувальної води з власної свердловини).

III. Залежності, що виникають в процесі експлуатації. Наслідки для споживачів або реципієнтів критичної інфраструктури від деградації ресурсів, що надаються критичною інфраструктурою.

В рамках вищезазначених типів залежностей слід зазначити чотири основні види таких зв’язків, що підкреслюють різний характер взаємодії між інфраструктурними об’єктами та ресурсами, необхідними для їх функціонування.

I. Фізична. Інфраструктура є фізично залежною, якщо стан її функціонування залежить від матеріального результату (результатів) іншої інфраструктури через функціональний та структурний зв’язок між входами та виходами двох активів: товар (тобто товар або послуга), вироблений або модифікований однією інфраструктурою (вихід), потрібен іншій інфраструктурі для її функціонування (вхід).

II. Кіберзалежність. Інфраструктура має кіберзалежність, якщо стан її функціонування залежить від інформації та даних, що передаються через інформаційну інфраструктуру електронними або інформаційними каналами зв’язку. Виходи інформаційної інфраструктури є входами для іншої інфраструктури, а товаром, що передається між об’єктами інфраструктури, є інформація.

III. Географічна. Інфраструктурні активи є географічно залежними, якщо локальна природна подія може спричинити зміни у стані функціонування всіх інфраструктурних активів. Географічна залежність виникає, коли елементи інфраструктурних активів знаходяться в безпосередній просторовій близькості (наприклад, спільна смуга відводу для інженерних комунікацій).

IV. Логічна. Інфраструктура є логічно залежною, якщо стан її функціонування залежить від стану іншої інфраструктури через механізм, який не є фізичним, кібернетичним або географічним зв'язком. Логічна залежність пов’язана з людськими рішеннями та діями і не є результатом фізичних або кібернетичних процесів.

Зв’язки, що виникають між окремими системами критичної інфраструктури, створюють численні і часто складні залежності [318]. Виникнення великої кількості зв’язків автоматично робить окремі системи критичної інфраструктури чутливими до різних видів втручань. Окремі системи критичної інфраструктури до різних видів втручань, що в результаті може призвести до пошкодження або повного руйнування компонентів системи. Однак ці зв’язки та залежності не можна розглядати лише крізь призму загроз як таких, що послаблюють критичну інфраструктуру. Завдяки існуючим зв’язкам можливе функціонування окремих систем критичної інфраструктури, які, якби вони створили повністю незалежну, окрему повністю незалежну, окрему систему, вони не змогли б функціонувати. Існуючі зв’язки мають двоякий характер, з одного боку, вони підвищують ефективність функціонування систем за рахунок інтеграції їх елементів, з іншого – підвищують їх вразливість до будь-якого роду збоїв. Позитивний та негативний вплив зв’язків критичної інфраструктури на ефективність її функціонування відзначають функціональність критичної інфраструктури.

Різні види залежностей у критичній інфраструктурі, як зазначено у дослідженнях П. Мішсек та А. Сколімовська [318], є поширеними у державному і приватному секторах, мають низку суттєвих відмінностей у масштабах та рівні складності. Тому для глибокого розуміння взаємозалежностей між різними інфраструктурними системами необхідний багатовимірний підхід до їх вивчення. Згідно до висновків зазначених авторів, ключові аспекти, що характеризують взаємозалежності між інфраструктурою, охоплюють: тип збоїв; особливості інфраструктури; масштаб та область впливу наслідків залежності; стан функціонування інфраструктури; тип взаємозалежності; зовнішні та внутрішні умови та середовище; а також зв'язки між інфраструктурами.

У своїй науковій праці Д. С. Бірюков, С. І. Кондратов, О. І. Насвіт, О. М. Суходоля [8] наголошують на важливості системного підходу до аналізу загроз, пов’язаних з аваріями та небезпечними природними явищами. У своїх роботах О. П. Єрменчук [28;69] підкреслює значення міжнародного досвіду в

організації захисту критичної інфраструктури, звертаючи увагу на необхідність систематичного планування безпекових заходів.

З розвитком нової концепції державного управління (NPM) управління критичною інфраструктурою зазнало значної трансформації, зокрема щодо децентралізації функцій володіння, експлуатації та обслуговування об’єктів критичної інфраструктури та розподілу цих повноважень між державними та приватними структурами в межах держави [168]. Така організаційна перебудова зумовила необхідність наукових досліджень, спрямованих на оцінку її впливу на надійність і функціональну стійкість інфраструктурних об'єктів, що підтримують суспільство. Сучасні науковці, зокрема А. Венкатараман, С. Х. Ч. Лім, Л. Дж. Хао та К. П. Дж. Ві (A. Venkataraman, S. H. C. Lim, L. J. Hao, J. C. P. Wee) [360], значну увагу приділяють саме питанням надійності в умовах фрагментованого управління, однак аспекти реагування на надзвичайні ситуації та заходів відновлення залишаються недостатньо дослідженими. Попри це, Г. Пескаролі та інші (G. Pescaroli) [109] стверджують, що інституційно фрагментовані структури критичної інфраструктури часто зазнають серйозних випробувань у випадку інцидентів чи кризових ситуацій, що ускладнює ефективну координацію заходів з ліквідації наслідків. У даному контексті А. Седергрен, Дж. Йоханссон, Х. Хассель (A. Cedergren, J. Johansson, H. Hassel) [168] зазначають, що в інституційно фрагментованому середовищі існують певні загрози для стійкості критичної інфраструктури, зокрема через складність та потребу у додаткових ресурсах при здійсненні державного управління та операцій з реагування і подальшого відновлення.

На думку Я. Страгніцького [321] для підвищення ефективності державної політики в захисті критичної інфраструктури необхідно зосередити зусилля на інституційних трансформаціях, спрямованих на забезпечення її резильєнтності. У даному контексті автором пропонується впровадити регулювання публічно-приватної взаємодії; залучити представників силових структур; проводити періодичний скринінг готовності сил реагування; розробити відповідні програми навчання та тренінгів для працівників; інтегрувати фізичний та кібернетичний захист критичної інфраструктури; реалізувати превентивні заходи; а також

сформувати Превентивну концепцію резильєнтності об’єктів критичної інфраструктури.

З іншого боку Б. Ягусяк, В. Качмарек (B. Jagusiak, W. Kaczmarek) [242] для ефективного виконання завдань державної політики щодо захисту критичної інфраструктури пропонують удосконалення інституційного забезпечення з акцентом на тісну співпрацю між державними органами, приватними операторами та суспільством. Отримати очікуваний ефект від даного удосконалення автор пропонує шляхом підвищення обізнаності громадян щодо управління безпекою критичної інфраструктури та способів реагування на кризи, зокрема через різні види навчань і тренінгів.

В рамках впровадження структурованого сценарного процесу, що реагує на широке коло загроз, пов'язаних із критичною інфраструктурою, шляхом розробки модульної системи М. А. Елен та В. Варгас (M. A. Ehlen, V. Vargas) [260] пропонують інтегрувати економічний аналіз у традиційні підходи, враховуючи як матеріальні, так і нематеріальні наслідки екстремальних подій. Такий багаторівневий підхід до оцінки впливів на різні економічні суб'єкти, від окремих підприємств до макроекономіки, є важливим аспектом запропонованої методології.

У науковій літературі запропоновано також різноманітні підходи до публічного управління критичної інфраструктури, які варіюються від системного управління та централізованого контролю до ризик-орієнтованого підходу та гнучких моделей управління. Такі моделі відображають необхідність ефективної координації між різними інституціями, впровадження сучасних технологій і відповідної нормативно-правової бази, що адаптується до динамічних умов сучасного світу. Зокрема, в умовах децентралізації та глобальної інтеграції держави потребують нових стратегій управління, які враховують потенціал приватного сектору та міжнародних партнерів у забезпеченні безпеки й стабільності функціонування критичної інфраструктури. Підходи до публічного управління об’єктами критичної інфраструктури систематизовано у Таблиці 1.1.

Таблиця 1.1

Підходи до публічного управління об’єктами критичної інфраструктури

№	Підхід	Автори	Сутність
1.	Системний підхід	О. Мельничук [59], І. Жукова, Н. Трушкіна [31], А. О. Магомедов [53], Д. С. Бірюков, С. І. Кондратов, О. І. Насвіт, О. М. Суходоля [8] тощо.	Стратегічне управління, планування, розвиток КІ як частини системи національної безпеки на основі публічного менеджменту.
2.	Гнучкий підхід	Ю. В. Кузьменко, О. М. Коропатов, Р. В. Думанський [47] тощо.	Адаптація до загроз і ризиків, технологічних зрушень та швидке реагування на надзвичайні ситуації.
3.	Ризик-орієнтований підхід	О. Потій, А. Семенченко, О. Бакалинський, Д. Мялковський [74], В. Шиповський [102] тощо.	Ідентифікація загроз і ризиків, оцінка втрат, аналіз вразливостей, планування реагування на надзвичайні ситуації.
4.	Централізований підхід	О. С. Нєма [65], В. Р. Федик, Г. В. Денисенко [99] тощо.	Державний контроль і нагляд за секторами (транспорт, енергетика, телекомунікації, водопостачання).
5.	Фрагментований підхід	А. Венкатараман, С. Х. Ч. Лім, Л. Дж. Хао та К. П. Дж. Ві [360], Г. Пескаролі, Д. Александер, В. Мюррей та інші [109],А. Седергрен, Дж. Йоханссон, Х. Хассель [168] тощо.	Розподіл повноважень між державними та приватними структурами, децентралізація влади, переосмислення координації дій між різними структурами.
6.	Інституційне забезпечення	Я. Стрaгніцький [321], Б. Ягусяк, В. Качмарек [242], М. А. Елен та В. Варгас [260]тощо.	Впровадження механізмів для регулювання публічно-приватної взаємодії, інтеграція кібер- і фізичного захисту, сценарне моделювання загроз для забезпечення стійкості та підвищення резильєнтності КІ.
7.	Державно-приватне партнерство	І. Жукова, Н. Трушкіна [30], В. В. Круглов [46], О. Я. Лазор, І. Г. Юник [49], І. Г. Лук’яненко, М. Е. Мар’янович [51] тощо.	Співпраця між різними рівнями управління, залучення приватних компаній до керівних процесів.
8.	Міжнародне партнерство	А. О. Магомедов [54], К. В. Клименко, М. В. Савостьяненко [42] тощо.	Залучення міжнародних партнерів для забезпечення безпеки і надійності роботи КІ.

Джерело: сформовано автором на основі [8, 30, 31, 42, 44, 46, 47, 49, 51, 53, 54, 59, 65, 74, 99, 102, 168, 242, 260, 321, 360]

Таким чином, у науковій літературі пропонується розглядати публічне управління об’єктами критичної інфраструктури крізь ряд ключових напрямків його розвитку в сучасних умовах:

І. Системний підхід до стратегічного управління та планування об'єктів критичної інфраструктури є ключовою складовою забезпечення національної безпеки. Підхід обґрунтовується на інтеграції цих різноманітних елементів, процесів і методів, що дозволяє комплексно підходити до управління критичними об'єктами. В основі системного підходу лежать принципи розвитку та взаємозв’язку між ефективними компонентами інфраструктури, що включає як технічні, так і управлінські аспекти. Такі науковці, як О. Мельничук [59], І. Жукова, Н. Трушкіна [31], А. Магомедов [55] та інші, відзначають ефективність застосування системного підходу через його здатність забезпечувати координацію дій у рамках публічного менеджменту. Підхід забезпечує чітке планування на кожному етапі розвитку критичної інфраструктури, що включає не лише проектування та будівництво об’єктів, але й розробку стратегії їхнього захисту від зовнішніх і внутрішніх загроз. Методологічна основа системного підходу забезпечує використання принципів інтеграції, прогнозування та адаптивного управління, що дозволяє зменшити динамічність зовнішнього середовища та можливості ризиків; а моніторинг, аналіз загроз, розробка планів реагування, є невід’ємними елементами цього підходу, що дозволяє забезпечити стійкість і надійність об’єктів критичної інфраструктури.

ІІ. Основною перевагою централізованого підходу на думку О. С. Нєма [65], В. Р. Федик, Г. В. Денисенко [99] є можливість швидкого та ефективного реагування на загрози, що відображається у стратегічно важливих сферах. Проте в умовах децентралізації, коли повноваження делегуються на місцевий рівень, централізоване управління втрачає свою ефективність. Розподіл функцій публічного менеджменту між вищими інституційними рівнями вимагає більших гнучких механізмів, які враховують місцеві особливості, автономність і самодостатність регіональних органів влади [28]. Такий підхід не дозволяє забезпечити специфічні місцеві потреби та умови, що можуть спричинити неузгодженість дій і неефективне управління на місцях.

ІІІ. Гнучкий підхід до публічного управління об’єктами критичної інфраструктури є важливою складовою сучасної системи національної безпеки, яка здатна адаптуватися до постійних змін у середовищі загроз та ризиків.

Важливим аспектом цього підходу є його здатність швидко інтегрувати новітні технології, які сприяють підвищенню рівня захисту критичної інфраструктури. На думку сучасних авторів, зокрема Ю. В. Кузьменко, О. М. Коропатов, Р. В. Думанський [47] тощо, такий підхід не лише регулює ризики, а й передбачає проактивне планування, яке дозволяє прогнозувати можливості загрози та мінімізувати їх вплив; що є особливо важливим для забезпечення безперервної роботи критично важливих об'єктів у випадках надзвичайних ситуацій, зокрема військових конфліктів. Гнучкість системи управління дозволяє ефективніше реагувати на події, зменшуючи час реагування та підвищуючи рівень координації між загальними інституційними рівнями.

IV. Ризик-орієнтований підхід у публічному управлінні критичною інфраструктурою акцентує увагу на систематичній ідентифікації можливих загроз та оцінці ймовірних втрат у випадку реалізації неприйнятних подій. Як відзначають О. Потій, А. Семенченко, О. Бакалинський, Д. Мялковський [74], В. Шиповський [102] ті інші ризик-орієнтований підхід до кіберзахисту критичних об’єктів дозволяє створити ефективні моделі взаємодії між більшими суб’єктами безпеки, враховуючи їх функціональні можливості. Використання ризик-орієнтованих методів управління сприяє покращенню виконання управлінських завдань шляхом чіткого розподілу обов’язків та зосередженості на превентивних заходах.

V. Великої підтримкою наукової спільноти користується підхід, що забезпечує налагодження партнерства та співпрацю між ефективними інституційними рівнями публічного управління, є інноваційним і надзвичайно високим у контексті забезпечення безпеки об’єктів критичної інфраструктури. Він обґрунтовується на тісній взаємодії державного та приватного секторів, що дозволяє залучити приватні компанії до керівних процесів, підвищуючи загальний рівень захисту інфраструктурних об’єктів. Такий підхід відкриває можливості для ефективної реалізації публічних функцій, зокрема тих, які можуть бути делеговані на приватний або місцевий рівень управління. На думку, І. Жукова, Н. Трушкіна [30], В. В. Круглов [46], О. Я. Лазор, І. Г. Юник [50], І. Г. Лук’яненко, М. Е. Мар’янович [51] тощо завдяки оптимальному

використанню ресурсів і знань приватного сектору, який часто володіє передовими технологіями та експертизою в галузі захисту критичної інфраструктури. Крім того, таке співробітництво полегшує реалізацію заходів безпеки на національному, регіональному, місцевому та локальному рівнях, останній рівень кожного отримує доступ до належних ресурсів і компетенцій.

VI. Необхідність міжнародної кооперації у забезпеченні стабільного функціонування критичних систем, обладнання та мережі відзначається у роботах К. В. Клименко, М. В. Савостьяненко [42] тощо. Автори стверджують, що інтеграція досвіду і технічних можливостей міжнародних партнерів дозволяє створити більш стійкі до загроз системи управління та безпеки. Залучення міжнародних партнерів до підвищення стандартів безпеки та надійності, що дозволяє використовувати передові методології та технологічні рішення, які вже довели свою ефективність у різних країнах. Така співпраця також відкриває можливості для спільного реагування на надзвичайній ситуації, підвищення рівня кібербезпеки та захисту інфраструктури від гібридних загроз.

Таким чином, різні погляди на публічне управління об’єктами критичної інфраструктури висвітлюють багатоаспектний підхід до забезпечення їхньої безпеки та функціонування, що охоплює централізовані, децентралізовані, гнучкі, партнерські та ризик-орієнтовані моделі управління.

1.3. Основні функції та особливості управління об’єктами критичної інфраструктури

Публічне управління об’єктами критичної інфраструктури (КІ) відіграє надзвичайно важливу роль у забезпеченні стабільності та безпеки держави, що передбачає не тільки підтримку надійної роботи окремих секторів, але й забезпечення їх захищеності та здатності протистояти різним загрозам. Усі чинники та наслідки ризику наведено на Рис. 1.4. Особливості управління критичними об'єктами вимагають використання стратегічного підходу, що

враховує специфічні вимоги безпеки, оперативного реагування та постійного моніторингу. У даному контексті функції управління охоплюють аналіз ризиків, розробку політик з попередження загроз, організацію міжвідомчої співпраці та залучення різних ресурсів і технологій для забезпечення готовності до можливих кризових ситуацій.

Функції публічного управління слід розглядати як об'єктивно визначені прояви влади, які виявляють цілеспрямований, організаційний та регуляторний вплив з боку державних інституцій на різноманітні суспільні та природні процеси. Даний вплив, на думку М. Б. Домарацького [21], що реалізуються через конкретні дії, формують специфічні зміни в об'єктах управління, включаючи свідомість, поведінку та діяльність індивідів у суспільстві.

Дані функції охоплюють низку важливих напрямів, які спрямовані на забезпечення безпеки, стійкості та належного функціонування критичних секторів держави.

По-перше, політико-адміністративна функція полягає в координації державних органів та прийнятті управлінських рішень, що забезпечують захист та ефективне управління критичними об'єктами, зокрема в умовах надзвичайних ситуацій. По-друге, економічна функція передбачає забезпечення безперервного функціонування економічно значущих об'єктів інфраструктури, таких як енергетичні та транспортні системи, що є основою для підтримання економічної стабільності країни. Крім того, соціальна функція державного управління у цьому контексті полягає в гарантуванні доступу населення до життєво необхідних послуг, таких як охорона здоров'я, водопостачання та продовольче забезпечення. Також важливу роль відіграє оборонна функція, яка спрямована на захист інфраструктурних об’єктів стратегічного значення, особливо в умовах загроз державній безпеці, та забезпечення готовності до реагування на кризові ситуації [58]. Таким чином, до загальних функцій публічного управління планування, яке полягає у визначенні стратегій і заходів для підтримання надійності та безпеки критичних об’єктів. Регулювання передбачає встановлення норм і правил для забезпечення їх функціонування відповідно до законодавчих вимог і стандартів.



Рис. 1.4. Матриця загроз критичній інфраструктурі

Джерело: власна розробка автора

Координація включає узгодження дій різних органів державної влади та приватних суб'єктів для належного управління об'єктами інфраструктури, що мають критичне значення. Облік полягає у веденні реєстрів та іншої документації, що дозволяє стежити за станом і діяльністю цих об'єктів. Контроль виконує роль моніторингу й оцінки діяльності об’єктів критичної інфраструктури з метою забезпечення відповідності стандартам безпеки та ефективності управління. Натомість допоміжні функції, спрямовані на забезпечення дієздатності управлінських органів, що відповідають за об'єкти критичної інфраструктури. Серед таких функцій визначаємо кадрову, що полягає в підборі, підготовці та управлінні персоналом, що безпосередньо працює на об’єктах критичної інфраструктури; матеріально-технічну, що забезпечує постачання необхідних ресурсів та обладнання, що гарантує безперервну діяльність таких об'єктів; а також діловодство відіграє важливу роль у веденні документальної бази, необхідної для ефективного функціонування системи управління критичною інфраструктурою. Зазначені допоміжні функції є обов'язковими для всіх управлінських структур, адже без їх якісної реалізації діяльність публічного управління неможлива.

У даному контексті також важливо виокремити основні ознаки публічного управління об’єктами критичної інфраструктури. Однією з основних характеристик є державно-приватна взаємодія, яка передбачає системний обмін інформацією між органами державної влади, приватними структурами та громадським сектором. Зазначена колаборація є невід’ємною частиною оперативного реагування на наявні загрози критичній інфраструктурі, оскільки забезпечує формування інтегрованої системи захисту. Важливість даного аспекту підкреслюється Постановою Кабінету Міністрів України «Про затвердження Регламенту обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури» № 1174 від 14 жовтня 2022 р. [81], в якій сформульовано механізм інформаційної взаємодії, що забезпечує захист критичної інфраструктури та підтримку її стійкості. Крім того, Постанова «Деякі питання подання інформації у сфері захисту критичної інфраструктури» № 1175 від 14 жовтня 2022 р. [26] детермінує структуру звітності, що створює необхідні

умови для підзвітності операторів та секторальних органів, уповноважених на захист критичної інфраструктури. Дані нормативні акти ілюструють зростання значення міжсекторального діалогу, що стимулює ефективну координацію зусиль усіх учасників, залучених до процесу управління.

Ще однією важливою ознакою є активне залучення територіальних громад до процесів публічного управління критичною інфраструктурою, що включає розробку програм співпраці з муніципалітетами, метою яких є підтримка населення в критичних ситуаціях. Налагодження ефективної комунікації з громадянами для попередження про потенційні загрози, наслідки надзвичайних ситуацій, а також необхідні дії в разі руйнування об’єктів критичної інфраструктури, особливо в умовах повномасштабного вторгнення, стає критично важливим. Залучення населення до процесів управління не лише підвищує рівень обізнаності, але й забезпечує більшу готовність до реагування на надзвичайні ситуації.

У свою чергу міжвідомча взаємодія є ще однією важливою характеристикою публічного управління критичною інфраструктурою. Координація дій між міністерствами, уповноваженими органами, місцевими виконавчими органами та органами місцевого самоврядування має стратегічне значення для забезпечення стійкості та безперервності функціонування об'єктів критичної інфраструктури. Взаємодія цих структур дозволяє формувати єдину систему управління, що відповідає сучасним викликам і ризикам. Зазначені характеристики публічного управління критичною інфраструктурою визначають його специфіку, безпосередньо впливають на забезпечення безпеки, захисту, стійкості та надійності роботи секторів, які є критично важливими для життєдіяльності населення.

Управління об'єктами критичної інфраструктури охоплює широкий спектр функцій та завдань, спрямованих на забезпечення стабільності та безпеки життєво важливих елементів, від яких залежить економічна, соціальна та гуманітарна стійкість суспільства. Критична інфраструктура, зокрема, є сукупністю об’єктів, пристроїв, установок і послуг, чиє неперервне функціонування є основою для забезпечення суспільного добробуту та

стабільного розвитку країни. Будь-які порушення у роботі цих об’єктів можуть мати катастрофічні наслідки, включно з втратою життів, завданням шкоди здоров’ю населення, порушенням повсякденного життя громадян та значним впливом на суспільну довіру [369].

Розуміння ролі та функцій критичної інфраструктури передбачає комплексний підхід до її ідентифікації, класифікації та оцінки ризиків. Це дозволяє точно визначити об'єкти, що вимагають посилених заходів безпеки, та сформувати адаптовані стратегії захисту, орієнтовані на запобігання функціональним збоям або руйнуванням. Завдяки чітко встановленим критеріям відбору елементів до складу критичної інфраструктури можна забезпечити їхню пріоритетність у процесі захисту та ефективного управління. Вивчення наукових та практичних підходів до управління критичною інфраструктурою у роботі K. Фіконь (K. Ficoń) [215] підтверджує, що її захист є багатокомпонентним процесом, що вимагає оцінки вразливостей та ризиків і, крім того, системного моніторингу, контролю й адаптації заходів безпеки у відповідь на зміну масштабів та наслідків загроз.

Головною особливістю публічного управління критичною інфраструктурою є те, що воно має багатокомпонентну структуру, впровадження якої обумовлено необхідністю забезпечення безперервності функціонування стратегічно важливих об'єктів, їх захищеності та здатності прогнозувати та уникати різноманітні загрози. Наведена у Таблиці 1.2 структура включає в себе ряд особливостей та ключових напрямків, що спрямовані на підтримку та розвиток публічного управління критичною інфраструктурою в Україні.

Таблиця 1.2

Основні напрямки та особливості публічного управління критичною інфраструктурою в Україні

№	Напрямок	Сутність	Заходи
1.	Стратегічне планування	Систематичне визначення завдань у секторах критичної інфраструктури та координація дій суб’єктів управління	Розробка стратегій та планів дій для запобігання та реагування на загрози; координація дій між різними рівнями та секторами публічного управління
2.	Управління активами	Використання програмних систем управління активами підприємства	Впровадження EAM-систем для ефективної інвентаризації активів,

		(EAM) для моніторингу всіх критичних активів	планування технічного обслуговування та управління життєвим циклом
3.	Аналіз даних і прогнозне технічне обслуговування	Використання аналітичних інструментів для виявлення закономірностей і тенденцій	Застосування методів прогнозованого технічного обслуговування для запобігання збоям обладнання та зменшення часу простою
4.	Системи диспетчерського контролю та збору даних	Впровадження SCADA для моніторингу фізичних процесів критичної інфраструктури	Використання SCADA-систем для дистанційного контролю, збору даних в реальному часі та прийняття обґрунтованих рішень
5.	Системи резервування та резервного копіювання	Впровадження систем резервування для забезпечення безперервності операцій	Регулярне тестування резервних систем і проведення заходів для їхньої ефективності
6.	Безпека і захист інформації	Забезпечення конфіденційності та цілісності інформації щодо об'єктів критичної інфраструктури	Впровадження заходів щодо захисту інформації, моніторинг та управління доступом до даних об'єктів критичної інфраструктури
7.	Моніторинг і безпека мережі	Впровадження інструментів моніторингу та безпеки для постійного моніторингу мережевої інфраструктури	Використання рішень для виявлення та реагування на кіберзагрози, уразливості та аномалії
8.	Віддалений моніторинг і контроль	Реалізація можливостей дистанційного моніторингу та керування	Використання програмних рішень для централізованого контролю систем критичної інфраструктури з метою швидкого реагування на інциденти
9.	Системний моніторинг та оцінка ризиків	Постійний контроль стану безпеки та ідентифікація загроз критичній інфраструктурі	Впровадження механізмів моніторингу та оцінки ризиків; аналіз потенційних загроз, вразливостей, а також оцінка можливих втрат і відновлення
10.	Запобігання кризам та надзвичайним ситуаціям	Підготовка суб’єктів управління до кризових явищ та надзвичайних ситуацій	Розробка і впровадження планів реагування на терористичні акти, природні катастрофи, техногенні аварії та збройні агресії; регулярні тренування та навчання
11.	Ризикоорієнтовний підхід	Оцінка та пріоритезація ризиків для систем інфраструктури	Впровадження заходів з управління ризиками та розподіл ресурсів на основі критичності активів і потенційного впливу збоїв
12.	Реагування на інциденти та аварійне відновлення	Розробка комплексних планів реагування на інциденти	Створення покрокових процедур для реагування на кібератаки, стихійні лиха та інші надзвичайні ситуації
13.	Співпраця та обмін інформацією	Сприяння співпраці та обміну інформацією між зацікавленими сторонами	Організація спільних заходів для обміну інформацією про загрози та найкращі практики серед державних установ, галузевих партнерів та організацій з кібербезпеки
14.	Публічно-приватне партнерство	Співпраця держави та приватного сектора у сфері управління критичною інфраструктурою	Залучення приватних компаній до управлінських процесів; розподіл функцій і відповідальності між державним сектором та бізнесом для підвищення ефективності управління
15.	Нормативно-правова база	Визначення стандартів, норм та вимог для управління критичною інфраструктурою	Формування і впровадження нормативно-правової бази; дотримання стандартів та вимог, встановлених

			міжнародними організаціями та партнерами
16.	Відповідність і нормативні вимоги	Забезпечення відповідності програмних систем до норм і стандартів	Перевірка відповідності стандартам кібербезпеки, захисту даних і галузевим вимогам

Джерело: власна розробка автора

Центральною ланкою такого управління є стратегічне планування, яке передбачає глибокий аналіз ризиків та розробку комплексних програм запобігання надзвичайним ситуаціям, що ґрунтується на системному підході до кожного з секторів критичної інфраструктури, з урахуванням їхніх унікальних характеристик та взаємозалежностей. Крім того, ключовим елементом стратегічного планування є координація дій між численними суб’єктами публічного управління на національному, регіональному та місцевому рівнях, а також між різними секторами економіки та безпеки. Даний процес передбачає синергію зусиль різних органів державної влади, операторів критичних об'єктів, а також приватного сектора, що забезпечує інтегрований підхід до протидії загрозам та мінімізації наслідків можливих катастроф. Важливою є також розробка оперативних планів реагування на випадок виникнення надзвичайних ситуацій, що спрямовані на мінімізацію шкоди та швидке відновлення функціональності об’єктів.

Забезпечення готовності до надзвичайних ситуацій та кризових явищ, включно з тероризмом, природними катастрофами, техногенними аваріями, а також наслідками збройної агресії росії, вимагає від органів державної влади розробки та реалізації планів реагування. Визначені плани мають враховувати всі можливі ризики та передбачати комплекс заходів, спрямованих на мінімізацію наслідків можливих кризових ситуацій, забезпечуючи таким чином безперервність функціонування критичних інфраструктурних об'єктів.

Моніторинг і оцінка ризиків, а також аналіз рівня безпеки критичної інфраструктури є ключовими елементами сучасної моделі публічного управління, спрямованої на забезпечення стабільності та надійності функціонування цих об’єктів. Така система дає змогу вчасно виявляти можливі загрози, вразливості, оцінювати масштаби потенційних збитків і здатність

об'єктів до відновлення. Важливо також встановити відповідальних за захист і безпеку конкретних інфраструктурних об'єктів у різних секторах економіки.

Згідно з Постановою Кабінету Міністрів України «Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури» № 821-2022-п від 22 липня 2022 р. [80], затверджено порядок проведення моніторингу рівня захищеності критичних об'єктів. Даний процес включає систематичні заходи, спрямовані на збір, обробку та аналіз даних про фактичний стан безпеки об'єктів, дотримання законодавчих норм у сфері критичної інфраструктури, а також контроль ризиків. Крім того, моніторинг дозволяє підвищувати заходи з безпеки, забезпечувати стійкість та визначати перспективи подальшого розвитку системи захисту критичної інфраструктури.

Модель публічно-приватного партнерства є важливою для ефективного управління критичною інфраструктурою, особливо у процесі приватизації. Використання ресурсів приватного сектору спільно з державними органами сприяє підвищенню ефективності управлінських рішень, надаючи приватному бізнесу можливість брати участь в управлінні окремими аспектами діяльності інфраструктурних об’єктів. У даному контексті ефективна охорона критичних об'єктів вимагає координації державних органів і залучення широкого кола суб’єктів, а такі взаємини носять публічно-правовий характер [68].

Управління критичною інфраструктурою ґрунтується на встановлених державних стандартах, нормативних актах та вимогах, що формуються як на національному, так і на міжнародному рівнях. Зокрема, Закон України «Про критичну інфраструктуру» № 1882-IX від 21 вересня 2024 р. [83], визначає правові та організаційні основи функціонування національної системи захисту критичної інфраструктури. Дана система включає комплекс органів управління, а також сили і засоби, що належать як центральним, так і місцевим органам виконавчої влади (в тому числі в контексті військово-цивільних адміністрацій), органам місцевого самоврядування та операторам, які можуть бути як юридичними, так і фізичними особами, незалежно від форми власності. Вони здійснюють управління та забезпечують функціонування критичної інфраструктури, реалізуючи державну політику в її захисті. Також важливими

аспектами державної політики у цій сфері є Постанови Кабінету Міністрів України, які регламентують ведення Реєстру об'єктів критичної інфраструктури. Постанова «Про затвердження Порядку ведення Реєстру об’єктів критичної інфраструктури, включення таких об’єктів до Реєстру, доступу та надання інформації з нього» № 415 від 28 квітня 2023 р. [79] та Постанова «Деякі питання паспортизації об’єктів критичної інфраструктури» № 818 від 4 серпня 2023 р. [25] визначають основні принципи державної політики щодо захисту критичної інфраструктури. Дані документи встановлюють ключові фактори, що впливають на стан об'єктів критичної інфраструктури, включаючи збереження матеріальних і нематеріальних цінностей, основи економіки, фінансів, організації праці та управлінських процесів. Крім того, вони окреслюють правила ділового етикету, охорони праці та протипожежного захисту, а також основи роботи з інформаційними технологіями, що забезпечують ефективне функціонування інфраструктурних об'єктів. У даному контексті пропонується сформувати загальну систему елементів управління та захисту об’єктів критичної інфраструктури (Рис. 1.5), що спрямовані передусім на реалізацію механізмів управління у відповідності до поточних загроз та потенційних ризиків для критичних об’єктів інфраструктури. Однією з ключових рис публічного управління критичною інфраструктурою, які стають особливо актуальними в умовах сучасних викликів, пов’язаних із війною, є суворе обмеження доступу до інформації про об'єкти критичної інфраструктури, яке здійснюється в умовах воєнного стану. Доступ надається виключно уповноваженим особам суб'єктів національної системи захисту критичної інфраструктури, що свідчить про необхідність забезпечення конфіденційності та безпеки в умовах підвищених загроз.

Крім того, реалізація державної політики у сфері захисту критичної інфраструктури покладена на міністерства та центральні органи виконавчої влади, які відповідають за різні сектори інфраструктури, що забезпечує інтеграцію зусиль національних інституцій і систематизацію підходів до управління, дозволяючи більш ефективно реагувати на виклики та загрози, які можуть виникати.

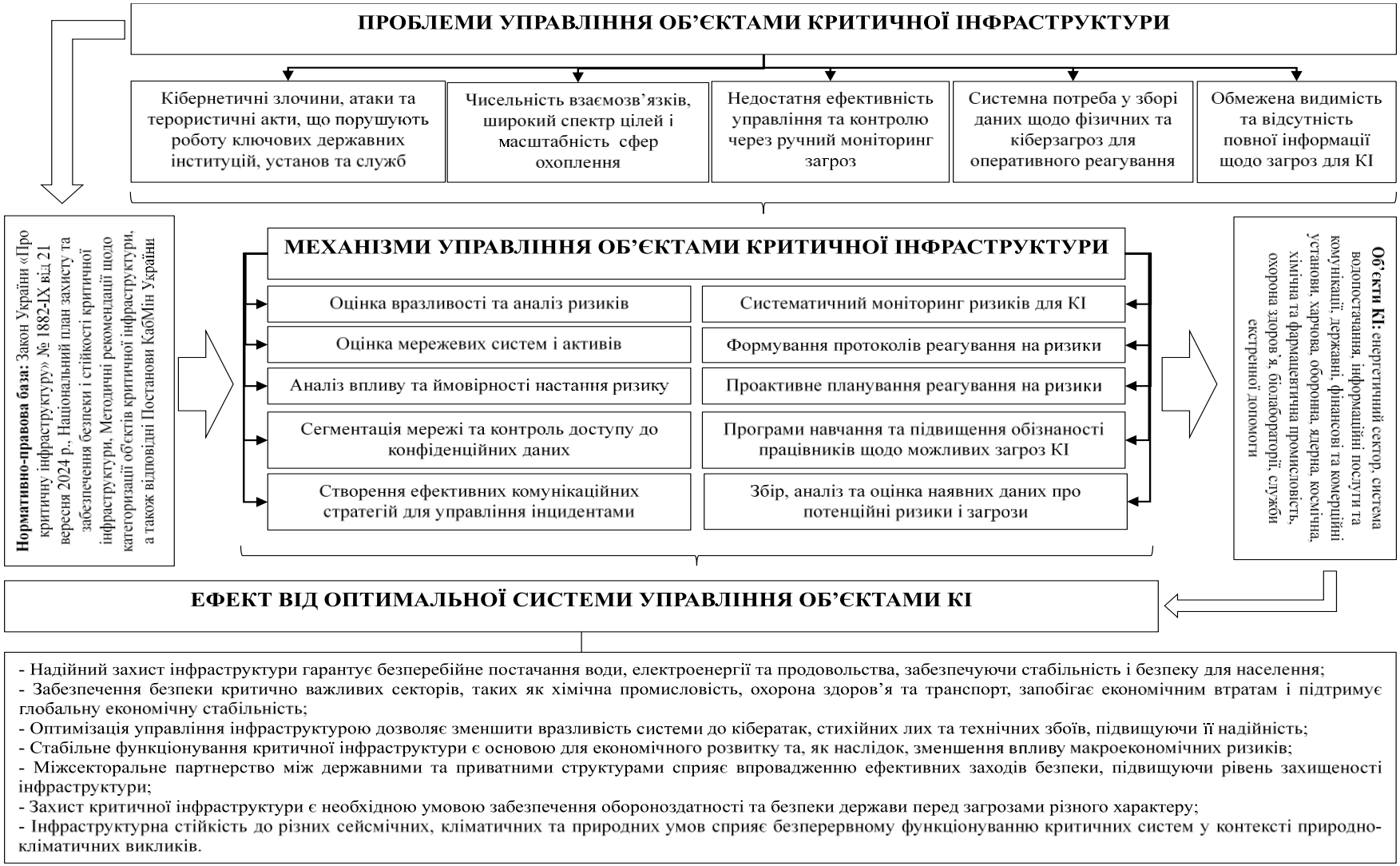


Рис. 1.5. Характеристика елементів системи управління та захисту об'єктів критичної інфраструктури

Джерело: власна розробка автора

Також спостерігається тенденція до спрощення та уніфікації регуляторних процесів, пов'язаних з об'єктами критичної інфраструктури. У рамках даного процесу здійснюється об'єднання діючих норм, правил та наказів, що регулюють захист, безпеку та надійність таких об'єктів. Важливим кроком у цьому напрямку стало створення Реєстру об'єктів критичної інфраструктури [79], який надає власникам переважне право на відновлення об'єктів, виходячи з їх критичності для життєдіяльності суспільства.

Серед найбільш важливих об'єктів можна виділити атомні електростанції, для яких функціонування реєстру передбачає створення паспортів, як містять розрахунки ресурсів, необхідних для їх захисту та відновлення, що забезпечує прозорість управлінських рішень і підвищує ефективність заходів безпеки.

Крім того, публічне управління критичною інфраструктурою передбачає розробку спеціальної моделі державного врядування, яка включає уповноважені органи та відповідальних осіб за захист, безпеку та надійність цих об'єктів. В Україні основи даної моделі закріплені в Законі «Про критичну інфраструктуру» № 1882-IX від 21 вересня 2024 р. [83], який визначає управління національною системою захисту на кількох рівнях. У даному контексті загальнодержавний рівень передбачає участь Кабінету Міністрів України, уповноважених органів, таких як Державна служба спеціального зв'язку та захисту інформації, а також інших центральних органів виконавчої влади, що відповідають за виконання законодавства. Натомість на регіональному та галузевому рівнях управління здійснюється центральними та місцевими органами виконавчої влади, які формують і реалізують державну політику у сфері захисту інфраструктури в окремих секторах. Місцевий рівень управління забезпечується місцевими органами виконавчої влади та органами місцевого самоврядування відповідно до їх повноважень. Об'єктовий рівень охоплює операторів критичної інфраструктури, які діють на основі регуляторних та нормативно-правових актів, що регулюють дану сферу.

З огляду на пріоритетні напрямки та особливості публічного управління критичною інфраструктурою в Україні слід проаналізувати сучасні можливості для управління критичною інфраструктурою за допомогою програмних рішень.

Системний підхід до впровадження таких рішень дозволяє забезпечити стабільність, надійність та безпеку критичної інфраструктури. Основні програмні рішення для моніторингу, контролю та захисту критичної інфраструктури наведено на Рис. 1.6.



Рис. 1.6. Програмні рішення для моніторингу, контролю та захисту критичної інфраструктури

Джерело: власна розробка автора

Управління критичною інфраструктурою за допомогою програмних рішень є ключовим елементом забезпечення її стабільності, надійності та безпеки. Завдяки застосуванню спеціалізованих систем моніторингу, контролю та захисту можливо не тільки ефективно керувати фізичними і цифровими активами, але й швидко реагувати на потенційні загрози. Важливим аспектом є

інтеграція комплексних програмних рішень, які охоплюють усі рівні управління інфраструктурою: від моніторингу фізичних процесів до кіберзахисту та відповідності нормативним вимогам. Таким чином, такі рішення дозволяють підвищити рівень прогнозування технічного обслуговування та попереджати можливі збої, що сприяє стійкості системи в цілому.

У міжнародному контексті, багато країн розробляють і впроваджують регуляторні рамки для управління критичною інфраструктурою. Наприклад, у США діють кілька ключових агентств, таких як Міністерство внутрішньої безпеки, Агентство з кібербезпеки та інфраструктурної безпеки (CISA) та Міністерство енергетики, які встановлюють стандарти безпеки для захисту критичних об'єктів. Важливою віхою стала Presidential Policy Directive 21, яка акцентує національну єдність у підходах до підтримки функціональної та захищеної критичної інфраструктури. Такий підхід підтверджує актуальність програмних рішень для моніторингу та захисту інфраструктури, що забезпечують стійкість до зовнішніх та внутрішніх загроз, підвищуючи загальну безпеку суспільства.

При впровадженні програмних заходів щодо захисту критичної інфраструктури також необхідно враховувати ступінь взаємозалежності національних і регіональних інфраструктурних об'єктів, оскільки ефективність безпекових заходів значною мірою залежить від координації зусиль державних регуляторів, місцевих органів влади, підприємств та громад, які контролюють ключові об'єкти, такі як енергопостачання, водопостачання, газові мережі та транспортна інфраструктура. Схему залежностей між інфраструктурними об’єктами у різних секторах економіки наведено на Рис. 1.7.

У даному контексті скоординоване управління та врахування взаємодії між різними секторами інфраструктури є ключовими для забезпечення загальної стійкості системи. Врахування взаємозалежностей дозволяє мінімізувати ризик каскадних збоїв, що полягають у відображенні впливу ускладнень в одному секторі на іншу інфраструктуру мережі взаємопов'язаних об'єктів. Зокрема, ефективне управління критичною інфраструктурою передбачає інтеграцію

заходів з моніторингу та швидкого реагування на різних рівнях: місцевому, регіональному та національному.

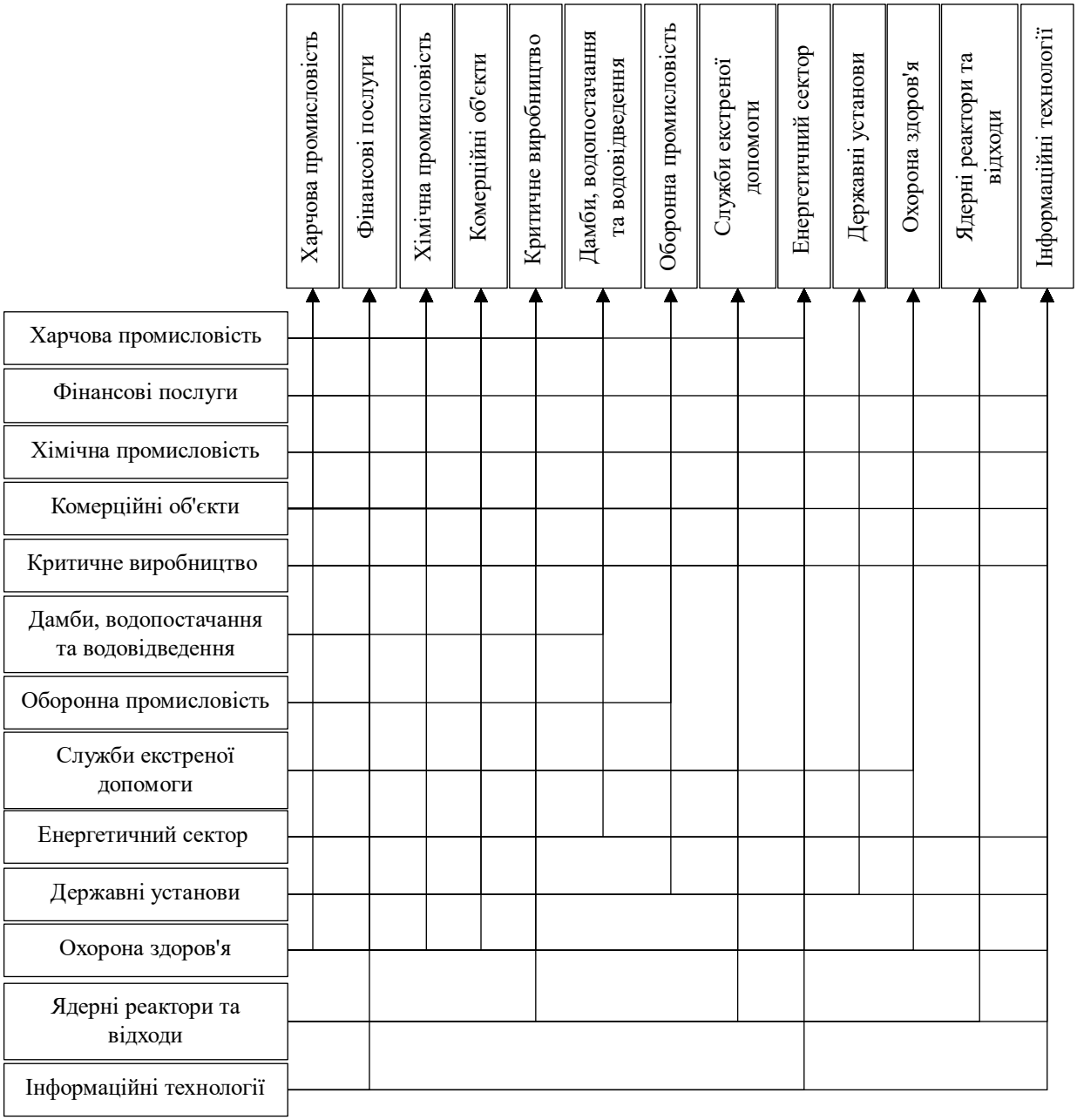


Рис. 1.7. Схема залежностей критичної інфраструктури

Джерело: власна розробка автора

Такий підхід забезпечує можливість оперативного перерозподілу ресурсів у разі загрози або надзвичайної ситуації, підвищуючи ефективність аварійних служб, безперебійність енергопостачання та функціонування транспортних мереж. Таким чином, об'єкти критичної інфраструктури відіграють фундаментальну роль у забезпеченні життєво важливих функцій держави, охоплюючи такі сфери, як енергетика, транспорт, охорона здоров'я, комунікації

та безпека. Їх функціонування є ключовим для підтримки стабільності суспільних процесів, економічної безпеки та захисту національних інтересів. Управління такими об'єктами вимагає комплексного підходу, що передбачає скоординовані дії державних і приватних суб'єктів, застосування системи планування, регулювання, координації та контролю. Водночас управління об'єктами критичної інфраструктури повинно враховувати їхні особливості, зокрема високий рівень залежності від зовнішніх факторів, що зумовлює необхідність підвищеної уваги до безпеки, стійкості та адаптивності в умовах кризових ситуацій.

1.4. Нормативно-правове забезпечення публічного управління у сфері трансформації об’єктів критичної інфраструктури

Сьогодні критична інфраструктура, особливо в умовах війни, відіграє ключову роль у забезпеченні функціонування економіки, соціальної стабільності та національної безпеки, адже включає в себе життєво важливі об’єкти в таких сферах, як енергетика, транспорт, охорона здоров’я, інформаційні технології та комунікації. Публічне управління критичними інфраструктурними об'єктами в сучасних умовах глобалізації характеризується значною інтеграцією між різними секторами, зокрема, постачальними ланцюгами, транспортними, енергетичними, інформаційними та технологічними системами. Така взаємозалежність створює додаткові ризики для їх функціонування, оскільки будь-які кризові події (наприклад, перебої з електроенергією, газом, водою або телекомунікаціями) можуть мати далекосяжні наслідки. Відповідно, на міжнародному рівні можна спостерігати активізацію процесів спрямованих на інвестування в заходи щодо забезпечення стійкості критичної інфраструктури та забезпечення її функціонування на всіх етапах життєвого циклу. Натомість в Україні, незважаючи на критичну важливість зазначеної проблеми, системний підхід до збільшення інвестицій у стійкість інфраструктури поки що не має належного розвитку. Однак, український уряд активно залучає кошти міжнародних

організацій та партнерів, особливо на тлі війни, що триває, та загострення проблем у функціонуванні ключових інфраструктурних систем [53].

Основою для створення системи захисту об’єктів критичної інфраструктури, доцільно, на нашу думку, вважати Концепцію створення державної системи захисту критичної інфраструктури, прийняту Розпорядженням Кабінету Міністрів України від 06.12.2017 р. № 1009-р (далі - Концепція) [88]. Згідно даної Концепції одним з пріоритетів реформування органів сектору оборони і безпеки України було визначено створення системи захисту критичної інфраструктури. При цьому серед основних проблем, які потребували свого належного розв’язання Концепцією зазначались такі, як: 1) відсутність єдиної системи захисту критичної інфраструктури; 2) недостатність та неузгодженість нормативно-правового регулювання з питань захисту систем і об’єктів критичної інфраструктури; 3) відсутність державного органу, відповідального за координації дій у сфері захисту критичної інфраструктури; 4) невизначеність повноважень державних органів у сфері захисту критичної інфраструктури, правового статусу власників (розпорядників) об’єктів критичної інфраструктури; 5) відсутність методології віднесення об’єктів до об’єктів критичної інфраструктури, порядку їх паспортизації та категоризації; 6) відсутність методології проведення оцінки можливих загроз критичній інфраструктурі; 7) нерозвиненість державно-приватного партнерства у сфері захисту критичної інфраструктури; 8) невизначеність джерел фінансування заходів щодо захисту критичної інфраструктури; 9) недостатній рівень міжнародного співробітництва у сфері захисту критичної інфраструктури [88].

Основним документом що визначає правові та організаційні засади створення та функціонування національної системи захисту критичної інфраструктури, є Закон України «Про критичну інфраструктуру» № 1882-IX від 21 вересня 2024 р. [83]. Даний Закон закріплює ключові принципи, на яких базується система управління об'єктами критичної інфраструктури, а також встановлює механізми їх захисту в умовах загроз національній безпеці. Норми та положення в рамках даного Закону підкріплюються іншими нормативно-правовими актами, зокрема Постанова КабМін від 24.09.2024 № 1109 «Деякі

питання об’єктів критичної інфраструктури» [23], Постанова КабМін від 14.10.2022 № 1175 «Деякі питання подання інформації у сфері захисту критичної інфраструктури» [26] тощо, для забезпечення комплексного підходу до управління об'єктами критичної інфраструктури, оптимізації процесів їх захисту, моніторингу безпеки та ефективної взаємодії між державними органами, приватними підприємствами та іншими учасниками системи. Такий підхід до формування правового забезпечення зумовлює ефективність системи, спрямованої на підвищення стійкості критичної інфраструктури, її адаптацію до мінливих умов зовнішнього середовища та реалізацію стратегічних цілей держави в сфері безпеки та розвитку критичної інфраструктури.

У свою чергу, затверджений у 2023 році, Національний план захисту та забезпечення безпеки і стійкості критичної інфраструктури [97] є програмним документом, що окреслює довгострокові цілі державної політики у цій сфері. У ньому детально визначено функціональні обов'язки суб'єктів національної системи захисту критичної інфраструктури, зокрема щодо моніторингу стану безпеки, оцінки рівня ризиків та впровадження превентивних заходів. План передбачає також створення ефективних механізмів управління ризиками, що базуються на системі прогнозування загроз, аналізі вразливих місць та розробці відповідних заходів реагування. Важливим аспектом визначеного плану є впровадження інтегрованої системи координації дій між усіма зацікавленими сторонами, включно з органами державної влади, суб’єктами захисту та операторами критичної інфраструктури. Особлива увага приділяється створенню механізмів обміну інформацією, зокрема щодо потенційних загроз та можливих наслідків порушення функціонування критичних об'єктів, що сприяє формуванню єдиної платформи для прийняття рішень, що дозволяє швидко та ефективно реагувати на виникаючі виклики. Основними законодавчими актами, що регулюють захист критичної інфраструктури (Таблиця 1.3):

1. Закон України «Про критичну інфраструктуру» № 1882-IX від 21 вересня 2024 р.

2. Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 «Деякі питання об’єктів критичної інфраструктури» (в редакції постанови Кабінету Міністрів України від 16 грудня 2022 р. № 1384)

3. Постанова Кабінету Міністрів України від 22 липня 2022 р. № 821 «Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури»

4. Постанова Кабінету Міністрів України від 14 жовтня 2022 р. № 1174 «Про затвердження Регламенту обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури»

5. Постанова Кабінету Міністрів України від 14 жовтня 2022 р. № 1175 «Деякі питання подання інформації у сфері захисту критичної інфраструктури»

6. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 № 23 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури».

Окремим пунктом варто згадати захист критичної інфраструктури в питаннях інформаційної та кібербезпеки.

Крім того, забезпечення безпеки та захисту інформації, що стосується об'єктів критичної інфраструктури, є одним із ключових аспектів публічного управління. В Україні дані питання регулюються рядом законодавчих актів, зокрема Закон України «Про інформацію» № 2657-XII від 27 липня 2023 р. [82], «Про державну таємницю» № 638-IV від 28 квітня 2023 р. [76] тощо. В умовах зростання кількості кібератак та інших видів кіберзлочинності, що включають витоки інформації про місце розташування критично важливих об’єктів, питання інформаційної безпеки набувають особливої актуальності.

У контексті захисту інформації, уповноважені органи державної влади, зокрема Державна служба спеціального зв’язку та захисту інформації України, виконують заходи з технічного захисту інформаційних та телекомунікаційних систем. Їх діяльність охоплює організацію проведення експертизи комплексних систем захисту інформації в межах своїх компетенцій та сфер управління.

Таблиця 1.3

Нормативно-правова база для забезпечення ефективності публічного управління об’єктами критичної інфраструктури

Нормативно-правові акти	Характеристика
Закон України «Про критичну інфраструктуру» № 1882-IX від 21 вересня 2024 р. [83]	Визначає правові та організаційні засади створення та функціювання національної системи захисту КІ і є складовою законодавства у сфері національної безпеки.
Постанова Кабінету Міністрів України від 24 вересня 2024 р. № 1109 «Деякі питання об’єктів критичної інфраструктури» (в редакції постанови Кабінету Міністрів України від 16 грудня 2022 р. № 1384) [23]	Затверджує механізм віднесення об’єктів до КІ та їх категоризації.
Постанова Кабінету Міністрів України від 22 липня 2022 р. № 821 «Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури» [80]	Затверджує механізм проведення моніторингу рівня безпеки об’єктів КІ та його періодичність.
Постанова Кабінету Міністрів України від 14 жовтня 2022 р. № 1174 «Про затвердження Регламенту обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури» [79]	Затверджує механізм інформаційної взаємодії між суб’єктами національної системи захисту КІ з метою забезпечення захисту та стійкості КІ.
Постанова Кабінету Міністрів України від 14 жовтня 2022 р. № 1175 «Деякі питання подання інформації у сфері захисту критичної інфраструктури» [26]	Затверджує методологію та закріплює типову форму річного звіту про виконання секторальним органом повноважень та форму річного звіту про виконання оператором КІ повноважень, визначених у ЗУ «Про критичну інфраструктуру» № 1882-IX від 21 вересня 2024 р.
Постанова Кабінету Міністрів України від 28 квітня 2023 р. № 415 «Про затвердження Порядку ведення Реєстру об’єктів критичної інфраструктури, включення таких об’єктів до Реєстру, доступу та надання інформації з нього» [79]	Затверджує процедури формування і ведення Реєстру об’єктів КІ та їх включення до даного реєстру, внесення до нього інформації про об’єкти КІ та їх виключення, доступу та надання інформації з зазначеного реєстру.
Постанова Кабінету Міністрів України від 4 серпня 2023 р. № 818 «Деякі питання паспортизації об’єктів критичної інфраструктури» [25]	Затверджує вимоги до розроблення оператором КІ паспорта безпеки на об’єкт КІ та його складових, а також механізм його погодження секторальними і функціональними органами у сфері захисту КІ.
Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 № 23 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури» [77]	Затверджує Методичні рекомендації щодо категоризації об'єктів КІ, що розроблені на виконання вимог ЗУ «Про критичну інфраструктуру» № 1882-IX від 21 вересня 2024 р. та п. 5 Методики категоризації об'єктів КІ, затвердженої постановою Кабінету Міністрів України № 1109 від 24 вересня 2024 року.
Національний план захисту та забезпечення безпеки і стійкості критичної інфраструктури [78]	Визначає стратегічні цілі, повноваження Міністерств, Адміністрації Державної служби спеціального зв’язку та захисту інформації та місцевих органів самоврядування щодо безпеки та стійкості КІ.

Джерело: власна розробка автора

Особливу роль у законодавчому забезпеченні кібербезпеки відіграє Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 28 червня 2024 р. [84] у якому об’єкти критичної інфраструктури, зокрема комунікаційні та інформаційні системи у сфері електронного урядування, офіційно визнані об’єктами кібербезпеки та кіберзахисту. У даному контексті заходи, висвітлені у Стратегії кібербезпеки України, затвердженої Указом Президента України № 447/2021 від 26 серпня 2021 р. [87], включають протидію конкретним загрозам, що можуть виникати у кіберпросторі. Серед них, слід виокремити, інформаційну та кібервійну росії щодо українських систем, інституцій на інфраструктурних об’єктів в цифровій сфері, кіберзлочинність, а також організовані кібератаки, і використання кіберпростору іншими терористичними організаціями.

Значне місце цьому безпековому напрямку відведене в нормах чинного законодавства України, де він визнаний пріоритетним у контексті політики національної безпеки. Постанова Кабінету Міністрів України “Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури” від 19.06.19 р. № 518; Постанова Кабінету Міністрів України “Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимогу щодо захисту якої встановлено законом” від 11.11.20 р. № 11; Постанова Кабінету Міністрів України “Про затвердження Методичних рекомендацій щодо категоризації об’єктів критичної інфраструктури від 9.10.20 р. № 1109. Додатково, слід відобразити нормативно правову базу, що регулює питання кібербезпеки у процесі забезпечення ефективності публічного управління об’єктами критичної інфраструктури (Таблиця 1.4).

Таблиця 1.4

Нормативно-правові акти, що регулюють питання кібербезпеки у процесі забезпечення ефективності публічного управління об’єктами критичної інфраструктури

Нормативно-правові акти	Характеристика
Закон України «Про боротьбу з тероризмом» № 638-IV від 28 квітня 2023 р. [75]	Визначає правові та організаційні основи боротьби з тероризмом повноваження і обов'язки виконавчої влади та зацікавлених сторін, порядок координації їх діяльності. Закон зобов'язує органи влади та операторів КІ здійснювати заходи для виявлення та нейтралізації терористичних загроз, що підвищує захист таких об'єктів від терористичних атак.
Закон України «Про державну таємницю» № 3855-XII від 1 січня 2024 р. [76]	Регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України. Він встановлює режим секретності для інформації, яка може бути використана для нанесення шкоди об’єктам КІ, обмежуючи доступ до конфіденційних даних, що підвищує їхню захищеність від диверсій і кібератак.
Закон України «Про інформацію» № 2657-XII від 27 липня 2023 р. [82]	Регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. Закон обмежує доступ до інформації про характеристики та заходи захисту КІ, водночас забезпечуючи право громадян на доступ до загальної інформації про діяльність цих об’єктів та їхній вплив на суспільство й довкілля.
Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 28 червня 2024 р. [84]	Визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі. Зокрема, Закон забезпечує правове підґрунтя для захисту кіберпростору, де функціонує КІ.
Положення «Про Положення про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України» № 379/99 від 11 червня 2022 р. [85]	Регулює діяльність Антитерористичного центру, який відповідає за координацію боротьби з тероризмом, включно із захистом КІ від терористичних загроз. Центр розробляє та впроваджує заходи щодо захисту стратегічних об'єктів, які можуть стати цілями диверсійних або терористичних актів.
Указ Президента України від 21.07.2001 № 1001/98 «Про Положення про робочу групу з проведення реформи місцевих органів виконавчої влади, органів місцевого самоврядування та державної служби» [86]	Затверджує вимоги до робочої групи з проведення реформи місцевих органів виконавчої влади, органів місцевого самоврядування та державної служби. Зокрема, реформування спрямоване на покращення взаємодії між місцевими та державними структурами, що відповідають за безпеку об'єктів КІ, і створення умов для швидкого реагування на загрози.
Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021 [87]	Стратегія визначає комплексний підхід до захисту національного кіберпростору, включаючи об’єкти КІ. Вона передбачає реалізацію заходів для виявлення, запобігання і реагування на кіберзагрози, які впливають на роботу таких об’єктів, а також розвиток національної системи кіберзахисту для забезпечення стійкості та безперервності функціонування КІ.

Джерело: власна розробка автора

У даному контексті законодавством передбачається визначення правових та організаційних аспектів створення, зберігання та передачі конфіденційних та державно-значущих документів, а також захист інформаційних систем та електронних носіїв від кіберзагроз, зокрема у контексті триваючої на тлі бойових дій інформаційної та кібервійни росії проти українських критично важливих об’єктів (інституцій, служб, банківської системи, тощо).

Загалом, незважаючи на велику кількість нормативних документів, в Україні спостерігається відсутність єдиного та чітко визначеного підходу до класифікації загроз, які впливають на критичну інфраструктуру, що ускладнює процес планування та реалізації ефективних заходів щодо її захисту. Зокрема, у Концепції створення державної системи захисту критичної інфраструктури [88], чітко окреслюються основні загрози, які можуть загрожувати цій сфері. Зокрема, акцентується увага на загрозах природного та техногенного характеру, а також на протиправних діях та їх комбінаціях, які можуть призвести до серйозних наслідків для національної безпеки.

Відповідно до положень Стратегії кібербезпеки України, затвердженої Указом Президента України від № 447/2021 26 серпня 2021 р. [87] забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Серед передумов та чинників, що формують загрози кібербезпеці України, Стратегія кібербезпеки України називає: недосконалість нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації; відсутність у значної частини державних органів відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом, здійснення фінансування робіт із кіберзахисту за залишковим принципом; відсутність механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності держави; невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців з питань кібербезпеки та кіберзахисту, зокрема неефективні механізми їх стимулювання до роботи в державному секторі; незавершеність заходів з упровадження організаційно-технічної моделі

кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки; недостатню захищеність від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури; невідповідність вимогам законодавства стану захисту інформаційно-комунікаційних систем державних органів та суб'єктів господарювання, в яких обробляється значна частина інформації з обмеженим доступом [24].

Крім того, Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 28 червня 2024 р. [84], виділяє «кіберзагрози» як окрему категорію загроз для критичної інфраструктури. Даний нормативно-правовий акт вказує на необхідність врахування специфіки кіберзагроз у контексті загального захисту критичної інфраструктури, що підкреслює важливість інтеграції кібербезпеки в стратегії її захисту.

У свою чергу Стратегія кібербезпеки України, затверджена Указом Президента України № 447/2021 від 26 серпня 2021 року [87], зазначає конкретні загрози, що можуть виникати у кіберпросторі. Серед них виділяються агресивні дії російської федерації щодо України в цифровій сфері, кіберзлочинність, а також організовані кібератаки, спонсоровані державами, і використання кіберпростору терористичними організаціями. Така класифікація загроз вказує на необхідність системного підходу до забезпечення безпеки критичної інфраструктури, що має включати не лише технічні, але й правові та організаційні аспекти.

Принципи класифікації загроз критичній інфраструктурі включають системність та комплексність, враховуючи природні, техногенні, людські й кіберзагрози. У даному контексті аналіз причинно-наслідкових зв'язків допомагає зрозуміти взаємозалежність між різними видами загроз, наприклад, між техногенними аваріями й людськими помилками. Тому акцент робиться на сучасних викликах, зокрема на кіберзагрозах, що відображається у законодавстві України. Класифікації також повинні бути адаптивними до змін у геополітичній ситуації й технологічному розвитку [15].

У контексті національної безпеки та викликів, що постають перед сучасним суспільством, важливо використовувати системний підхід до вирішення питань, пов’язаних із захистом інфраструктурних об’єктів. Встановлення чітких критеріїв та порядок віднесення об’єктів до критичної інфраструктури слугує первинним етапом у розробці ефективної системи їх захисту. Основним критерієм захисту є визнання того, що порушення стабільного функціонування одного об’єкта критичної інфраструктури призводить до серйозних наслідків, таких як надзвичайні ситуації або негативні впливи на екологічну, енергетичну, економічну, фінансову безпеку, а також на обороноздатність держави.

У даному контексті відповідно до вимог Закону України «Про критичну інфраструктуру» № 1882-IX від 21 вересня 2024 р. [83], Міністерство розвитку громад, територій та інфраструктури України на базі постанови КабМін «Деякі питання щодо ідентифікації та категоризації об’єктів критичної інфраструктури» № 1109-2020-п від 24 вересня 2024 р. [23] ініціювало формування Робочої групи, що має на меті ідентифікацію та категоризацію об’єктів критичної інфраструктури. Відповідно до зазначеного наказу, Мінінфраструктури визначено як секторальний орган, відповідальний за захист критичної інфраструктури, що підкреслює важливість та стратегічний характер його діяльності у цій сфері. Слід зазначити, що до інших секторальних органів входять Міненерго, Мінцифри, Мінфін, Мінекономіки, Мінстратегпром, Мінінфраструктури, МОЗ, МВС, НСЗУ та НКЦПФР. Крім того, даний документ також затверджує Положення про Робочу групу [86], в якому визначаються її функції та склад.

З огляду на постанову КМУ «Деякі питання оптимізації системи центральних органів виконавчої влади» № 29-2023-п від 8 березня 2023 р. [24], Міністерство розвитку громад і територій зазнало реорганізації, що включала його інтеграцію до Міністерства розвитку громад, територій та інфраструктури України. У результаті такої реорганізації Мінінфраструктури стало провідним органом серед центральних органів виконавчої влади, відповідальним за

розробку та реалізацію державної політики у сфері захисту критичної інфраструктури, що стосується не лише загальних принципів безпеки, а й специфічних аспектів, таких як забезпечення функціонування сектора «системи життєзабезпечення».

Крім того, слід зазначити, що переліки об’єктів критичної інфраструктури, які належать до типу основних послуг у сфері «системи життєзабезпечення», були затверджені постановою КабМін «Про затвердження Порядку ведення Реєстру об’єктів критичної інфраструктури, включення таких об’єктів до Реєстру, доступу та надання інформації з нього» № 415-2023-п від 28 квітня 2023 р. [79], що свідчить про системний підхід держави до ідентифікації та категоризації таких об’єктів, що є необхідним для формування ефективної стратегії їх захисту і підтримки стійкості в умовах сучасних викликів та загроз.

З метою реалізації ефективних заходів з охорони об'єктів критичної інсфраструктури необхідно оцінити їх значущість для надання критично важливих послуг у всіх секторах економіки, що дозволить тимчасово вжити заходів для запобігання кризовим ситуаціям і забезпечити стійкість інфраструктури до поточних загроз. Інтеграція цих заходів у державну політику не тільки підвищує рівень національної безпеки, а й зміцнить довіру громадськості до державних інститутів, які відповідають за забезпечення життєво важливих функцій суспільства. У контексті актуальності трансформації об’єктів критичної інфраструктури в сучасних умовах було сформовано схему процесу управління ідентифікацією та категоризацією об'єктів критичної інфраструктури на рівні держави, що наведена на рис. 1.8.

Також згідно з Методичними рекомендаціями, що стосуються категоризації об'єктів критичної інфраструктури [77] визначаються права і обов'язки робочої групи з ідентифікації та категоризації об'єктів критичної інфраструктури, що наведені на Рис. 1.9. Процес, який здійснюється робочою групою для визначення об’єктів як критичної інфраструктури та їх подальшої категоризації, починається з того, що всі об’єкти, які підпадають під I, II, III та IV категорії критичності, вносяться до відповідного галузевого реєстру [23].

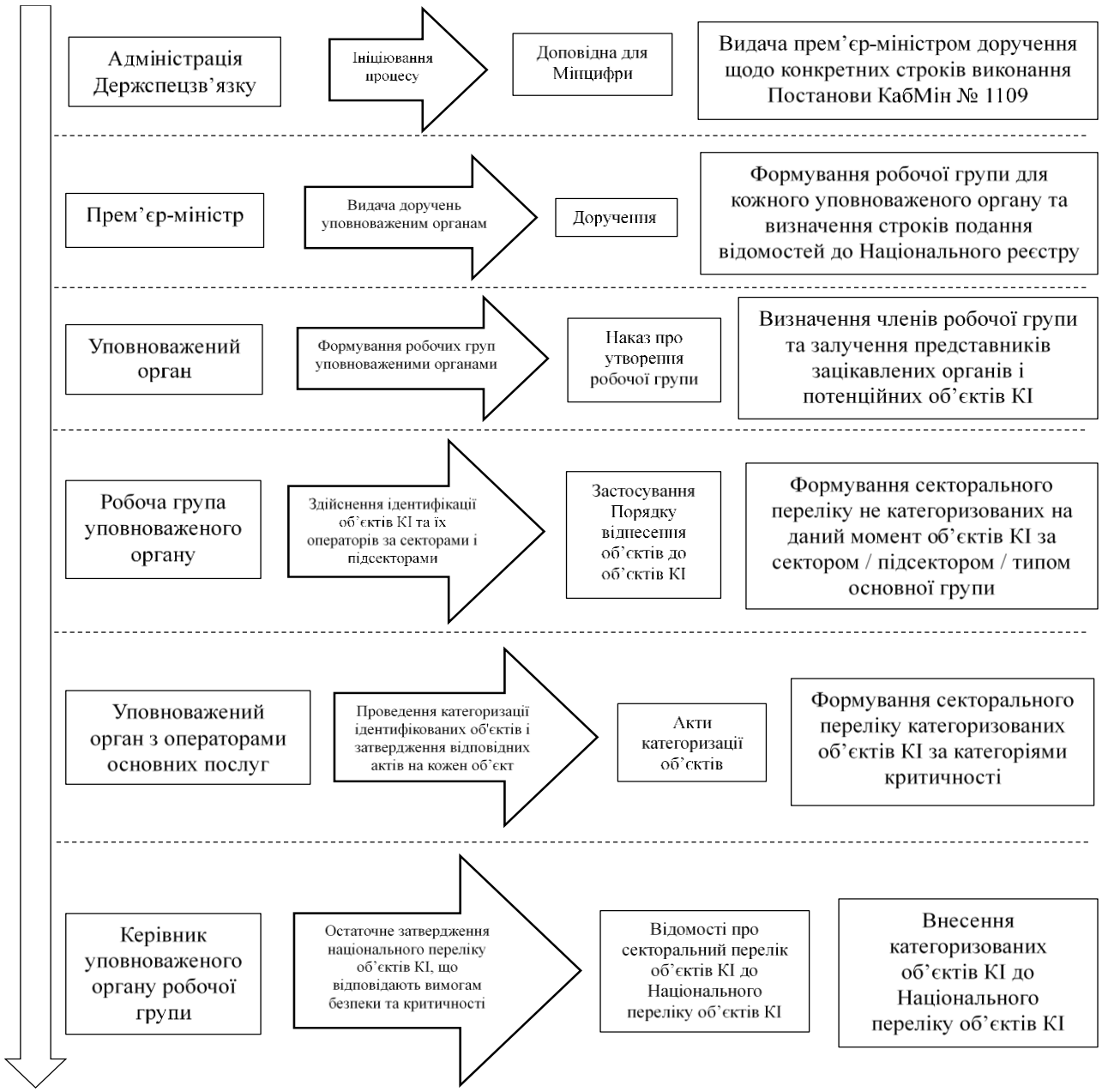


Рис. 1.8. Схема процесу управління ідентифікацією та категоризацією об'єктів критичної інфраструктури на рівні держави

Джерело: сформовано автором на основі [77].

Уповноважений орган на основі наявної інформації про об'єкти критичної інфраструктури, які перебувають під його контролем або у його володінні, а також спираючись на дані, надані операторами ключових послуг у відповідному секторі чи підсекторі, має забезпечувати постійне оновлення та підтримку актуального стану даного реєстру згідно з вимогами, визначеними пунктом 6

Порядку, ухваленого Постановою Кабінету Міністрів України № 1109-2020-п від 24 вересня 2024 р. [23].

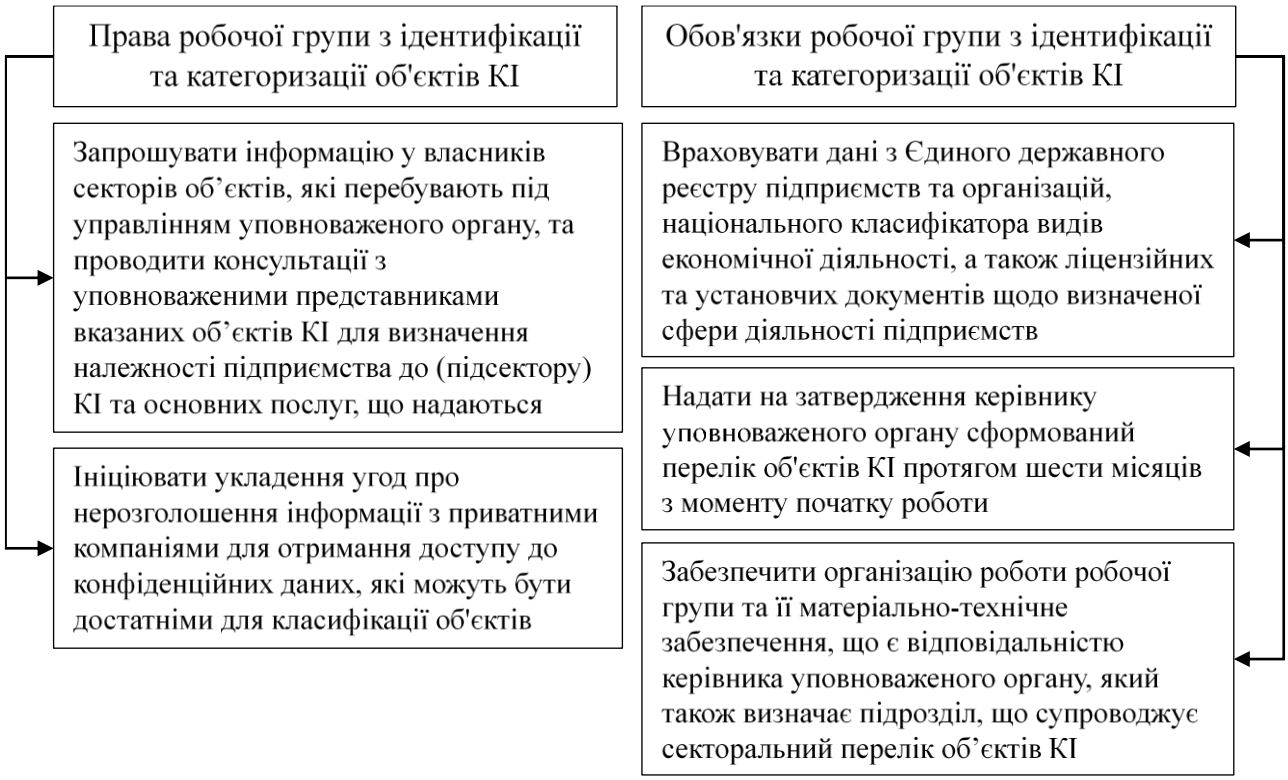


Рис. 1.9. Права і обов'язки робочої групи з ідентифікації та категоризації об'єктів критичної інфраструктури

Джерело: сформовано автором на основі [77].

По-друге, об’єкти критичної інфраструктури в секторальному переліку мають бути класифіковані за категоріями критичності, що дозволяє оптимізувати управлінські рішення щодо їх захисту та функціонування. Керівник уповноваженого органу несе пряму відповідальність за визначення підрозділу, відповідального за формування та супроводження даного переліку.

Крім того, уповноважений орган зобов'язаний отримувати та належним чином інформацію про облік, що дозволяє ідентифікувати об'єкти як критичну інфраструктуру, а також дані, що підтверджують їх категоризацію. Регулярне оновлення секторного переліку, яке передбачає кожні два роки або у разі значних змін у критичній інфраструктурі, таких як створення, модернізація або закриття

об’єктів, є невід’ємною частиною забезпечення безпеки та ефективності функціонування об’єктів критичної інфраструктури.

Таким чином, рівень критичності кожного інфраструктурного об'єкта визначається через детальне дослідження його характеристик, функціональних можливостей, а також приналежності до мережі залежностей, які існують як у звичайному робочому режимі, так і в умовах збоїв чи тимчасової зупинки функціонування. Проаналізований процес управління ідентифікацією та категоризацією об'єктів критичної інфраструктури дозволив сформувати основні завдання в рамках захисту та забезпечення стійкості КІ, що наведено на Рис. 1.10.

При формуванні пріоритетних процесів і завдань основні етапи здійснення ідентифікації було збережено у відповідності до сучасного законодавства України. Проте, з огляду на те, що при аналізі критичності робоча група може зосереджувати увагу як на окремих аспектах можливих наслідків, так і на комплексній оцінці потенційних ризиків; вважаємо, що для більшої точності у визначенні критичних об’єктів, необхідно адаптувати загальні концепції критичності до специфічних фізичних, системних та просторових особливостей інфраструктурних об’єктів, які досліджуються. Такий підхід сприяє розробці чітких та інтегрованих критеріїв оцінки, які враховують ключові загрози безпеки і відповідають мінімально допустимим стандартам. Отже, результатом ідентифікаційного процесу є формування переліку об’єктів критичної інфраструктури на місцевому рівні, який може бути оприлюднений для ознайомлення громадськості через офіційний веб-сайт або місцеві ЗМІ.

Включення об'єкта до даного переліку зумовлює особливі вимоги до його управління з боку місцевих органів та власників, що відповідає загальносвітовій практиці, де діяльність таких об’єктів регулюється відповідно до спеціально розробленої стратегії розвитку, яка узгоджується з основними цілями підприємства.

Другий етап реалізації системи управління критичною інфраструктурою спрямований на захист об’єктів КІ. На цьому етапі першочерговим завданням є діагностика елементів об’єктів критичної інфраструктури, зокрема їхньої

вразливості, зносостійкості, впливу на продуктивність, безперервність функціонування та інші показники, характерні для конкретного сектора інфраструктури.

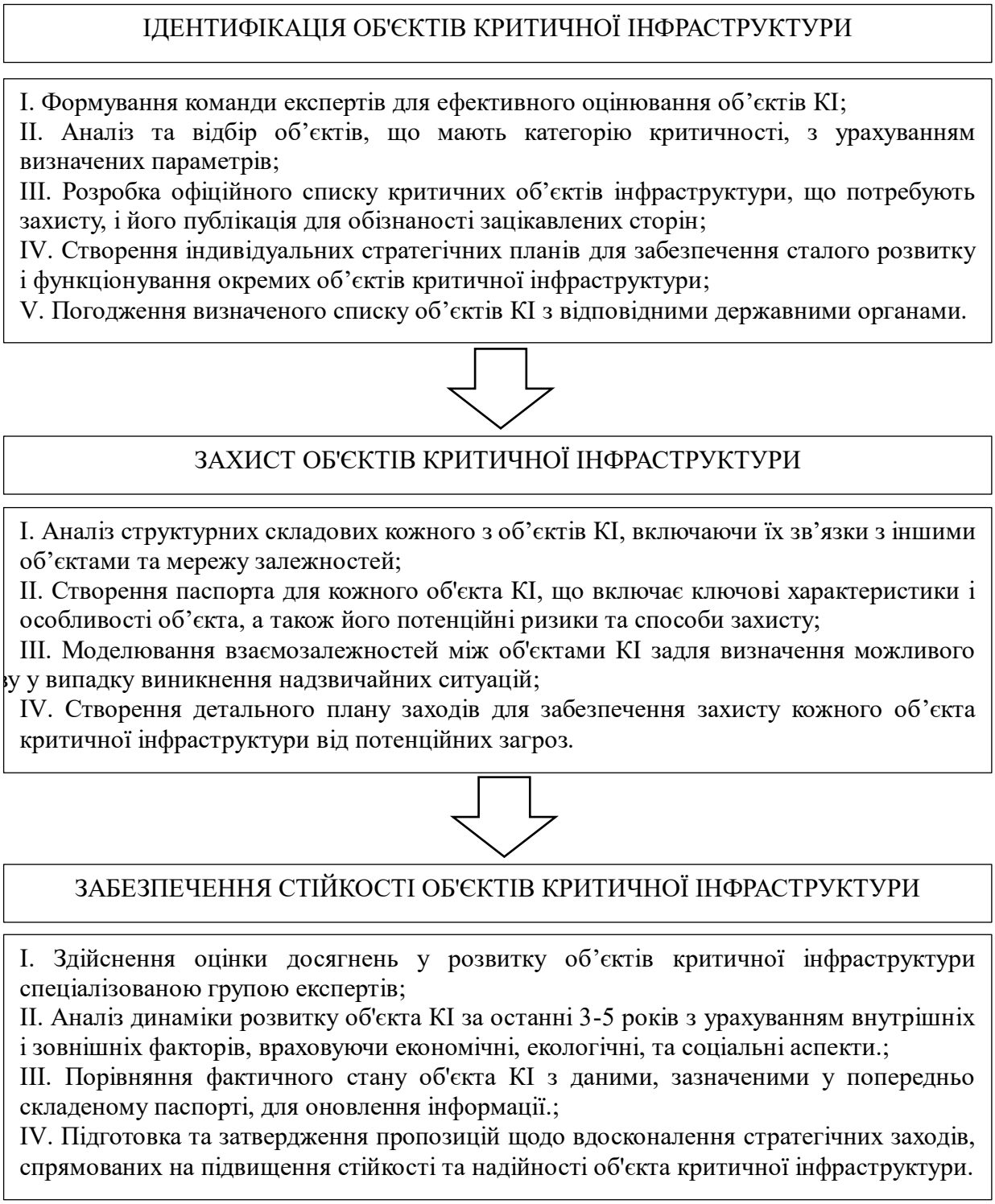


Рис. 1.10. Система управління об’єктами критичної інфраструктури*

*Джерело: власна розробка автора

Виявлені елементи, з урахуванням взаємозв'язків і взаємозалежностей, розподіляються за пріоритетністю уваги: елементи, що потребують особливої уваги; елементи, що потребують уваги; та елементи, яким достатньо періодичної уваги. Результати дослідження заносяться до паспорту об'єкта критичної інфраструктури, який містить інформацію про ризикові елементи та заходи з антитерористичної захищеності для запобігання надзвичайним ситуаціям і загрозам громадській безпеці. На основі даного документу створюються подальші стратегічні та проміжні плани та заходи щодо захисту об’єктів критичної інфраструктури; а також забезпечується чітка координація та відповідальність при реагуванні на критичні ситуації та у протидії терористичним загрозам.

Останній етап реалізації системи управління критичною інфраструктурою є забезпечення стійкості об'єктів цієї інфраструктури, що полягає в розвитку потенціалу для підготовки до запобігання та адекватного реагування на можливі загрози. У рамках цього етапу для забезпечення об'єктивності та дієвості стратегії розвитку конкретного об'єкта критичної інфраструктури важливим є проведення комплексного зовнішнього обстеження його складових елементів. В результаті цього процесу робоча група формулює обґрунтовані пропозиції щодо коригування або вдосконалення стратегії розвитку досліджуваного об'єкта, орієнтуючись на виявлені слабкі місця та можливості для підвищення ефективності. Реалізація розробленої стратегії здійснюється шляхом виконання конкретних заходів, передбачених дорожньою картою, що детально описує кроки та терміни виконання запланованих дій. На підставі отриманих результатів робоча група формулює відповідні рекомендації до стратегії розвитку досліджуваного об’єкта. Реалізація стратегії розвитку буде здійснюватися шляхом виконання окремих заходів, які передбачені дорожньою картою, у відповідності до раніше визначених принципів управління критичною інфраструктурою. Даний процес координується робочою групою, до складу якої можуть входити представники регуляторних органів національного рівня, а також фахівці з професійних об’єднань, що сприяє інтеграції різних експертних

думок та забезпеченню комплексного підходу до управління критичною інфраструктурою.

Таким чином, у сучасному контексті глобалізації та збройної агресії, що триває, стратегії трансформації об'єктів критичної інфраструктури України мають суттєве значення для забезпечення національної безпеки. Ефективне управління цими об'єктами передбачає інтеграцію новітніх технологій, модернізацію систем безпеки, а також активну координацію між різними секторами, такими як цивільний захист, антитероризм та кібербезпека. Системний підхід до інвестування в стійкість критичної інфраструктури є актуальним, особливо в умовах наростаючих загроз з боку терористичних актів та кібератак. Тому при розробці державної політики важливо зосередити зусилля на розвитку комплексних стратегій, які включають координацію дій між державними органами, міжнародними партнерами та приватним сектором, для забезпечення безперервного функціонування критичної інфраструктури в умовах невизначеності.

З огляду на посилення євроінтеграційних заходів, важливо забезпечити належне правове регулювання для підвищення стійкості критичної інфраструктури у відповідності до європейських стандартів, що сприятиме адаптації українських норм до вимог Європейського Союзу та зміцненню захисту таких об’єктів перед загрозами, що включає розробку національних нормативних актів, які узгоджуються з Директивою ЄС (NIS2) [208] щодо стійкості критично важливих об'єктів, зокрема до кібернетичних ризиків, що набула чинності 17 жовтня 2024 року. Проаналізувавши основні положення Директиви ЄС щодо стійкості критично важливих об’єктів було сформовано ряд заходів для зміцнення української інфраструктурної безпеки в умовах війни та відповідно до норм та вимог ЄС в рамках євроінтеграції. Перш за все, в Україні слід прийняти національну стратегію для забезпечення захисту критичної інфраструктури. Дана стратегія має включати детальні інструкції для ідентифікації суб’єктів, що відіграють життєво важливу роль для суспільства та економіки, ураховуючи ризики природного, техногенного та антропогенного характеру.

По-друге, необхідним є створення системних процедур оцінки ризиків, які включають систематичний аналіз потенційних загроз для ідентифікації критичних об’єктів та організацій, що надають основні послуги. Доцільним є впровадження тих методологій, які відповідають міжнародним стандартам і враховують, крім внутрішніх, міжсекторальні та транскордонні загрози. Крім того, важливо зобов'язати критично важливі суб’єкти проводити власну оцінку ризиків, яка охоплюватиме технічні, безпекові та організаційні аспекти. Згідно з цим аналізом, суб’єкти повинні вживати відповідні заходи для посилення своєї стійкості, зокрема підготовки до сповіщення державних органів у разі інцидентів. Також рекомендується створити національну базу даних, що міститиме інформацію про ключові інфраструктурні об’єкти, з регулярним оновленням даних про їхній статус і рівень загроз. У даному контексті Державні органи України мають сприяти підвищенню стійкості критичних суб’єктів, надаючи їм технічну та методичну підтримку, що включає фінансові інструменти, консультації та спільні навчальні заходи для перевірки стійкості об’єктів у випадку потенційних криз.

По-третє, необхідним є включення рекомендацій Європейської комісії щодо транскордонного обміну найкращими практиками до українського контексту та залучення українських представників до участі у спільних навчаннях та тренінгах для забезпечення координації з іншими державами та посилення здатності до протистояння міждержавним загрозам. Зокрема, за умови долучення України до групи стійкості критичних суб’єктів (CERG) заснована Директивою можливо активізувати співпрацю між державами-членами та з Комісією. Така взаємодія включає обмін інформацією та передовою практикою з питань, що стосуються стійкості критичної інфраструктури та критичних об’єктів.

Таким чином, на основі заходів, визначених Директивою ЄС щодо стійкості критично важливих об’єктів, було сформовано перелік пріоритетних напрямків удосконалення правового забезпечення публічного управління у сфері трансформації об’єктів критичної інфраструктури, що наведено у Таблиці 1.5.

Таблиця 1.5

Пріоритетні напрямки удосконалення правового забезпечення публічного управління об’єктами критичної інфраструктури

Напрямок	Характеристика
Оновлення оцінок ризиків з урахуванням поточних загроз	Адаптація національні оцінки ризиків для критичної інфраструктури, беручи до уваги сучасні виклики, включаючи потенційні акти саботажу, кіберзагрози та інші небезпеки. Оновлення повинні базуватися на спільних принципах ЄС та охоплювати ключові сектори: енергетичний, транспортний, фінансовий, охорону здоров’я та цифрову інфраструктуру. Результати оцінок мають сприяти виявленню слабких місць і розробці ефективних заходів для їх усунення.
Проведення стрес-тестів у ключових секторах	Впровадження стрес-тестів у ключових секторах економіки на основі загальноєвропейських принципів. Такі тести дозволять оцінити готовність критичних об’єктів до екстремальних ситуацій з метою підвищення стійкості національної інфраструктури України. Результати стрес-тестів дозволяють визначити слабкі місця і зміцнити інфраструктурну безпеки за допомогою провідних практик ЄС.
Розробка національного плану реагування на значні інциденти в критичній інфраструктурі	Розробка та узгодження дорожньої карти з реагування на кризові ситуації в критичній інфраструктурі, особливо транскордонного характеру. Даний план повинен включати заходи для захисту основних секторів, таких як енергетика, охорона здоров’я, банківська справа, цифрова інфраструктура та продовольча безпека. План має враховувати координацію між відомствами на всіх рівнях, забезпечувати обмін інформацією та підтримувати швидке реагування на надзвичайні ситуації.
Посилення міжнародного співробітництва з питань безпеки критичної інфраструктури	Розвиток мережі співпраці з міжнародними партнерами, зокрема з країнами ЄС, НАТО, США та Канадою, адже спільна робота та обмін інформацією забезпечить Україні високий рівень підготовки до потенційних транскордонних загроз; а участь у спеціальних робочих групах з питань безпеки (наприклад, цільова група ЄС-НАТО) сприятиме підвищенню рівня захисту критичної інфраструктури.
Залучення до європейських дослідницьких програм із безпеки критичної інфраструктури	Розширення можливостей для участі України у європейських дослідницьких програмах (наприклад, Horizon Europe), які спрямовані на розвиток інноваційних рішень для підвищення стійкості критичної інфраструктури. Таким чином, співпраця з європейськими науково-дослідними установами дозволить залучити фінансування для проєктів із захисту критичної інфраструктури, розробити нові технології та методи для управління кризами.
Формування єдиного управлінського механізму щодо захистом критичної інфраструктури	Створення єдиного управлінського механізму що забезпечить управління, нагляд, моніторинг, контроль та захист критичної інфраструктури в Україні має бути впорядкований у комплексну ієрархічну структуру управління захистом критичної інфраструктури, яка включає

	єдиний механізм координації з пріоритетом на рівні державної політики. Такий підхід забезпечить координацію між різними відомствами та сприятиме підвищенню ефективності реагування на загрози критичної інфраструктури.
Створення національної довідкової мережі захисту критичної інфраструктури	Створення національної платформи для обміну інформацією та найкращими практиками щодо захисту критичної інфраструктури, подібної до Європейської довідкової мережі (ERNCIP). Така мережа сприятиме підвищенню обізнаності серед ключових суб'єктів, надаватиме консультативну підтримку та допомагатиме інтегрувати міжнародний досвід у національні стратегії управління інфраструктурною безпекою.

Джерело: власна розробка автора

Таким чином, незважаючи на системність та повноту окреслених нормативно-правових актів в рамках правового забезпечення управління, захисту та подальшого безперебійного функціонування об'єктів критичної інфраструктури, адаптація українського законодавства до європейських норм, зокрема Директиви ЄС щодо стійкості критично важливих об'єктів, є необхідним кроком у напрямку підвищення стійкості критичної інфраструктури. Розробка нової національної стратегії та реформ в рамках державної політики передбачає створення чітких інструкцій для ідентифікації критичних суб'єктів, аналіз ризиків та впровадження системних процедур, забезпечить належний рівень захисту від загроз, що можуть виникати як зсередини, так і ззовні. На підставі вищезазначеного, пропонується зосередитися на удосконаленні правового забезпечення публічного управління у сфері трансформації об'єктів критичної інфраструктури, впроваджуючи нові організаційні структури управління, які базуються на міжнародних стандартах. Створення комплексної ієрархічної системи управління дозволить підвищити ефективність реагування на загрози, забезпечуючи стійке функціонування критичних об'єктів та національної економіки в цілому.

Висновки до розділу 1

За результатами проведеного дослідження основних теоретичних аспектів публічного управління у сфері трансформації об’єктів критичної інфраструктури було визначено:

1. Визначення та категоризація об’єктів критичної інфраструктури відповідно до їх критичності дозволяє систематизувати підходи до їх захисту та управління, що сприяє підвищенню рівня економічної, державної та соціальної безпеки. Аналіз функцій публічного управління, зокрема стратегічного планування, регулювання, координації та контролю, демонструє, що успішне управління критичною інфраструктурою передбачає інтеграцію дій державних органів і приватного сектора. Крім того, важливими є додаткові функції, такі як кадрове забезпечення, матеріально-технічна підтримка та діловодство, що створюють основи для ефективного функціонування системи управління. Особливу увагу слід звернути на виклики, що виникають у сучасних умовах, зокрема в умовах війни, коли безпека інформації та доступ до об'єктів критичної інфраструктури стають критично важливими. Тенденції до спрощення регуляторних процесів та створення єдиного реєстру об'єктів критичної інфраструктури також свідчать про необхідність адаптації управлінських структур до нових реалій. Отже, ефективне управління критичною інфраструктурою потребує багаторівневого підходу, що враховує специфіку різних секторів, а також постійного моніторингу і оцінки ризиків, щоб забезпечити надійність та безпеку в умовах непередбачуваних загроз.

2. Сучасні наукові дослідження показали різноманітність підходів до класифікації та управління критичною інфраструктурою, що є важливою складовою для ефективного функціонування економіки та соціальних систем. Значну увагу приділено необхідності систематизації управлінських процесів та впровадження новітніх технологій у захист критичної інфраструктури, що, у свою чергу, може підвищити ефективність заходів безпеки. Проте існуючі обмеження, такі як недостатнє врахування регіональних особливостей та

динамічні загрози, вказують на потребу в подальших дослідженнях та розробці комплексних стратегій управління. Системний, централізований, несправний, ризик-орієнтований, державно-приватний та міжнародний підходи до управління критичною інфраструктурою відкривають нові перспективи для ефективної взаємодії між державними органами та приватним сектором. Однак без єдиного підходу до ідентифікації загроз та управлінських процесів важко забезпечити належний рівень безпеки.

3. Інтеграція між різними секторами, такими як постачальні ланцюги, енергетичні та інформаційні системи, створює нові ризики для функціонування критичної інфраструктури, що вимагає системного підходу до її захисту. В умовах тривалої війни в Україні важливість забезпечення стійкості інфраструктури стає особливо актуальною, а залучення міжнародних ресурсів є ключовим елементом у формуванні стратегії. Критично важливим є створення єдиних державних систем цивільного захисту, запобігання терористичним актам та забезпечення кібербезпеки, що дозволяє не лише реагувати на загрози, але й запобігати їх виникненню. Проте в Україні досі бракує чіткої класифікації загроз, що ускладнює реалізацію ефективних заходів захисту. Визначення об'єктів критичної інфраструктури та їх оцінка є необхідними для розробки адекватних стратегій управління. Ефективна трансформація критичної інфраструктури вимагає інтеграції новітніх технологій та активної координації між державним та приватним секторами. Таким чином, стратегічна державна політика має зосереджуватися на розвитку комплексних підходів, включаючи спільні дії з міжнародними партнерами, з наданням стабільного функціонування критичної інфраструктури в умовах невизначеності та наявних загроз.

4. Проаналізована законодавча база, закладена у Законі України «Про критичну інфраструктуру» № 1882-IX від 21 вересня 2024 р., а також супутніми нормативно-правовими актами, створює правову основу для управління та захисту цих об’єктів. Прийняття Національного плану захисту та забезпечення безпеки критичної інфраструктури вказує на системний підхід до моніторингу, оцінки ризиків та інтеграції дій усіх учасників. Зокрема, необхідність

удосконалення механізмів інформаційної безпеки в умовах загострення кіберзагроз стала пріоритетною задачею для держави. Впровадження європейських стандартів та практик, адаптація українських норм до вимог ЄС, а також формування інтегрованої системи управління та координації дій між усіма зацікавленими сторонами підвищує стійкість критичної інфраструктури. Запропоновані підходи до організації управління відображають інноваційний підхід до забезпечення безпеки, з урахуванням міжнародного досвіду, зокрема у сфері захисту інфраструктури в США. Таким чином, ефективне правове забезпечення публічного управління критичною інфраструктурою є важливо складовою управління її безпекою та стійким розвитком України в умовах війни та супутньої нестабільності.

РОЗДІЛ 2
МЕХАНІЗМИ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ТРАНСФОРМАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

2.1. Структура та види механізмів публічного управління у сфері трансформації об'єктів критичної інфраструктури

Вимоги щодо трансформації системи державного управління та зміни пріоритетів публічної політики у напрямі забезпечення збалансованого соціально-економічного розвитку країни, ключового значення набуває розроблення і впровадження механізмів публічного управління, здатних не лише забезпечити стабільне функціонування базових інституцій, а й адаптуватися до викликів зовнішнього середовища з одночасним забезпеченням сталості розвитку територій, соціальних систем і базової інфраструктури.

Бурик З. М. пов'язує ефективність механізмів публічного управління з інноваційними та цифровими інструментами. Серед базових переваг ефективної системи публічного управління вона називає деполітизованість, пріоритет суспільних інтересів у межах концепції стійкого розвитку та постійне вдосконалення. Окремо підкреслює партнерський підхід, за якого держава і громадяни є рівноправними учасниками відносин, а дієва публічність досягається через електронний документообіг, цифровізацію управлінських процесів і інструменти штучного інтелекту. Авторка обґрунтовує шість принципів упровадження інновацій у публічне управління: децентралізацію, перспективність, системність, демократичність, адаптивність і моніторинг [12, с. 213].

Лелеченко А. П. розглядає механізми публічного управління крізь призму автономії місцевого самоврядування та децентралізації. Універсальну модель

автономії він описує як комплексну систему інструментів і механізмів для ефективного, прозорого та підзвітного місцевого врядування. До неї входять адміністративно-територіальні зміни, фінансова та владна децентралізація, стратегічне планування, громадська участь, прозорість, міжнародна співпраця та законодавче забезпечення, які мають діяти в синергії. Управлінську структуру регіону, на думку автора, слід будувати за принципом субсидіарності: органи вищого рівня виконують лише ті функції, з якими не можуть впоратися органи нижчого рівня. Він також наголошує, що вітчизняному самоврядуванню потрібні менеджмент-орієнтовані підходи для переходу до автономної, сервісно-орієнтованої моделі управління на місцевому рівні [51, с. 170].

Помаза-Пономаренко А. Л. зосереджується на інституційних, адаптивних та антикризових механізмах. Адаптивне управління вона трактує як превентивний процес, що має запобігати кризовим явищам. Антикризове натомість покликане розв'язувати кризи, які вже настали. Ефективне антикризове управління, за її моделлю, потребує взаємодії трьох елементів: держава встановлює правові межі та забезпечує ресурси, інститути громадянського суспільства здійснюють моніторинг і залучають громадян, а омбудсман контролює дотримання прав і формує рекомендації [91].

Сутність комплексного механізму публічного управління об’єктами критичної інфраструктури держави, на нашу думку, полягає у впорядкованій сукупності засобів, методів, процедур, інституційних компонентів, правових інструментів та організаційно-функціональних моделей, що забезпечують реалізацію державної політики у сфері управління цими об’єктами, з урахуванням специфіки галузевих ризиків, міжвідомчої взаємодії та стратегічних пріоритетів безпеки. Комплексний механізм має охоплювати весь цикл публічного управління – від ідентифікації об’єктів, їх класифікації, планування та регулювання, до моніторингу, реагування, відновлення та адаптації до змін середовища.

Основними структурними елементами комплексного механізму публічного управління можуть стати: нормативно-правова база, інституційна

система управління, організаційно-інформаційне забезпечення, інструменти фінансового регулювання, технологічна інфраструктура управління ризиками та цифрові рішення для забезпечення прозорості та безперервності державного контролю. Усі ці компоненти функціонують у взаємозв'язку, забезпечуючи спроможність держави ефективно управляти критичними ресурсами у звичайних та надзвичайних умовах.

Нормативно-правове забезпечення механізму публічного управління у даній сфері включає законодавчі та підзаконні акти, які визначають категорії критичної інфраструктури, повноваження органів влади, принципи взаємодії між державними, комунальними та приватними суб'єктами, стандарти безпеки, вимоги до кіберзахисту, механізми реагування на інциденти та правила проведення аудиту. Зокрема, базовим документом у цій сфері є Закон України «Про критичну інфраструктуру», який визначає засади її функціонування та захисту, а також окреслює принципи координації між відповідальними суб'єктами.

Інституційний компонент містить сукупність органів державної влади, які мають повноваження у сфері управління критичною інфраструктурою, зокрема Кабінет Міністрів України, Національну комісію з питань техногенно-екологічної безпеки, Державну службу з надзвичайних ситуацій, Службу безпеки України, Національний координаційний центр кібербезпеки при РНБО, а також профільні міністерства (енергетики, інфраструктури, охорони здоров'я, цифрової трансформації). Їхня діяльність має бути скоординованою відповідно до принципів єдиного управління, вертикальної підпорядкованості та горизонтальної комунікації для уникнення дублювання функцій, забезпечення безперервності управління та концентрації ресурсів у разі кризових ситуацій [10].

Організаційно-інформаційне забезпечення включає створення реєстрів об'єктів критичної інфраструктури, ведення їх паспортизації, організацію системи обміну інформацією між суб'єктами управління, використання аналітичних платформ для прогнозування ризиків, моделювання сценаріїв

порушення функціонування та оптимізації ресурсного забезпечення. На практиці це означає необхідність створення інтегрованих інформаційних систем, які дозволяють відстежувати стан об’єктів у режимі реального часу, проводити оцінку вразливостей та автоматизовано реагувати на інциденти [12]. Економічні інструменти в межах механізму публічного управління включають державне фінансування програм модернізації критичної інфраструктури, цільове бюджетне планування, державно-приватне партнерство, залучення коштів міжнародних фінансових інституцій, створення страхових фондів, механізмів компенсацій та пільгового кредитування підприємств, які здійснюють діяльність у критичних секторах. З метою практичної реалізації зазначеного підходу у сфері публічного управління доцільно обґрунтувати структурно-логічну модель механізму забезпечення сталого розвитку, яка б інтегрувала ключові компоненти управлінського процесу – цілі, принципи, функції, інструменти, суб’єкти реалізації та результативні індикатори, що у сукупності формують цілісну систему державного реагування (рис. 2.1.). Практика публічного управління при трансформаціях об’єктів критичної інфраструктури потребують не лише перегляду чинної системи планування й реалізації управлінських рішень, а й створення адаптивної, багаторівневої моделі управління, що базується на узгодженості інтересів усіх зацікавлених сторін, а також постійному моніторингу та оновленні стратегічних пріоритетів відповідно до змін внутрішнього та зовнішнього безпекового середовища [30 , с. 64]. Високого рівня ваги набуває формування чіткої системи оцінювання стану та динаміки розвитку інфраструктурної безпеки, що базується на інтегрованих показниках, здатних комплексно відобразити ступінь захищеності та адаптивності об’єктів, які мають стратегічне значення для життєдіяльності держави. У такому ключі основна увага має бути приділена не макроекономічним чи фінансовим аспектам, а насамперед індикаторам, що характеризують науково-технічну готовність інфраструктури до впровадження сучасних технологій безпеки [40, с. 261].



Рис. 2.1. Структурно-логічна модель комплексного механізму публічного управління об'єктами критичної інфраструктури країни *Джерело: власна розробка автора

В таблиці 2.1 розкрито зміст, переваги, виклики та шляхи вдосконалення кожного механізму, демонструючи їхню взаємодію та значення для сталого розвитку інфраструктури.

1.Нормативно-правовий механізм у сфері забезпечення роботи об'єктів критичної інфраструктури являє собою комплекс законодавчих і підзаконних актів, стандартів, регламентів та процедур, спрямованих на формування єдиної правової основи для їх захисту, модернізації та сталого функціонування. Його ключове завдання полягає у встановленні чітких правил і вимог, що визначають обов'язки та повноваження суб'єктів управління, порядок взаємодії між державними, комунальними й приватними операторами, а також вимоги до безпеки та кіберзахисту. Він формує передумови для уніфікації управлінських рішень, забезпечує правову визначеність і передбачуваність дій, сприяє гармонізації національних норм із міжнародними стандартами. Ефективність нормативно-правового механізму значною мірою залежить від швидкості адаптації законодавства до змін зовнішнього середовища, оновлення під впливом нових загроз і впровадження прогресивних регуляторних підходів.

2. Інституційний механізм відображає систему взаємодії органів державної влади, місцевого самоврядування, спеціалізованих агенцій і приватних операторів у процесі управління критичною інфраструктурою. Він забезпечує розподіл повноважень, визначення функцій та відповідальності кожного суб'єкта, створення ієрархії та процедур координації. У науковому вимірі цей механізм можна розглядати як ключову основу управлінської архітектури, що формує вертикаль і горизонталь комунікацій, запобігає дублюванню функцій і сприяє концентрації ресурсів у критичних точках. Його ефективність залежить від наявності єдиного координаційного центру, здатного швидко реагувати на кризові ситуації та забезпечувати скоординовану діяльність усіх учасників. Оптимальна інституційно-організаційна модель передбачає впровадження гнучких структур управління, інтеграцію регіональних ініціатив у національну політику та постійний моніторинг результативності організаційних рішень.

Таблиця 2.1

Види механізмів забезпечення публічного управління в сфері забезпечення роботи об’єктів критичної інфраструктури*

№	Вид механізму	Основний зміст	Переваги механізму	Виклики та обмеження	Пропоновані заходи для вдосконалення
1	Нормативно-правовий	Розробка та імплементація законодавчої бази, стандартів безпеки, процедур реагування	Забезпечує чіткі правові рамки, уніфіковані стандарти	Повільне оновлення законодавства, невідповідність сучасним загрозам	Прискорення перегляду законів, гармонізація з міжнародними стандартами
2	Інституційно-організаційний	Координація діяльності органів влади, розподіл повноважень	Сприяє чіткому розподілу відповідальності	Дублювання функцій, низька міжвідомча координація	Створення єдиного координаційного органу
3	Організаційно-інформаційний	Впровадження ІТ-систем, аналітичних платформ, реєстрів об’єктів	Підвищення прозорості, швидкості реагування	Висока вартість, вразливість до кібератак	Розробка захищених платформ, регулярне тестування
4	Економіко-фінансовий	Фінансування модернізації, ППП, залучення інвестицій	Стимулює модернізацію, залучає приватний сектор	Обмеженість бюджетів, ризики корупції	Прозорі тендери, механізми контролю за коштами
5	Технологічний	Модернізація обладнання, інженерний захист об'єктів, резервування потужностей, впровадження SCADA-систем	Підвищує фізичну стійкість і безперервність роботи об'єктів	Зношеність обладнання, імпортозалежність, тривалі строки модернізації	Локалізація виробництва обладнання, впровадження стандартів ЄС, створення резервного фонду обладнання
6	Цифровий	Впровадження цифрових двійників, ГІС-моніторингу, предиктивної аналітики та штучного інтелекту	Забезпечує прогнозування збоїв і прийняття рішень на основі даних	Низька цифрова зрілість операторів, брак ІТ-фахівців, кіберризики.	Розробка стандартів цифровізації КІ, навчання персоналу, сертифікація кіберзахисту.
7	Прогностично-планувальний	Розробка стратегій, сценарне моделювання, управління ризиками	Дозволяє прогнозувати та мінімізувати ризики	Недостатня точність прогнозів, брак експертизи	Впровадження сучасних методів аналізу, навчання фахівців
8	Координаційний	Синхронізація дій між суб’єктами, усунення дублювань	Підвищення ефективності взаємодії	Конфлікти інтересів, бюрократичні затримки	Формування міжсекторальних робочих груп
9	Контрольно-наглядовий	Моніторинг стану об’єктів, аудит, оцінка ефективності	Забезпечує контроль якості, виявлення недоліків	Недостатня незалежність аудиторів, формальність перевірок	Впровадження незалежного аудиту, автоматизований моніторинг

*Джерело: власна розробка автора

Інституційний механізм охоплює систему органів і організацій, відповідальних за захист і функціонування КІ, а також розподіл повноважень між ними на національному, регіональному та місцевому рівнях. До нього належать Кабінет Міністрів, РНБО, уповноважений орган у сфері захисту КІ, секторальні та функціональні органи, ДСНС, СБУ, органи місцевого самоврядування й оператори. Його призначення – усунути дублювання функцій і забезпечити вертикальну та горизонтальну координацію.

3. *Організаційно-інформаційний механізм* забезпечує взаємодію суб'єктів управління через планування, координацію та обмін інформацією. Він включає категоризацію й паспортизацію об'єктів, ведення реєстру, обмін даними про загрози та інциденти, а також місцеві плани взаємодії на випадок кризових ситуацій. Саме він робить систему керованою в режимі реального часу. Охоплює системи збору, обробки, аналізу та передачі даних, необхідних для ефективного управління об’єктами критичної інфраструктури. Він включає створення державних реєстрів, цифрових платформ моніторингу, інтегрованих аналітичних систем та інформаційно-комунікаційних каналів, що забезпечують прозорість і швидкість прийняття рішень. Наукова значущість цього механізму полягає у здатності забезпечувати безперервний обмін достовірною інформацією між усіма стейкхолдерами, що підвищує готовність до реагування на загрози та зменшує час на координацію дій. Він також дозволяє здійснювати моделювання сценаріїв розвитку подій, прогнозування ризиків і планування ресурсів. Розвиток організаційно-інформаційного механізму потребує інвестицій у захищені цифрові технології, регулярного оновлення програмного забезпечення та впровадження кіберзахисних рішень, що знижують вразливість інфраструктури до інформаційних атак.

4. Фінансово-економічний механізм – це сукупність джерел і інструментів фінансування захисту, відновлення та розвитку КІ: державний і місцеві бюджети, кошти операторів, державно-приватне партнерство, міжнародна допомога, страхування. Сюди ж належать економічні важелі впливу: тарифне регулювання, податкові пільги, компенсації, санкції. Механізм покликаний забезпечити

сталість функціонування об'єктів і стимулювати операторів інвестувати в безпеку. Механізм спрямований на забезпечення фінансової спроможності модернізації, підтримки та захисту об’єктів критичної інфраструктури. Він охоплює бюджетне фінансування, механізми державно-приватного партнерства, залучення міжнародних інвестицій, пільгове кредитування та страхування ризиків. У науковому аспекті цей механізм розглядається як інструмент економічної мотивації і стимулювання модернізаційних процесів, що забезпечує стабільність інфраструктурних систем у довгостроковій перспективі. Його ефективність залежить від прозорості фінансових потоків, конкурентних процедур розподілу коштів та впровадження механізмів контролю за цільовим використанням ресурсів. Розвиток економіко-фінансового механізму передбачає поєднання державних і приватних інвестицій, створення резервних фондів та адаптивних схем фінансування, що враховують сезонні та кризові коливання попиту на інфраструктурні послуги.

5. Технологічний механізм (управління ризиками) спрямований на виявлення загроз і вразливостей об'єктів, оцінювання ризиків і впровадження заходів фізичного, інженерного та кіберзахисту. Він передбачає технічне переоснащення, резервування потужностей, моделювання каскадних ефектів між секторами та сценарне планування.

6. Цифровий механізм (прозорість і контроль) ґрунтується на використанні цифрових платформ для моніторингу стану об'єктів, контролю за використанням коштів і виконанням проєктів відновлення.

Окремо можемо виділити прогностично-планувальний, координаційний та контрольно-наглядовий механізми.

1. Прогностично-планувальний механізм охоплює методи передбачення, сценарного моделювання та стратегічного планування розвитку критичної інфраструктури. Його сутність полягає у системному зборі та аналізі даних для формування прогнозів щодо потенційних загроз, технічного зносу, потреб модернізації й оптимізації ресурсів. У науковому вимірі цей механізм розглядається як основа довгострокового управління ризиками, що дозволяє

забезпечити стійкість інфраструктурних об’єктів до зовнішніх і внутрішніх викликів. Ефективна прогностично-планувальна діяльність передбачає використання сучасних аналітичних методів, математичного моделювання, геоінформаційних систем, а також постійне оновлення прогнозів залежно від зміни факторів середовища. Такий підхід дає змогу приймати обґрунтовані рішення, які зменшують імовірність кризових ситуацій і підвищують адаптивність інфраструктури до швидкоплинних змін.

2. Координаційний механізм передбачає узгодження дій між усіма суб’єктами публічного управління, операторами інфраструктури та іншими зацікавленими сторонами з метою ефективної реалізації стратегій розвитку і захисту критичних об’єктів. Він включає формування міжвідомчих робочих груп, організацію спільних навчань, розробку протоколів взаємодії та кризових планів. У науковій площині координаційний механізм розглядається як інтеграційний інструмент, що мінімізує дублювання функцій, усуває конфлікти компетенцій і забезпечує комплексність рішень. Його ефективність залежить від чіткості процедур комунікації, регулярності обміну інформацією та здатності швидко адаптувати плани дій до зміни обставин. Оптимальна реалізація цього механізму сприяє підвищенню синергії між учасниками процесу, що є ключовим чинником у сфері безпеки та модернізації критичної інфраструктури.

3. Контрольно-наглядовий механізм відповідає за моніторинг технічного стану об’єктів критичної інфраструктури, перевірку відповідності стандартам безпеки, аудит управлінських рішень і оцінку ефективності реалізації програм модернізації. Його наукова значущість полягає у створенні системи зворотного зв’язку, яка дозволяє виявляти відхилення від встановлених показників, аналізувати причини порушень і розробляти заходи для їх усунення. Ефективний контрольно-наглядовий механізм базується на поєднанні незалежного аудиту, автоматизованих систем моніторингу та процедур внутрішнього контролю. Він має бути гнучким, щоб реагувати не лише на вже виявлені недоліки, але й запобігати їх виникненню шляхом превентивних заходів. Розвиток цього механізму передбачає впровадження інноваційних методів оцінки, підвищення

прозорості контрольних процедур і зміцнення незалежності наглядових структур.

У межах комплексного механізму виділено взаємопов’язані блоки: а) блок стратегічного планування, б) блок координації та в) блок операційного реагування.

а) Блок стратегічного планування визначає довгострокові цілі, пріоритети та напрями розвитку системи захисту критичної інфраструктури. Він охоплює розроблення й актуалізацію стратегічних документів (Стратегії національної безпеки, Національного плану захисту та забезпечення безпеки та стійкості КІ, галузевих і регіональних програм), оцінювання загроз і прогнозування ризиків, визначення секторальних пріоритетів і обсягів ресурсного забезпечення. Ключовими суб'єктами блоку є Кабінет Міністрів України, РНБО, уповноважений орган у сфері захисту КІ та профільні міністерства. Результат роботи блоку — узгоджена система цілей, індикаторів і планів, на яку спираються два інші блоки. Найтісніше він пов'язаний із нормативно-правовим і фінансово-економічним механізмами.

б) Блок координації забезпечує узгодженість дій суб'єктів управління по вертикалі (національний, регіональний, місцевий рівні) і по горизонталі (між секторами КІ, державним і приватним сектором, міжнародними партнерами). Він включає розподіл повноважень і відповідальності, функціонування системи обміну інформацією між суб'єктами національної системи захисту КІ, міжвідомчу взаємодію, ведення реєстру та паспортизацію об'єктів, а також координацію міжнародної допомоги. Цей блок перетворює стратегічні рішення на скоординовані дії, усуває дублювання функцій і зменшує ризик каскадних збоїв між секторами. Він спирається насамперед на інституційний та організаційно-інформаційний механізми.

в) Блок операційного реагування відповідає за безпосередні дії під час загроз, інцидентів і кризових ситуацій. Він охоплює моніторинг стану об'єктів у реальному часі, раннє виявлення загроз, реагування на аварії, атаки та кіберінциденти, локалізацію наслідків, аварійно-відновлювальні роботи та

забезпечення безперервності надання життєво важливих послуг. Основні виконавці блоку — оператори КІ, ДСНС, CERT-UA, Держспецзв'язку, місцеві органи виконавчої влади та органи місцевого самоврядування. Найбільшою мірою він реалізується через технологічний (управління ризиками) і цифровий механізми.

Блоки утворюють замкнений управлінський цикл. Стратегічне планування задає цілі та ресурси, координація забезпечує їх узгоджене виконання, а операційне реагування реалізує заходи на рівні конкретних об'єктів. Дані, отримані під час реагування (інциденти, виявлені вразливості, ефективність заходів), через контур зворотного зв'язку повертаються на рівень стратегічного планування й слугують підставою для коригування цілей, планів і нормативної бази. Саме такий циклічний характер забезпечує адаптивність механізму та його здатність підтримувати стійкість критичної інфраструктури в умовах трансформацій.

До базових компонентів оцінки ефективності публічного управління у сфері трансформації критичної інфраструктури належать показники рівня інженерної модернізації, наявності резервних технологічних потужностей, ступеня впровадження автоматизованих систем контролю, а також індикатори, що відображають кадровий потенціал регіонів, рівень підготовки фахівців у сфері захисту критичних об’єктів, доступність спеціалізованої освіти та участь населення в заходах громадянської безпеки. Саме ці чинники мають враховуватись під час розробки та реалізації державних і регіональних програм модернізації об’єктів критичної інфраструктури, оскільки вони забезпечують стійкість до ризиків природного, техногенного чи гібридного характеру.

На рис. 2.2. і було продемонстровано системні складові формування й реалізації стратегічних цілей трансформації об’єктів критичної інфраструктури, що передбачає гармонізацію управлінських рішень між центральними та місцевими рівнями влади, а також координацію дій між усіма залученими суб’єктами, від урядових структур до операторів інфраструктури. Все це базується на ієрархічній моделі публічного управління, згідно з якою ключові

орієнтири задаються на макрорівні через затверджені національні стратегії та нормативні акти, що дозволяє створити системну вертикаль, спрямовану на зниження вразливості інфраструктурних об'єктів до зовнішніх та внутрішніх загроз [19, с. 102].

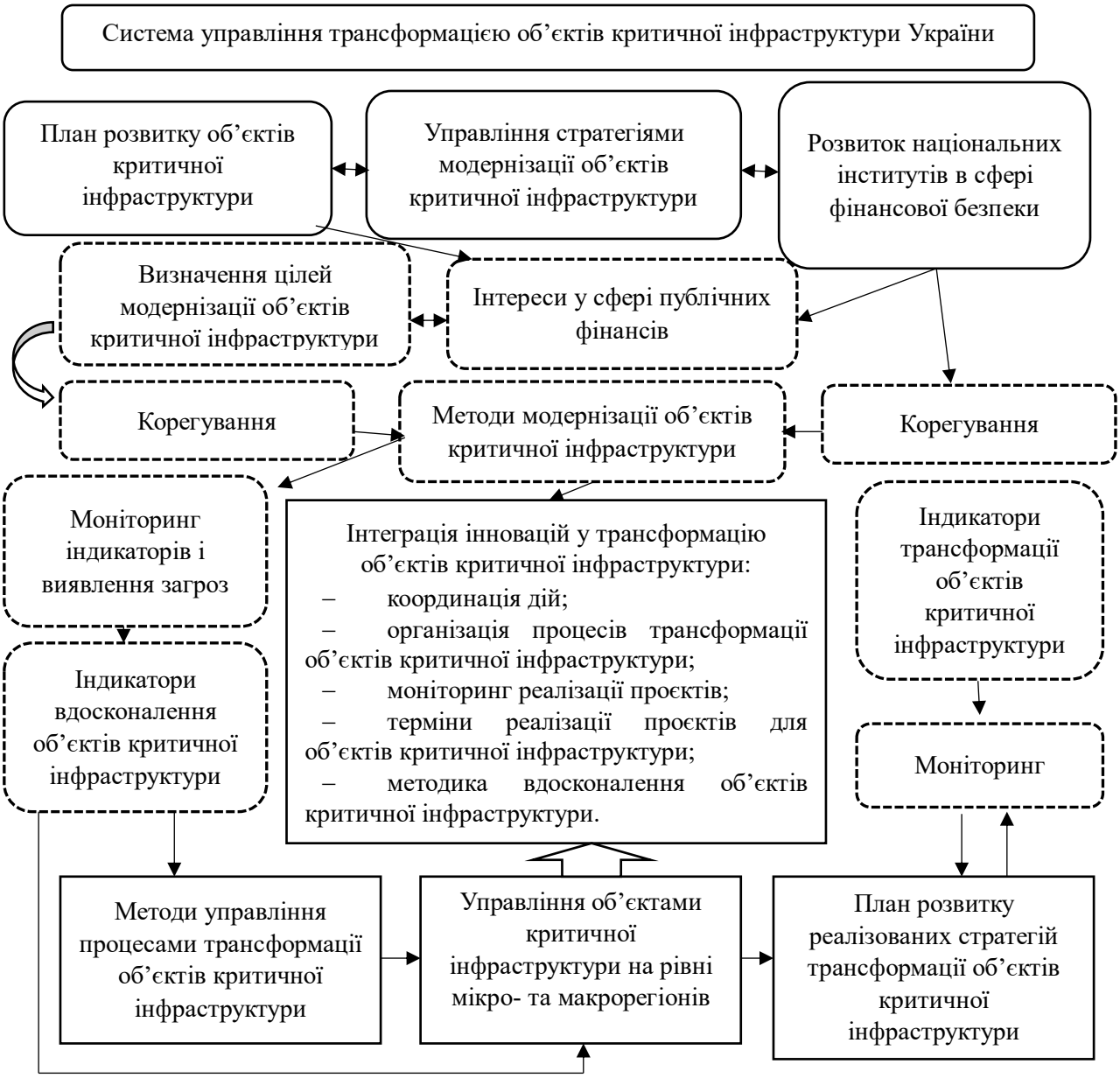


Рис. 2.2. Система управління трансформацією об'єктів критичної інфраструктури України*

*Джерело: власна розробка автора

Проблематика визначення відповідального інституційного суб'єкта та налагодження ефективної взаємодії між рівнями управління давно постає однією з ключових перешкод на шляху практичного впровадження стратегічних

документів у сфері забезпечення національної безпеки. У контексті дослідження механізму публічного управління у сфері трансформації об’єктів критичної інфраструктури України це питання набуває особливої актуальності, адже саме від ступеня узгодженості інтересів і дій між центральною виконавчою владою, органами місцевого самоврядування, операторами інфраструктури та спеціалізованими службами безпеки залежить ефективність модернізації, захисту та стійкості об’єктів, що забезпечують життєво важливі функції держави. Недостатнє інституційне опрацювання процедур координації та відсутність чітко визначеного механізму інтеграції стратегічних рішень на різних рівнях управління призводять до того, що більшість ініціатив у сфері критичної інфраструктури залишаються декларативними або реалізуються фрагментарно, без досягнення системного ефекту [15, с. 43].

У межах таких пошуків, вже доцільно розглядати стратегію комплексного планування трансформації об’єктів критичної інфраструктури, яка передбачає багаторівневе управління з виокремленням мезорівня як ключового простору для координації дій регіональних і місцевих органів влади. Така стратегія повинна ґрунтуватися на проведенні всеохоплюючої інвентаризації стану об’єктів критичної інфраструктури, оцінці ризиків, ступеня фізичного та кіберзахисту, а також на визначенні потреб у ресурсному, кадровому, технологічному та інформаційному забезпеченні. Цінним управлінським інструментом у цьому контексті є формування системи міжсекторального партнерства на умовах чітко регламентованих договорів, які регулюють розподіл відповідальності та зобов’язань між учасниками процесу. Водночас в умовах сучасної децентралізації та високої залежності безпеки критичної інфраструктури від регіональних факторів виникає конфлікт інтересів між різними управлінськими суб’єктами: державними органами, громадами приватними операторами об’єктів, що ускладнює реалізацію єдиної політики безпеки [4, с. 45-46] (табл. 2.2).

Таблиця 2.2

Методи (інструменти) аналізу задля забезпечення ефективного публічного управління трансформацією об’єктів критичної інфраструктури України*

№	Методи (інструменти) аналізу	Опис методу
1	Карта зацікавлених сторін	Інструмент, який використовується керівництвом органу державної влади або групою управлінців для формування, наприклад, за допомогою методу «мозкового штурму», суб’єктивного уявлення про те, чиї інтереси можуть бути зачеплені в процесі реалізації стратегій захисту та трансформації об’єктів критичної інфраструктури, таких як енергетичні мережі, транспортні вузли чи системи зв’язку, а також для визначення того, як ці інтереси впливають на безпеку та стабільність функціонування інфраструктури на регіональному чи національному рівні
2	Інтереси ключових стейкхолдерів	Документ, який фіксує показники, що оцінюють ступінь впливу ключових суб’єктів, рівень їхньої підтримки чи опору ініціативам, спрямованим на забезпечення безпеки критичної інфраструктури, такої як водопостачання чи телекомунікаційні системи, а також інформацію про їхні інтереси, що дозволяє розробити стратегію взаємодії, яка враховує ці інтереси та сприяє підвищенню ефективності публічного управління захистом об’єктів інфраструктури в Україні
3	Матриця оцінки підтримки та впливу	Інструмент, який дає змогу ідентифікувати зацікавлені сторони, що створюють ризики для реалізації політики захисту критичної інфраструктури через низький рівень підтримки за наявності значного впливу, а також визначити тих, чия підтримка є високою, для посилення співпраці з метою забезпечення безпеки та надійності об’єктів, таких як енергетичні чи транспортні системи, що є критично важливими для національної безпеки
4	Інтегральна оцінка середовища безпеки критичної інфраструктури	Метод, який аналізує ризики, що виникають у системі безпеки критичної інфраструктури через поведінку стейкхолдерів, яка може дестабілізувати функціонування об’єктів, таких як системи водопостачання чи інформаційні мережі, і використовується для оцінки зовнішніх і внутрішніх загроз, таких як кібератаки чи організаційні збої, у контексті публічного управління з метою розроблення заходів для їхньої нейтралізації.
5	Багатокритеріальний аналіз зацікавлених сторін	Метод, який передбачає оцінку довгострокових наслідків реалізації стратегій захисту критичної інфраструктури, їхньої значущості для безпеки об’єктів, таких як транспортні чи енергетичні системи, і застосовується для аналізу інтересів стейкхолдерів під час вибору управлінських проєктів, прогнозування потенційних конфліктів, при цьому оцінка впливу проєктів ґрунтується на експертних судженнях, а баланс інтересів досягається через методи багатокритеріальної оптимізації

*Джерело: власна розробка автора

Визначений варіант дослідження показує свою ефективність у стратегічному плануванні соціально значущих процесів, дозволяє сформувати обґрунтовану, гнучку механізм державної політики, що відповідає реаліям регіонального розвитку, і водночас йде і узгоджена з загальнонаціональними інтересами у сфері критичної інфраструктури [25]. Координація діяльності між цими суб'єктами, яка враховує як загальнодержавні пріоритети, так і регіональні особливості, потребує інтеграції механізмів публічного управління в систему стратегічного планування, що дозволяє не лише гармонізувати інтереси всіх залучених сторін, але й забезпечити стійкість і безпеку критичної інфраструктури на різних рівнях [3, с. 131].

Вирішення конфліктів інтересів, які неминуче виникають у процесі трансформації об'єктів критичної інфраструктури, набуває стратегічного значення, оскільки від цього залежить не лише ефективність реалізації проектів, але й загальна стабільність функціонування ключових інфраструктурних систем, що є основою життєдіяльності держави. Об'єкти критичної інфраструктури зазнають постійних викликів, пов'язаних із технологічними, безпековими та організаційними змінами, управлінські механізми повинні бути гнучкими, адаптивними та орієнтованими на довгострокову стабільність, що забезпечується шляхом чіткого планування, яке дозволяє регіонам визначати пріоритети розвитку, ефективно використовувати наявні ресурси для забезпечення надійності критичної інфраструктури (рис. 2.3.) [27, с. 420]..

У контексті змін в політиці забезпечення об'єктів критичної інфраструктури, таких як енергетичні, транспортні чи комунікаційні системи, безперервне планування відіграє ключову роль у забезпеченні ефективного публічного управління, оскільки воно дозволяє не лише прогнозувати потенційні виклики, пов'язані з невизначеністю зовнішнього середовища та динамічними змінами, але й розробляти комплексні управлінські рішення, які сприяють захисту та стабільному функціонуванню цих об'єктів, забезпечуючи їхню стійкість до внутрішніх і зовнішніх загроз [49].



Рис. 2.3. Процеси координації та напрями вдосконалення трансформації об'єктів критичної інфраструктури в системі публічного управління України*

*Джерело: власна розробка автора

Технології планування, які включають розробку деталізованих планів, графіків і систем показників для оцінки виконання завдань, дають змогу чітко визначити цілі управління критичною інфраструктурою, необхідні ресурси для їх реалізації, а також методи, які є найбільш ефективними для конкретних регіональних умов, при цьому забезпечуючи можливість своєчасного

моніторингу та коригування заходів, спрямованих на підвищення безпеки та надійності об’єктів інфраструктури [49].

Етап прогнозування, який зазвичай передує плануванню, відіграє важливу роль у моделюванні різних сценаріїв розвитку подій у сфері управління критичною інфраструктурою, дозволяючи оцінити потенційні ризики, такі як технологічні негаразди чи зовнішні загрози, та обрати оптимальний шлях для їхньої нейтралізації, що сприяє зміцненню безпеки на регіональному та національному рівнях. Стратегічне планування, у свою чергу, виступає ключовим інструментом для визначення довгострокових цілей у сфері захисту критичної інфраструктури, розробки альтернативних управлінських стратегій на основі аналізу перспектив розвитку регіонів і створення комплексної системи заходів для протидії потенційним загрозам, що можуть вплинути на функціонування об’єктів, які є критично важливими для життєдіяльності суспільства та держави [46, с. 145].

На загальнодержавному рівні стратегічне планування сприяє узгодженню інтересів між різними інституційними суб’єктами, залученими до трансформації критичної інфраструктури, забезпечуючи гармонізацію поточних і довгострокових цілей, а також підвищення ефективності управлінських процедур, що реалізуються як на регіональному, так і на національному рівнях, що є важливим для забезпечення стабільності та безпеки ключових інфраструктурних систем (табл. 2.3). У межах поточного дослідження на свій рівень уваги також заслуговують питання розроблення адаптивних управлінських моделей, які здатні забезпечити своєчасне реагування на регіонально специфічні загрози, що мають безпосередній вплив на стійкість та функціонування інфраструктурних систем, життєво важливих для населення та держави. У ситуаціях, коли рівень загроз має змінний, часто асиметричний характер, надзвичайно важливим стає не лише вміння оперативно мобілізувати необхідні ресурси, а й наявність гнучких стратегій управлінської адаптації, які забезпечать безперервність функціонування об’єктів критичної інфраструктури навіть за умов кризових сценаріїв [44].

Таблиця 2.3

Функціональні аспекти публічного управління трансформацією об’єктів критичної інфраструктури України*

№	Функція публічного управління	Зміст функції публічного управління забезпеченням безпеки критичної інфраструктури
1	Планування	Процес визначення цілей і завдань забезпечення безпеки об’єктів критичної інфраструктури, таких як енергетичні мережі, транспортні системи чи телекомунікаційні об’єкти, розробка стратегій і механізмів їхньої реалізації з урахуванням пріоритетів розвитку регіонів, що включає стратегічне планування для довгострокової стійкості інфраструктури, індикативне планування для оцінки ключових показників безпеки, а також оперативне й поточне планування для адаптації до змін у середовищі, пов’язаних із потенційними загрозами, такими як кібератаки чи природні катаклізми
2	Організація	Створення умов для досягнення поставлених цілей захисту критичної інфраструктури шляхом формування регіональних управлінських структур, які сприяють координації дій зацікавлених сторін, включаючи державні органи, місцеве самоврядування та приватний сектор, постановка управлінських завдань для забезпечення безпеки об’єктів, а також делегування повноважень органам влади різних рівнів для ефективного публічного управління трансформацією інфраструктури
3	Мотивація	Розробка системи стимулів для органів державної влади, місцевого самоврядування та інших стейкхолдерів, яка активізує їхню діяльність у процесі вирішення завдань захисту критичної інфраструктури, включаючи створення програм співпраці з приватним сектором і громадськими організаціями для залучення їх до реалізації стратегій забезпечення безпеки об’єктів, таких як водопостачання чи інформаційні системи, що є критично важливими для національної безпеки
4	Контроль	Здійснення моніторингу показників безпеки об’єктів критичної інфраструктури

*Джерело: власна розробка автора

Організаційна функція публічного управління у сфері трансформації критичної інфраструктури повинна бути спрямована передусім на формування цілісного управлінського середовища, здатного забезпечити координацію між усіма задіяними суб’єктами – від центральних органів виконавчої влади до регіональних структур цивільного захисту, а також операторів відповідних інфраструктурних систем. На цьому етапі особливого значення набуває аналіз форм і механізмів міжінституційної взаємодії, включаючи використання таких методів управлінського впливу, як нормативно-розпорядчі акти, інструкції,

протоколи взаємодії та адміністративні процедури, що регламентують дії у разі виникнення надзвичайних загроз або потреби у трансформації об’єктів [22].

Додатково до цього важливим елементом є застосування методів організаційного впливу, які передбачають розробку нормативних положень щодо функціональних обов’язків структур публічного управління у сфері інфраструктурної безпеки, оптимізацію кадрового забезпечення, встановлення чітких протоколів техногенної й кібернетичної безпеки, а також інформування персоналу про вимоги до підтримання безперебійної роботи об’єктів у критичних умовах [57, с. 233-234].

З метою досягнення дієвого узгодження інтересів між регіональними органами публічного управління, місцевими громадами та технічними операторами інфраструктури доцільно створити спеціалізовані інституційні підрозділи, які виконуватимуть функцію координації процесів трансформації, моніторингу технічного стану об’єктів, аналізу потреб у модернізації, а також забезпечення належної реакції на загрози. Вони мають функціонувати в рамках уже існуючих систем державного управління, однак мати чітко визначений мандат, кадрову автономію та інструментарій впливу на регіональні рішення щодо критичної інфраструктури (табл. 2.4).

Таблиця 2.4

Функціональні аспекти публічного управління трансформацією критичної інфраструктури України*

№	Функція	Основні завдання	Методи реалізації	Рівень впровадження	Очікуваний ефект
1	Організаційна функція	Забезпечення ресурсами та координація діяльності всіх залучених сторін, включаючи державні органи, регіональні адміністрації, приватний сектор і громадськість, для реалізації проєктів трансформації об’єктів критичної інфраструктури, таких як енергетичні мережі, транспортні системи чи телекомунікаційні об’єкти, шляхом створення структурованих управлінських механізмів, які сприяють чіткому розподілу обов’язків і ефективному виконанню завдань	Застосування розпорядчих і організаційних методів, таких як створення спеціалізованих робочих груп, розподіл ресурсів і розробка процедур, які забезпечують структуровану взаємодію для реалізації проєктів трансформації критичної інфраструктури	Державний, регіональний	Оптимізація взаємодії між усіма учасниками процесу трансформації критичної інфраструктури, що сприяє підвищенню ефективності реалізації проєктів модернізації об’єктів, таких як водопостачання чи транспортні мережі

2	Координаційна функція	Синхронізація дій державних органів, регіональних адміністрацій, приватних компаній і громадських організацій у процесі трансформації об'єктів критичної інфраструктури, таких як інформаційні системи чи енергетичні комплекси, для забезпечення узгодженого виконання проєктів, спрямованих на їхню модернізацію та вдосконалення	Створення координаційних підрозділів, які відповідають за налагодження комунікацій між органами влади, організацію спільних заходів і забезпечення злагодженої роботи всіх учасників процесу трансформації критичної інфраструктури	Регіональний	Гармонізація діяльності всіх залучених сторін, що сприяє ефективному впровадженню проєктів трансформації об'єктів критичної інфраструктури та їхньому функціональному вдосконаленню
3	Мотиваційна функція	Залучення зацікавлених сторін, включаючи державні установи, приватний сектор і громадськість, до активної участі в реалізації проєктів трансформації об'єктів критичної інфраструктури, таких як транспортні вузли чи системи зв'язку, шляхом створення стимулів, які спонукають до співпраці та активної участі в модернізації інфраструктури	Розробка механізмів морального та організаційного заохочення, таких як програми співпраці з приватним сектором, громадськими організаціями та місцевими громадами, для активізації їхньої участі в проєктах трансформації критичної інфраструктури	Державний, регіональний	Підвищення рівня залученості стейкхолдерів до реалізації проєктів, що сприяє ефективному вдосконаленню об'єктів критичної інфраструктури та їхній адаптації до сучасних вимог
4	Контрольна функція	Моніторинг ходу реалізації проєктів трансформації об'єктів критичної інфраструктури, таких як водопостачальні системи чи енергетичні об'єкти, шляхом аналізу прогресу, виявлення відхилень від запланованих цілей і оцінки ефективності впроваджених управлінських заходів для забезпечення їхньої відповідності встановленим стандартам	Розробка процедур моніторингу, стратегічних планів і нормативних документів, які дозволяють відстежувати виконання проєктів трансформації критичної інфраструктури, оцінювати їхній прогрес і вносити необхідні коригування для досягнення поставлених цілей	Національний, регіональний	Підвищення якості реалізації проєктів трансформації об'єктів критичної інфраструктури шляхом своєчасного виявлення недоліків і вдосконалення управлінських процесів
5	Регуляторна функція	Розробка та впровадження державної політики у сфері трансформації об'єктів критичної інфраструктури, що передбачає створення нормативно-правової бази для регулювання діяльності, спрямованої на модернізацію таких об'єктів, як телекомунікаційні системи чи транспортна інфраструктура, з метою забезпечення їхнього структурованого розвитку	Нормативно-правове регулювання, яке включає розробку законів, стандартів і процедур, що визначають вимоги до трансформації об'єктів критичної інфраструктури та забезпечують їхню відповідність національним і регіональним пріоритетам	Державний	Забезпечення стабільності та структурованості процесів трансформації об'єктів критичної інфраструктури шляхом створення чіткої нормативної основи для їхньої модернізації та вдосконалення

*Джерело: сформовано автором на основі [17], [41], [45]

Обґрунтований варіант розгортання подій, сприятиме формуванню надійного фундаменту для довгострокового розвитку інфраструктури, забезпечуючи її адаптивність до сучасних викликів, таких як технологічні зміни, кібератаки чи природні катаклізми, та створюючи умови для гармонійного

врахування потреб усіх залучених сторін у процесі управління. Для ефективного публічного управління у сфері трансформації критичної інфраструктури необхідна концептуальна механізм, яка передбачає комплексний підхід до розроблення управлінських рішень через проходження кількох послідовних етапів, що дозволяють системно підійти до захисту ключових об'єктів. На першому етапі здійснюється концептуальне осмислення сутності безпеки критичної інфраструктури, визначення основних загроз, таких як фізичні пошкодження, кібернетичні атаки чи організаційні недоліки, а також ідентифікація стратегічних пріоритетів, які мають бути покладені в основу національної політики у цій сфері [11, с. 123-124]. Наступним кроком є аналіз проблемних аспектів, пов'язаних із забезпеченням безпеки критичної інфраструктури, що дає змогу окреслити потенційні ризики на державному та регіональному рівнях і розробити заходи для їхньої мінімізації. Завершальним етапом є створення ефективної моделі публічного управління, яка включає розроблення механізмів регулювання, інструментів прогнозування можливих загроз і засобів контролю, що забезпечують стійкість і надійність критичної інфраструктури у довгостроковій перспективі, сприяючи її захисту від зовнішніх і внутрішніх викликів [1, 21].

Контрольна функція в межах цього управлінського механізму має бути не просто формальним етапом, а гнучкою, динамічною складовою загальної моделі публічного управління, яка дозволяє оперативно виявляти проблемні ділянки в процесі взаємодії між державними органами, місцевими громадами, експлуатантами об'єктів інфраструктури та службами безпеки [14]. У результаті впровадження такої моделі публічного управління досягається не лише загальне підвищення ефективності реалізації трансформаційних заходів, а й значне зміцнення системи національної безпеки через зменшення внутрішніх конфліктів, нейтралізацію міжінституційних суперечностей і формування стійкого середовища взаємодії. Функціональна структура публічного управління захистом критичної інфраструктури ґрунтується на комплексному підході до стратегічного планування, який охоплює кілька ключових етапів: планування,

що включає прогнозування можливих сценаріїв розвитку, визначення пріоритетів і розроблення програм для реалізації заходів, спрямованих на захист об’єктів; організацію, яка передбачає створення спеціалізованих управлінських структур, розподіл повноважень між органами влади та забезпечення умов для ефективної реалізації державної політики у сфері безпеки інфраструктури; виконання, що охоплює практичну реалізацію запланованих заходів, налагодження комунікацій між різними суб’єктами управління та координацію дій на державному й регіональному рівнях; а також контроль, який забезпечує моніторинг ефективності управлінських рішень, оцінку відповідності отриманих результатів стратегічним цілям і внесення необхідних коригувань для підвищення надійності критичної інфраструктури (рис. 2.4.) [28, с. 529].

До додаткових принципів окрім раніше виділених системності; ризик-орієнтованості; безперервності управління; вертикальної та горизонтальної координації; прозорості; адаптивності формування зазначеного механізму належать:

– багатофакторна оцінка спроможності об’єкта критичної інфраструктури функціонувати в умовах впливу дестабілізуючих чинників, що передбачає інтеграцію показників технічного стану, рівня захищеності, соціальної значущості та ступеня взаємозалежності з іншими інфраструктурними вузлами;

– узгодження інтересів ключових суб’єктів управління, включаючи органи виконавчої влади, місцеве самоврядування, спеціалізовані служби, що забезпечує скоординоване планування, розподіл відповідальності та уникнення конфліктів компетенцій [31, с. 82];

– системна підтримка міжінституційної взаємодії, що передбачає створення механізмів постійної кооперації, обміну інформацією та спільного управління ризиками між органами публічної влади на різних рівнях;

– контроль за використанням і розподілом стратегічно важливих ресурсів, які є критичними для стабільного функціонування об’єктів, у тому числі резервного забезпечення, логістичної інфраструктури та енергопостачання;

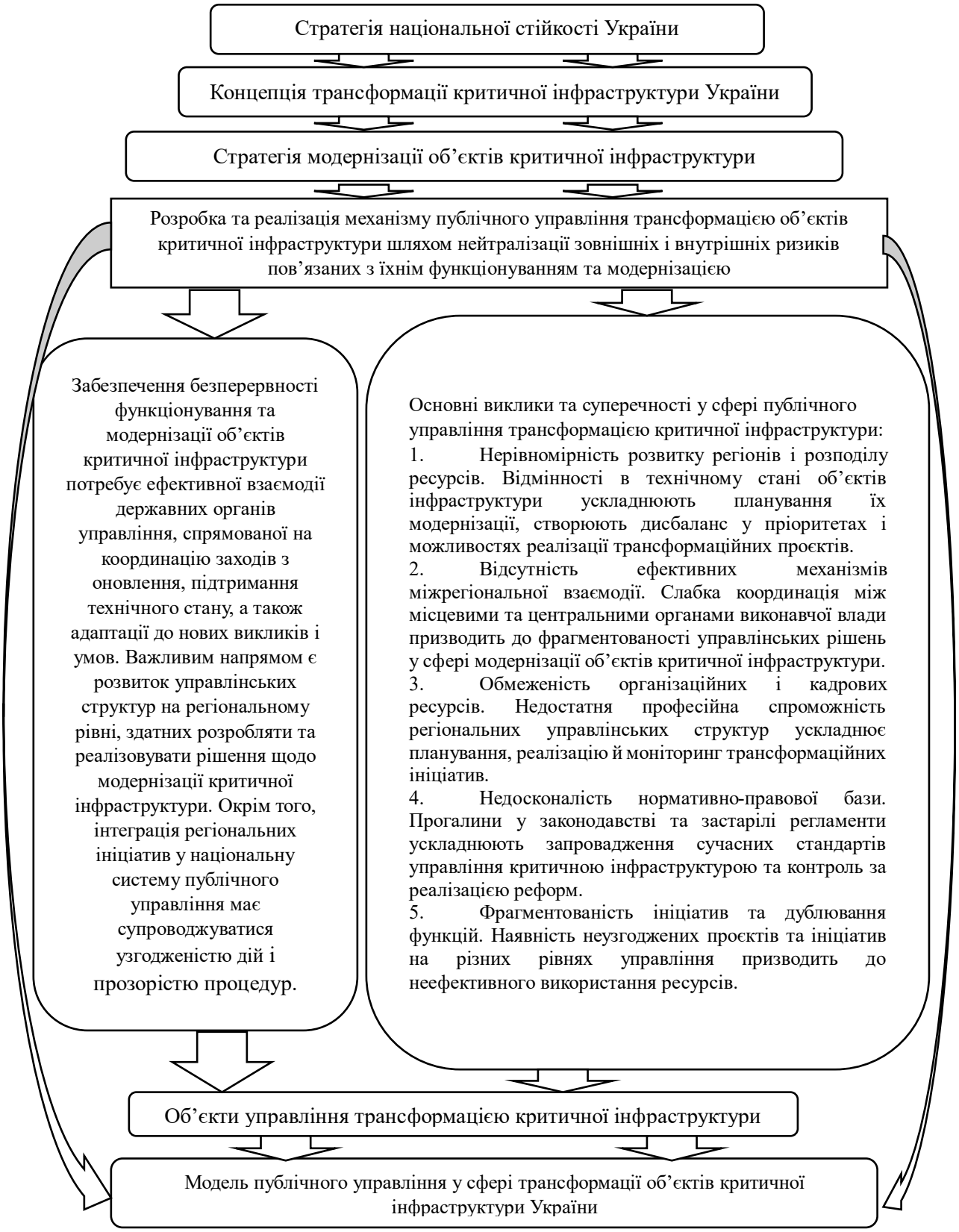


Рис. 2.4. Інституційна модель реалізації публічного управління в трансформації об'єктів критичної інфраструктури України*

*Джерело: власна розробка автора

– впровадження систем управління якістю процесів експлуатації та обслуговування об’єктів, з акцентом на екологічну, технологічну та соціальну безпеку, із застосуванням інструментів функціонального аудиту, державно-громадського моніторингу та адаптивного регулювання;

– здатність до трансформації механізмів управління в умовах кризової ситуації або невизначеності зовнішнього середовища, що передбачає сценарне планування, резервне моделювання рішень та адаптивне бюджетування;

– побудова гнучких організаційно-управлінських структур, які забезпечують безперервність функціонування об’єктів у випадку порушення системи центрального управління або обмеженого доступу до ресурсів;

– формування як формалізованих, так і неформальних зв’язків між учасниками процесу управління, що посилює ефективність координації дій у разі надзвичайних ситуацій та підвищує рівень міжвідомчої комунікації;

– управління обсягом, якістю та актуальністю інформаційної бази щодо технічного стану об’єктів, можливих загроз, очікуваних сценаріїв розвитку подій, що забезпечує оперативність і достовірність управлінських рішень;

– узгодженість стратегічного та оперативного планування, що вимагає чіткої інтеграції довгострокових програм розвитку інфраструктурних секторів з інструментами щорічного програмно-цільового бюджетування, заснованого на достовірних даних та сучасних цифрових платформах.

На основі узагальнення наукових підходів до формування систем управління у сфері безпеки, національної стійкості та територіального розвитку, сформульовано комплекс фундаментальних принципів побудови комплексного механізму публічного управління об’єктами критичної інфраструктури країни, які є комплементарними та взаємодоповнюваними, а також враховують динамічність зовнішнього середовища, багаторівневу управлінську ієрархію та високий ступінь ризику в експлуатації таких об’єктів на основі забезпечення ефективності управлінських рішень (рис. 2.5).



Рис. 2.5. Комплексний механізм публічного управління об'єктами критичної інфраструктури на основі забезпечення ефективності управлінських рішень* *Джерело: власна розробка автора

Виділення видів механізмів публічного управління об’єктами критичної інфраструктури формує їхню комплексну природу та необхідність узгодженої взаємодії. Метою функціонування комплексного механізму є – забезпечення стійкості, захищеності та безперервності функціонування об’єктів критичної інфраструктури країни в умовах трансформації; з точки зору ефективності метою є – забезпечення належного рівня ефективності управлінських рішень у процесі функціонування об’єктів критичної інфраструктури. Однак виклики, такі як застаріле законодавство, бюрократія чи кіберзагрози, потребують подолання: оновлення нормативно-правової бази, створення координаційних центрів, впровадження сучасних технологій і прозорих процедур. Це забезпечить адаптивність і стійкість критичної інфраструктури, сприяючи національній безпеці та сталому розвитку в умовах динамічних викликів.

2.2. Процеси та складові публічного управління захисту, безпеки, стійкості та трансформації об’єктів критичної інфраструктури в сучасних умовах

Виділені концептуальні складові публічного управління у сфері трансформації об’єктів критичної інфраструктури України (нормативно-правова база, стратегічне планування, інституційне забезпечення) мають визначальний фактор впливу у створенні єдиної теоретичної та методологічної платформи, яка сприяє як ґрунтовному аналізу поточного стану, так і практичному розробленню багатошарової, міжвідомчої системи управління, спроможної забезпечити адаптивність, стійкість і безперервність роботи об’єктів критичної інфраструктури в умовах сучасних загроз, що постають перед Україною (рис. 2.6.).

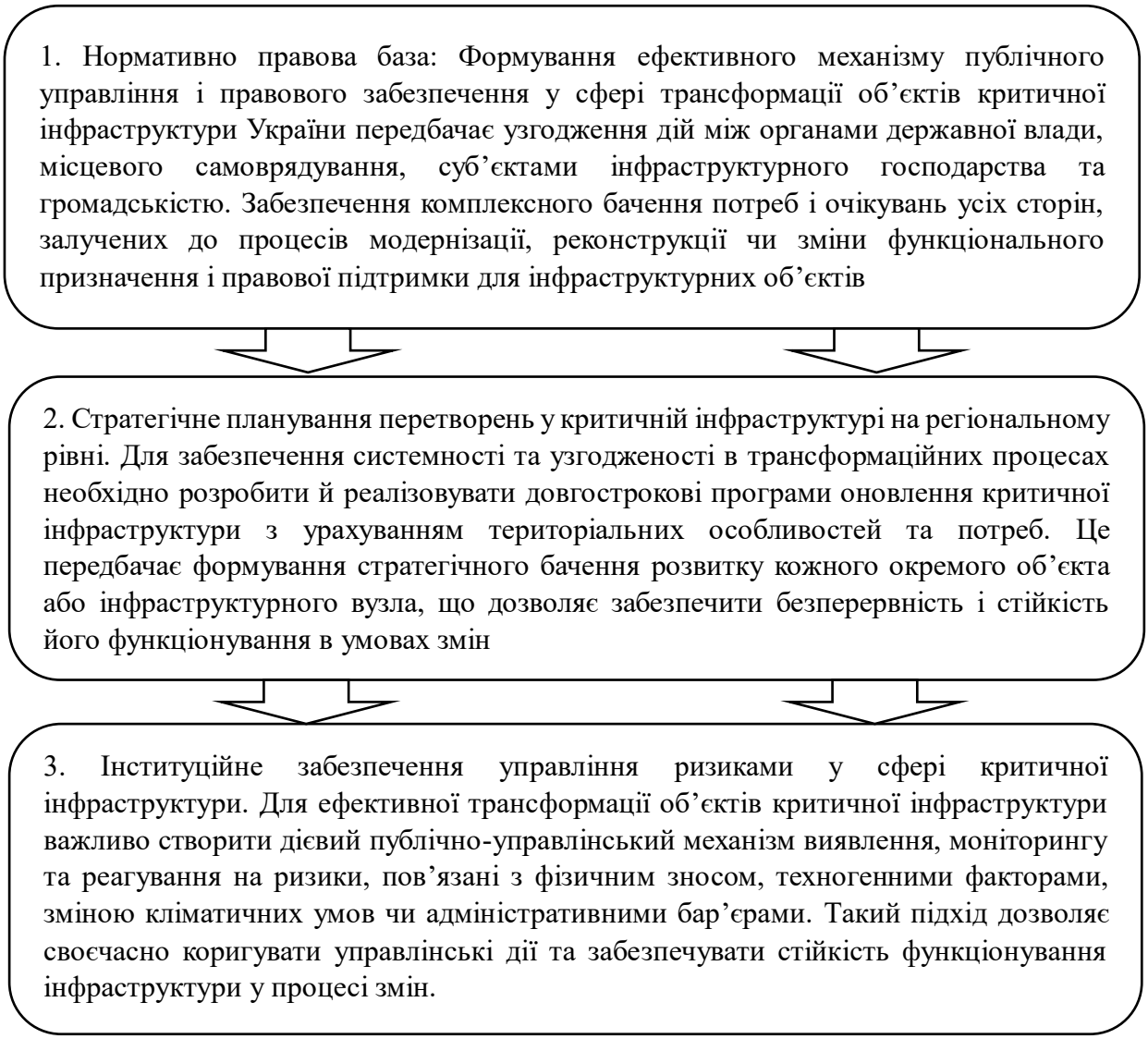


Рис. 2.6. Базові складові публічного управління у сфері трансформації об'єктів критичної інфраструктури України*

*Джерело: власна розробка автора

Застосування концептуального аналізу дає можливість обґрунтувати логічно послідовні та змістовно узгоджені управлінські моделі, у межах яких правове забезпечення публічного управління трансформацією об'єктів критичної інфраструктури розглядається як складний, багатокомпонентний процес, що включає нормативно-правові основи, організаційні структури, кадрові ресурси, технологічні рішення та інституційні інструменти, які разом формують основу для ефективного функціонування цих систем [8, с. 135].

У цьому контексті концептуальні підходи забезпечують перехід від абстрактних теоретичних рамок до конкретних практичних засобів управління,

зокрема через розробку архітектури багатоступеневих управлінських систем, які враховують розподіл повноважень від центрального рівня до місцевих громад, а також сприяють гармонізації інтересів усіх учасників процесу, таких як центральні органи влади, служби цивільного захисту, місцеві органи самоврядування, оператори інфраструктури та представники громадськості [13].

Саме концептуальне планування відкрило перспективи для подальшого створення універсальних стратегій реагування на надзвичайні обставини, модернізації слабких ланок інфраструктури та впровадження передових технологій для захисту та вдосконалення цих об'єктів [38].

З огляду на це, нормативно-правовий механізм публічного управління трансформацією об'єктів критичної інфраструктури України має базуватися на принципах інтегрованої координації та балансування інтересів усіх суб'єктів, залучених до управлінської діяльності, з урахуванням не лише офіційно визначених повноважень, а й неформальних потреб, очікувань та взаємозв'язків між ними, що сприяє створенню збалансованої системи управління. Вказаний механізм має містити компоненти вже стратегічного планування на основі прогнозування ризиків за допомогою сценарного моделювання, адаптацію інституційних структур до умов зростання загроз, чітке розподілення функціональних обов'язків, а також впровадження гнучких систем стимулювання та контролю, які підвищують стійкість управлінських рішень до дестабілізуючих чинників, таких як воєнні дії чи техногенні аварії. Правове забезпечення публічного управління в аспекті підтримки функціонування критичної інфраструктури набуває форми багатогранного та багатошарового процесу, у якому поєднуються методи стратегічного адміністрування, управління кризовими ситуаціями, координація з цивільними службами, забезпечення інформаційної стабільності та міжсекторальна співпраця, а головним викликом залишається досягнення злагодженої взаємодії між цими елементами в умовах постійно мінливого безпекового середовища [18, с. 16].

В Україні, де триває тривалий збройний конфлікт, є застарілою інфраструктура, а також виникають виклики, пов'язані з глобалізацією,

технологічними змінами та кліматичними факторами, які створюють значні перешкоди для ефективного управління об’єктами КІ, нормативно-правове забезпечення публічного управління відіграє вирішальну роль у забезпеченні їхнього захисту, безпеки, стійкості та трансформації, що є критично важливим для підтримки національної стійкості та інтеграції в європейський простір. Основним нормативним документом, який регулює цю сферу, є Закон України «Про критичну інфраструктуру» (Закон №1882-IX), прийнятий 16 листопада 2021 року, який закладає правові та організаційні засади для створення національної системи захисту критичної інфраструктури, визначаючи принципи державної політики, ключові терміни та механізми координації дій між усіма зацікавленими сторонами [34].

Нормативно-правова основа публічного управління захистом, безпекою, стійкістю та трансформацією об’єктів критичної інфраструктури в Україні базується передусім на Законі України «Про критичну інфраструктуру» (Закон №1882-IX), який був прийнятий Верховною Радою 16 листопада 2021 року та набрав чинності з 2022 року, ставши центральним нормативно-правовим актом, що регулює функціонування, захист та модернізацію таких об’єктів, як енергетичні мережі, транспортні артерії, водопостачальні системи та телекомунікаційні мережі, встановлюючи правові засади для забезпечення їхньої стійкості та адаптації до нових умов, а також визначаючи ключові принципи державної політики, які спрямовані на підтримку безперервної роботи цих систем у мирний час, у період воєнного стану та в умовах надзвичайних ситуацій [34]. Закон визначає критичну інфраструктуру як сукупність систем і об’єктів, чиє порушення чи деградація може спричинити значні наслідки для життєдіяльності суспільства, охоплюючи широкий спектр секторів, таких як енергетика, транспорт, телекомунікації, водопостачання, охорона здоров’я та соціальна сфера, що дозволяє чітко класифікувати об’єкти за їхньою критичністю та пріоритетністю для держави, створюючи основу для розробки цільових програм їхньої модернізації та захисту [2, с. 10].

Закон України «Про критичну інфраструктуру» вводить 24 ключові терміни, які формують концептуальну основу для управління цими об’єктами, серед яких такі поняття, як «захист», «життєво важливі функції», «інцидент», «категоризація», «криза», «критична інфраструктура», «оператор» та «реєстр», що забезпечують чітке розуміння ролі та значення цих об’єктів у державній системі, а також створюють правову основу для їхньої ідентифікації, класифікації та координації дій між усіма учасниками процесу. Наприклад, «критична інфраструктура» визначається як сукупність об’єктів і систем, які є необхідними для забезпечення життєдіяльності суспільства та виконання державних функцій, тоді як «захист» включає комплекс заходів, спрямованих на запобігання порушенням їхнього функціонування, включаючи фізичний захист від зовнішніх загроз та захист від технологічних збоїв [36]. Принципи державної політики, визначені законом, включають визнання необхідності стійкості та надійності критичної інфраструктури, встановлення чітких законодавчих вимог до її захисту, визначення суб’єктів та їхніх повноважень, створення умов для зниження ризиків і раннього виявлення потенційних загроз, що дозволяє формувати комплексний підхід до управління цими об’єктами, адаптований до сучасних умов, зокрема в умовах воєнного стану.

Окрім Закону України «Про критичну інфраструктуру», управління цими об’єктами регулюється низкою інших нормативно-правових актів, які доповнюють його положення та деталізують окремі аспекти захисту, стійкості та трансформації, створюючи цілісну правову систему, що охоплює різні рівні управління та сектори інфраструктури. Так безпосередньо, Закон України «Про національну безпеку України» (Закон №2469-VIII) визначає критичну інфраструктуру як складову національної безпеки, підкреслюючи її стратегічне значення для держави, тоді як Закон України «Про кібербезпеку України» (Закон №2163-VIII) регулює захист критичної інформаційної інфраструктури від кіберзагроз, що є особливо актуальним у контексті цифровізації та гібридних загроз. Закон України «Про енергетичну ефективність будівель» (Закон №3664-VI) встановлює принципи забезпечення стійкості енергетичної інфраструктури,

а міжнародні договори, укладені в рамках асоціації з Європейським Союзом, сприяють гармонізації українських норм із європейськими стандартами, такими як Директива 2008/114/ЄС про ідентифікацію та позначення європейської критичної інфраструктури. Наведені нормативні акти разом створюють багатошарову правову основу для управління критичною інфраструктурою, забезпечуючи її захист і модернізацію на різних рівнях, від місцевих громад до національного масштабу [32, 34, 43].

Закон України «Про критичну інфраструктуру» зазначає, що особливості захисту та правового режиму об’єктів критичної інфраструктури в умовах надзвичайних ситуацій, воєнного стану чи спеціального періоду регулюються окремими законами, такими як Закон України «Про правовий режим воєнного стану» (Закон №389-VIII), Закон України «Про правовий режим надзвичайного стану» (Закон №1550-III) та Закон України «Про функціонування єдиної транспортної системи України в особливий період» (Закон №1532-IX), що дозволяє адаптувати управління до специфічних умов, забезпечуючи стійкість об’єктів у кризових ситуаціях. Наприклад, у воєнний час можуть застосовуватися додаткові заходи для захисту енергетичних мереж від пошкоджень, транспортних вузлів від блокування та водопостачальних систем від руйнувань, що є критично важливими для підтримки життєдіяльності населення та функціонування державних інституцій.

Якісне управління захистом, безпекою, стійкістю та трансформацією об’єктів критичної інфраструктури вимагає чіткої інституційної структури, яка забезпечує координацію дій між державними органами, регіональними адміністраціями, операторами критичної інфраструктури та громадськими організаціями, створюючи злагоджену систему управління, здатну реагувати на сучасні виклики, такі як воєнні дії, технологічні збої чи природні катаклізми, та підтримувати безперебійне функціонування об’єктів, таких як енергетичні мережі, транспортні системи, водопостачання та телекомунікації. Закон України «Про критичну інфраструктуру» (Закон №1882-IX) встановлює таку структуру, визначаючи ключові ролі та відповідальність кожного учасника процесу, що

дозволяє забезпечити цілісний підхід до управління цими об’єктами на всіх рівнях, від місцевих громад до національного масштабу.

У контексті воєнної агресії Російської Федерації та ведення бойових дій на території України, особливо актуальним стало ухвалення Закону України «Про внесення змін до деяких законодавчих актів України щодо забезпечення діяльності об’єктів критичної інфраструктури під час дії воєнного стану» від 22 травня 2024 року № 3723-IX. Закон містить положення про заборону відчуження майна операторів КІ, встановлює тимчасову заборону на примусове стягнення боргів під час дії воєнного стану та впродовж двох років після його завершення. Це спрямовано на забезпечення цілісності критичних об’єктів, їх правового захисту від зовнішнього втручання та недопущення втрати державного або стратегічного контролю [32].

На рівні підзаконного регулювання значну роль відіграє Постанова Кабінету Міністрів України від 9 жовтня 2020 року № 1109 «Деякі питання об’єктів критичної інфраструктури» (із змінами станом на 16 грудня 2022 року), яка визначає порядок ведення Державного реєстру об’єктів критичної інфраструктури, критерії класифікації, вимоги до суб’єктів управління та порядок подання даних до центральних органів виконавчої влади. Цей документ забезпечує організаційне та інформаційне підґрунтя для структуризації національного переліку КІ. Окремим документом у частині моніторингу стану безпеки є Постанова Кабінету Міністрів України від 22 липня 2022 року № 821 «Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури», яка визначає індикатори оцінки, порядок збору та узагальнення інформації про безпекові характеристики об’єктів, а також механізми взаємодії між суб’єктами публічного управління під час проведення аналізу ризиків.

Особливу увагу у сфері забезпечення надійної міжвідомчої взаємодії слід звернути на Постанови Кабінету Міністрів України від 14 жовтня 2022 року № 1174 "Про затвердження Регламенту обміну інформацією у сфері захисту критичної інфраструктури" та № 1175 «Про деякі питання подання інформації у

сфері захисту критичної інфраструктури». Зазначені нормативно-правові акти регулюють механізми збору, зберігання, обміну й захисту інформації, у тому числі конфіденційної, що має критичне значення для національної безпеки.

Щодо методичного забезпечення процесу категоризації об'єктів КІ, важливим є Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15 січня 2021 року № 23, яким затверджено Методичні рекомендації щодо категоризації об'єктів критичної інфраструктури. У документі передбачено поетапну процедуру визначення критичності об'єкта за рівнем наслідків його виходу з ладу для економіки, суспільства та державної безпеки. У стратегічному контексті особливу роль відіграє Постанова Кабінету Міністрів України від 2023 року № 825, якою затверджено Національний план захисту критичної інфраструктури. Цей план містить вимоги до змісту паспортів безпеки, визначає алгоритм реагування на надзвичайні ситуації, запроваджує стандарти кризового управління та визначає відповідальність органів публічного управління за координацію заходів у межах відповідного сектору критичної інфраструктури. Не менш вагоме місце для правового забезпечення має і Постанова Кабінету Міністрів України від 19 червня 2019 року № 519 «Про затвердження Порядку захисту об'єктів критичної інформаційної інфраструктури», яка регулює заходи із забезпечення кіберзахисту, встановлює вимоги до технічних рішень, порядок доступу до інформаційних систем, критерії ризиковості та відповідальність за невиконання вимог у сфері кібербезпеки.

Правову систему захисту КІ також доповнює Указ Президента України № 695/2023 від 17 жовтня 2023 року, яким введено в дію рішення Ради національної безпеки і оборони України щодо організації захисту об'єктів критичної інфраструктури, з особливим акцентом на енергетичний сектор. Указ спрямовано на підвищення рівня оперативної готовності, створення міжвідомчих координаційних структур та запровадження стандартів реагування в умовах надзвичайних ситуацій [43]. Нарешті, слід зазначити, що вищезгадані законодавчі та нормативно-правові документи функціонують у межах більш широкого правового поля, закріпленого в Конституції України, зокрема в статтях

3, 17, 27, 92, які встановлюють обов'язок держави захищати життя, безпеку та гідність громадян, а також в ратифікованих міжнародних договорах України, що є частиною національного законодавства згідно зі статтею 9 Основного Закону. У сукупності ці акти формують правову рамку для формування інтегрованого, ефективного та відповідального механізму публічного управління у сфері захисту, стійкості та трансформації критичної інфраструктури України (табл. 2.5).

Таблиця 2.5

Порівняльний аналіз нормативно-правового забезпечення процесів публічного управління при здійсненні трансформацій для об'єктів критичної інфраструктури України*

Сфера регулювання	Ключовий нормативний акт	Основні положення	Уповноважені органи	Механізми реалізації
Загальні засади управління критичною інфраструктурою	Закон України «Про критичну інфраструктуру» №1882-IX	Визначає поняття, принципи, категоризацію об'єктів, повноваження суб'єктів	Національна комісія з питань захисту критичної інфраструктури	Реєстр об'єктів, ідентифікація, класифікація, координація
Захист в умовах надзвичайного чи воєнного стану	Закони України «Про правовий режим воєнного стану», «Про надзвичайний стан»	Регулюють специфіку управління інфраструктурою у кризовий період	Кабінет Міністрів України, РНБО, військові адміністрації	Додаткові захисні заходи, мобілізація, спеціальний режим функціонування
Кіберзахист критичної інформаційної інфраструктури	Закон України «Про кібербезпеку України» №2163-VIII	Охоплює питання захисту IT-інфраструктури, даних і зв'язку	Державна служба спеціального зв'язку та захисту інформації	Оцінка ризиків, аудит, державний нагляд, сертифікація
Енергетична інфраструктура	Закон України «Про енергетичну ефективність будівель» №3664-VI	Встановлює вимоги до енергоефективності та модернізації систем	Міненерго, Держенергоефективності	Технічні регламенти, інвестпрограми, контроль за споживанням
Міжнародне співробітництво	Директива ЄС 2008/114/ЄС та Угода про асоціацію з ЄС	Гармонізація стандартів та спільні проєкти з ЄС і НАТО	Єврокомісія, Міністерство закордонних справ України	Проєкти технічної допомоги, обмін досвідом, фінансування
Публічно-приватне партнерство	Закони України про державно-приватне партнерство	Сприяння залученню приватного капіталу до модернізації інфраструктури	Міністерство економіки України, місцеві органи влади	Концесії, договори, інвестпрограми, податкові стимули

*Сформовано автором на основі [33], [34], [35]

У контексті зростаючого спектра ризиків, що супроводжують функціонування держави у воєнний час, а також у період відбудови, суттєвого значення набуває формування комплексного правового механізму, який би визначав повноваження, обов'язки, координаційні функції та відповідальність органів державної влади, залучених до забезпечення безперебійного функціонування об'єктів критичної інфраструктури (КІ), як на загальнодержавному, так і на регіональному рівнях.

Базовим актом, що закладає правову основу діяльності органів державної влади у сфері управління критичною інфраструктурою, є Закон України «Про критичну інфраструктуру». Відповідно до статті 4 цього закону, координацію державної політики в цій сфері здійснює Кабінет Міністрів України, який затверджує нормативно-правові акти, координує діяльність центральних органів виконавчої влади та утворює міжвідомчі координаційні органи, зокрема міжсекторальну робочу групу з питань захисту КІ. У статті 5 передбачено, що національну систему захисту критичної інфраструктури формують уповноважені суб'єкти, серед яких центральні органи виконавчої влади, органи місцевого самоврядування, Служба безпеки України, Національна поліція, Державна служба з надзвичайних ситуацій, Державна служба спеціального зв'язку та захисту інформації, Національний координаційний центр кібербезпеки при РНБО [22].

Роль Кабінету Міністрів України як центрального координатора посилюється також у Постанові № 1109 від 9 жовтня 2020 року "Деякі питання об'єктів критичної інфраструктури", де закріплюється порядок ведення Реєстру об'єктів КІ, порядок їхньої класифікації, а також розподіл повноважень між відповідальними органами. Цей акт визначає, що визначення належності об'єкта до критичної інфраструктури здійснюється на підставі пропозицій суб'єктів, а рішення про внесення до Реєстру ухвалює уповноважений центральний орган виконавчої влади за погодженням з іншими суб'єктами.

Окремо слід наголосити на функціях Державної служби спеціального зв'язку та захисту інформації України, яка згідно з Наказом № 23 від 15 січня

2021 року виконує методичну функцію у сфері категоризації об’єктів критичної інфраструктури, здійснює технічне та аналітичне забезпечення процесу оцінювання, а також розробляє рекомендації з урахуванням специфіки об’єкта. Згідно з пунктом 2 зазначеного наказу, саме Держспецзв’язку є органом, відповідальним за забезпечення інформаційної безпеки, захисту інформаційних систем та каналів зв’язку, які обслуговують об’єкти критичної інфраструктури [9].

Підтримку функціонування об’єктів КІ забезпечує Служба безпеки України, яка відповідно до статті 5 Закону № 1882-IX, є одним із основних суб’єктів захисту критичної інфраструктури та уповноважена здійснювати заходи з виявлення, запобігання та нейтралізації загроз, у тому числі загроз диверсійного, терористичного, кібератакового або гібридного характеру.

У сфері оперативного реагування на надзвичайні ситуації діє Державна служба України з надзвичайних ситуацій (ДСНС), на яку покладено реалізацію державної політики у сфері цивільного захисту, моніторинг техногенних загроз, координацію аварійно-рятувальних заходів, а також безпосереднє управління мобілізаційними ресурсами. Її функціональні повноваження визначено в Законі України «Про цивільний захист населення» та підтверджено у відповідних статтях Закону № 1882-IX. Значну увагу в системі функціонування КІ приділено кібербезпеці, що регламентується Постановою Кабінету Міністрів України від 19 червня 2019 року № 519 «Про затвердження Порядку захисту об’єктів критичної інформаційної інфраструктури» [35]. У документі деталізуються повноваження Національного координаційного центру кібербезпеки при РНБО, Держспецзв’язку та інших уповноважених органів у сфері технічного та криптографічного захисту інформації. Визначено порядок проведення аудитів, оцінки вразливості, забезпечення резервування даних, процедур реагування на кіберінциденти.

Крім того, органи місцевого самоврядування, зокрема обласні та міські військові адміністрації, відповідно до ст. 9 та 10 Закону України «Про критичну інфраструктуру», мають здійснювати повноваження з організації та координації

заходів у межах своєї територіальної юрисдикції. Вони забезпечують виконання державної політики на місцях, беруть участь у розробці кризових планів, забезпечують комунікацію з регіональними операторами та організовують тимчасову мобілізацію ресурсів. Загальнодержавна координація з питань стратегічної безпеки покладається на Раду національної безпеки і оборони України, яка відповідно до Указу Президента України № 695/2023 від 17 жовтня 2023 року координує виконання рішень у сфері захисту КІ, зокрема в енергетичному секторі, та має повноваження формувати політику кризового реагування в умовах воєнного стану [23].

Закон України «Про критичну інфраструктуру» сприяє інтеграції міжнародних стандартів і найкращих практик у сфері захисту та трансформації критичної інфраструктури, що дозволяє Україні адаптувати своє законодавство до норм Європейського Союзу, таких як Директива 2008/114/ЄС про ідентифікацію та позначення європейської критичної інфраструктури, сприяючи впровадженню інноваційних технологій і підходів у модернізацію об’єктів, таких як транспортні системи чи водопостачання, та гармонізації національних норм із міжнародними стандартами. Сьогодні Україна співпрацює з ЄС в плані проєктів із кіберзахисту, що дозволяє підвищувати стійкість критичної інформаційної інфраструктури, а також бере участь у програмах модернізації енергетичної інфраструктури, які передбачають використання відновлюваних джерел енергії, що є важливим кроком на шляху до європейської інтеграції [29].

Разом з тим, для підвищення ефективності нормативно-правового регулювання у розділ доцільно включити посилання на низку нових законів і підзаконних актів, ухвалених у 2023–2025 роках, зокрема: Закон України «Про національну систему кібербезпеки» (2023 р.), який значно розширює повноваження уповноважених органів у сфері захисту інформаційних систем критичної інфраструктури, запроваджує обов’язкові вимоги до кіберзахисту об’єктів та створює умови для інтеграції національної кібербезпекової інфраструктури з європейською мережею CERT-EU [24].

Слід вказати і на Закон України «Про енергетичну безпеку» (2024 р.), що систематизує нормативну базу у сфері захисту енергетичних об'єктів, передбачає створення резервних потужностей та механізмів швидкого відновлення генерації; зміни до Закону України «Про оборону України» (2024 р.) у частині удосконалення управління мобілізаційною підготовкою та цивільним захистом об'єктів критичної інфраструктури. Свій внесок має і Постанова Кабінету Міністрів України № 456 від 12.06.2024 р. «Про затвердження Порядку проведення оцінки вразливості об'єктів критичної інфраструктури», яка вводить уніфіковану методику оцінювання загроз та ризиків. Виділяємо і Національну стратегію захисту та стійкості критичної інфраструктури на 2024–2030 роки, схвалену Указом Президента України у 2024 р., яка визначає стратегічні цілі, пріоритети та індикатори ефективності заходів у цій сфері; а також Концепцію відновлення та модернізації об'єктів критичної інфраструктури в післявоєнний період (2025 р.), що передбачає впровадження принципів «build back better» з урахуванням європейських стандартів безпеки та екологічної стійкості [31].

Закон трактує і можливу співпрацю між державними органами та приватним сектором, що є ключовим для залучення інвестицій, технологій та експертизи в процес трансформації об'єктів критичної інфраструктури, дозволяючи поєднувати державні ресурси з приватним капіталом для реалізації великих проєктів модернізації, таких як оновлення транспортних магістралей чи водопостачальних систем [9]. Таке партнерство сприяє створенню умов для інновацій, залученню міжнародних інвесторів та розподілу ризиків між учасниками, що є надзвичайно доречним фактором, саме у період обмежених бюджетних можливостей, викликаних воєнними діями, які тривають в Україні з 24 лютого 2022 року.

Вагомим елементом нормативно-правового забезпечення, який доцільно розширити, є міжнародно-правова складова, адже Україна, інтегруючись у правовий простір Європейського Союзу, бере на себе зобов'язання з імплементації положень Директиви (EU) 2022/2557 «Про стійкість критичних суб'єктів» та Директиви (EU) 2016/1148 (NIS Directive) у редакції NIS2, що

стосується безпеки мережевих та інформаційних систем. Імплементація цих документів вимагає адаптації українського законодавства до вимог ЄС у частині ідентифікації критичних суб’єктів, оцінки ризиків, обміну інформацією, координації між секторами, а також запровадження системи регулярного звітування та незалежного аудиту. Власне розвиток нормативно-правового забезпечення у сфері критичної інфраструктури має відбуватися на засадах комплексності, скоординованості та адаптивності, що передбачає поєднання превентивних та реактивних інструментів, синхронізацію секторних стратегій (енергетичної, транспортної, кібербезпекової, оборонної) та забезпечення гнучкого механізму оновлення правових норм у відповідь на динаміку загроз. Необхідно також інтегрувати положення про публічно-приватне партнерство, адже значна частина об’єктів критичної інфраструктури належить або експлуатується приватними операторами, і без належної правової бази взаємодії ефективний захист таких об’єктів неможливий.

2.3. Інституційне та організаційно-інформаційне забезпечення публічного управління у сфері трансформації об’єктів критичної інфраструктури

Інституційне забезпечення розуміємо як сукупність органів публічної влади, установ, організацій та операторів, наділених повноваженнями у сфері захисту, функціонування й розвитку критичної інфраструктури, а також правил їхньої взаємодії. Організаційно-інформаційне забезпечення охоплює сукупність процедур, методів і засобів, які забезпечують планування, координацію, обмін інформацією, моніторинг і контроль у процесі управління об'єктами критичної інфраструктури. Саме ця складова перетворює інституційну структуру на дієву систему, здатну ухвалювати обґрунтовані рішення в режимі реального часу.

Ключову координаційну роль у сфері державної політики з питань критичної інфраструктури виконує Кабінет Міністрів України, який визначає стратегічні пріоритети, ухвалює програми розвитку та модернізації галузей, забезпечує узгодженість міжвідомчих дій, а також затверджує нормативно-правові акти, що регламентують порядок захисту, функціонування та відновлення інфраструктурних об'єктів у кризових умовах, при цьому формуючи комплексну політику, що охоплює як питання фізичної безпеки, так і кіберзахисту. Міністерство економіки України здійснює формування та реалізацію економічних інструментів підтримки критичної інфраструктури, розробляє стимули для модернізації виробничих потужностей та впровадження інновацій, а також координує питання державно-приватного партнерства, що дозволяє залучати інвестиції в інфраструктурні об'єкти та зменшувати навантаження на державний бюджет при одночасному підвищенні якості та стійкості послуг, що ними забезпечуються [6, с. 179-180].

Міністерство внутрішніх справ України відповідає за забезпечення громадської безпеки та охорону об'єктів критичної інфраструктури, здійснює організацію сил охорони, координує діяльність Національної поліції та Державної служби України з надзвичайних ситуацій у частині запобігання та ліквідації наслідків аварій, диверсій чи терористичних актів, що можуть поставити під загрозу безперервність роботи важливих систем [42, с. 34].

Державна служба України з надзвичайних ситуацій (ДСНС) виконує функції оперативного реагування на надзвичайні ситуації, організовує рятувальні та відновлювальні роботи, здійснює контроль за готовністю об'єктів критичної інфраструктури до дій в умовах кризових сценаріїв, проводить навчання персоналу та тренування сил цивільного захисту, а також формує рекомендації щодо підвищення стійкості інженерних і технологічних систем.

Служба безпеки України (СБУ) має повноваження з протидії терористичним загрозам та диверсіям, проводить розвідувально-контррозвідувальні заходи з виявлення потенційних ризиків у сфері критичної інфраструктури, координує заходи з кіберзахисту, а також забезпечує захист

інформації з обмеженим доступом, що стосується вразливостей інфраструктурних об’єктів та планів їхнього захисту.

Міністерство енергетики України займається управлінням об’єктами енергетичної інфраструктури, розробляє галузеві стратегії підвищення енергоефективності та енергетичної безпеки, забезпечує інтеграцію національної енергосистеми з європейською, а також координує відновлення об’єктів, пошкоджених унаслідок надзвичайних ситуацій чи воєнних дій, впроваджуючи сучасні технологічні рішення для зменшення залежності від централізованих систем постачання [52].

Міністерство інфраструктури України відповідає за транспортні та логістичні об’єкти, організовує процеси модернізації транспортних мереж, забезпечує функціонування морських, залізничних, автомобільних і авіаційних сполучень, розробляє плани відновлення інфраструктурних вузлів у разі їх пошкодження, а також координує взаємодію з міжнародними партнерами щодо отримання технічної та фінансової допомоги для відновлення й розвитку транспортної інфраструктури.

Міністерство цифрової трансформації України забезпечує розвиток цифрової інфраструктури, координує впровадження технологій кіберзахисту та моніторингу, відповідає за створення і функціонування національних платформ управління даними, здійснює впровадження електронних сервісів, які дозволяють здійснювати оперативний обмін інформацією між суб’єктами критичної інфраструктури, а також реалізує проєкти з цифрової стійкості, включаючи захист від кібератак та технологічних збоїв. Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг (НКРЕКП) виконує функції контролю та регулювання діяльності підприємств енергетичного та комунального секторів, встановлює тарифи, затверджує технічні стандарти, проводить перевірки дотримання вимог безпеки, а також координує взаємодію між виробниками, операторами та споживачами критично важливих ресурсів. Територіальні органи міністерств і центральних органів виконавчої влади забезпечують безпеку об’єктів критичної інфраструктури на

територіальному рівні, здійснюють моніторинг їхнього стану, організовують заходи із захисту, евакуації населення та відновлення функціонування систем життєзабезпечення, а також координують взаємодію з регіональними підрозділами центральних органів виконавчої влади [37, 39].

Обласні державні (військові) адміністрації, включаючи обласні державні адміністрації та міські ради, відіграють важливу роль у локальному управлінні критичною інфраструктурою, відповідаючи за ідентифікацію та категоризацію об'єктів на своїй території, моніторинг їхнього стану, а також координацію дій з операторами та центральними органами влади, що дозволяє враховувати регіональні особливості, такі як кліматичні умови чи специфіка транспортних мереж, при реалізації проєктів модернізації. Так у свою чергу, регіональні адміністрації можуть визначати пріоритетні об'єкти, такі як місцеві водопостачальні системи чи транспортні вузли, які потребують негайного оновлення, і співпрацювати з операторами для реалізації відповідних заходів, адаптуючи загальнодержавні політики до місцевих потреб [9].

Оператори критичної інфраструктури, які є юридичними особами, що володіють або управляють об'єктами, такими як енергетичні компанії, транспортні оператори чи телекомунікаційні провайдери, відіграють ключову роль у забезпеченні їхньої безпечної та надійної роботи, впровадженні заходів зниження ризиків, а також у співпраці з державними органами для моніторингу, захисту та модернізації цих об'єктів, що є необхідним для підтримки їхньої стійкості в умовах воєнного стану та інших криз. Закон встановлює вимоги до операторів щодо проведення регулярних оцінок ризиків, розробки планів дій у разі надзвичайних ситуацій, впровадження заходів фізичного та кіберзахисту, а також інвестування в модернізацію об'єктів, таких як електростанції чи водоочисні споруди, для забезпечення їхньої довгострокової функціональності, що сприяє підвищенню загальної стійкості критичної інфраструктури [7, с. 261].

Трансформація об'єктів критичної інфраструктури, таких як енергетичні мережі, транспортні системи, водопостачання та телекомунікаційні об'єкти, є стратегічним напрямком їхнього управління, особливо в умовах швидких

технологічних змін, зростання попиту на інфраструктурні послуги, а також необхідності адаптації до нових викликів, таких як цифровізація, зміна кліматичних умов чи урбанізація, що вимагає впровадження інноваційних підходів, технологій та інвестицій для забезпечення їхньої стійкості, ефективності та відповідності сучасним стандартам. Закон України «Про критичну інфраструктуру» (Закон №1882-IX) передбачає низку механізмів, які сприяють модернізації та покращенню функціональності цих об'єктів, створюючи умови для їхньої адаптації до потреб суспільства та інтеграції в європейський простір, що є поточним пріоритетом України [29].

Одним з способів трансформації є процедура ідентифікації та категоризації об'єктів критичної інфраструктури, яка дозволяє державним органам у співпраці з операторами визначити об'єкти, що мають стратегічне значення для забезпечення життєдіяльності суспільства, такі як електростанції, залізничні вузли, водоочисні споруди чи телекомунікаційні центри, а також класифікувати їх за рівнем критичності, що сприяє пріоритизації ресурсів і зусиль для їхньої модернізації та захисту [20, с. 74]. Виділена процедура включає оцінку потенційного впливу порушень на функціонування суспільства, визначення їхньої ролі в національній системі та розробку планів дій для їхнього оновлення, що дозволяє державі зосередитися на найбільш важливих об'єктах і забезпечити їхню стійкість у довгостроковій перспективі. Організаційно-управлінський механізм у сфері трансформації критичної інфраструктури доцільно розглядати як динамічну сукупність інституційних повноважень, адміністративно-правових рішень та координаційних дій, які реалізуються через взаємодію між секторальними координаторами, органами загальної компетенції та виконавцями проєктних рішень. У цьому контексті важливо забезпечити не лише вертикальну інтеграцію управлінських дій, але й горизонтальну взаємодію суб'єктів публічного управління для досягнення ефективної трансформації об'єктів критичної інфраструктури на національному та регіональному рівнях [55]. До функціональних блоків, які формують організаційно-управлінське забезпечення трансформаційних процесів у зазначеній сфері, належать:

– інфраструктурно-обліковий блок, який відповідає за централізоване збирання, актуалізацію та верифікацію інформації про стан об’єктів критичної інфраструктури, їхній технічний ресурс, строк служби та рівень експлуатаційної придатності;

– міжвідомчо-координаційний блок, завданням якого є забезпечення скоординованих управлінських дій між Кабінетом Міністрів України, центральними органами виконавчої влади, військовими адміністраціями та органами місцевого самоврядування щодо реалізації державної політики трансформації КІ;

– аналітично-прогностичний блок, що виконує функції формування варіантів розвитку інфраструктурних змін із урахуванням імовірнісного моделювання ризиків, потреб безпеки громад, індикаторів зношеності та адаптації до стратегічних викликів;

– ресурсно-забезпечувальний блок, який визначає джерела фінансування, формує резерви матеріально-технічних засобів, забезпечує кадрове наповнення та логістику реалізації інфраструктурних рішень;

– інформаційно-аналітичний блок, що забезпечує безперервний моніторинг стану реалізації управлінських заходів, оцінює динаміку їх ефективності та забезпечує прозорість результатів для всіх зацікавлених сторін.

Окрім структурної побудови, механізм публічного управління трансформацією об’єктів критичної інфраструктури виконує низку ключових функцій:

1) Створення національної цифрової платформи для обліку, інвентаризації та аналізу технічного стану об’єктів КІ, що дозволяє оперативно виявляти ризики порушення функціонування та ініціювати відповідні управлінські рішення.

2) Проведення пріоритетизації об’єктів щодо модернізації, що ґрунтується на результатах експертної оцінки технічного стану, функціонального значення, соціального впливу та рівня критичності кожного об’єкта в загальнонаціональній мережі.

3) Формування ефективних механізмів міжінституційної взаємодії, у межах яких забезпечується узгодженість дій між міністерствами, агентствами, Службою безпеки України, Держспецзв'язку, ДСНС, Національною поліцією, а також іншими суб'єктами відповідно до законодавства [60, с. 63–64].

4) Забезпечення наявності резервних потужностей та ресурсів, які можуть бути оперативно використані в умовах виникнення аварійних ситуацій, воєнних дій або природних катастроф.

Проведення своєчасного аналізу нових управлінських викликів, включаючи кіберзагрози, порушення логістики або втрату функціональності об'єкта, з метою адаптації планів реагування та довгострокових програм трансформації.Оцінювання результативності реалізованих проєктів трансформації з використанням індикаторів ефективності, економічної доцільності, соціального ефекту та технологічної інноваційності з подальшою корекцією стратегії трансформації для підвищення загальної інфраструктурної стійкості держави [60, с. 64].

У такій взаємодії особливу роль відіграють механізми багаторівневої координації, які забезпечують узгодженість рішень у сфері впровадження інфраструктурних змін, включаючи розробку, затвердження та реалізацію проєктів трансформації, спрямованих на досягнення функціональної надійності та стійкості об'єктів критичної інфраструктури [50, 53]. Одним з засадничих компонентів механізму є створення та ведення системи підсумкових і проміжних документів, які відображають стан виконання проєктних завдань на локальному, регіональному й національному рівнях, базуючись на стратегічних планах розвитку відповідних територій і галузей. Такі документи мають виступати інструментом звітності та основою для прийняття коригувальних управлінських рішень, що, своєю чергою, дозволяє гармонізувати дії всіх залучених суб'єктів у напрямі досягнення єдиної цілісної стратегії трансформації інфраструктури в умовах динамічних змін безпекового середовища [48, с. 183]. Така узгодженість, як на рівні окремих громад, так і в контексті регіональної координації, створює підґрунтя для формування ефективної інституційної моделі, яка дозволяє

інтегрувати управлінські ресурси, планові документи, технічні засоби у межах єдиної системи трансформаційного управління (рис. 2.7).

Відзначаємо, що в процесі публічного управління необхідно враховувати багаторівневу взаємодію між центральними органами виконавчої влади, місцевими державними адміністраціями, органами місцевого самоврядування, а також профільними технічними операторами й аналітичними структурами, що дозволяє здійснювати комплексне планування, координацію та реалізацію заходів модернізації інфраструктури. Систематизація завдань оцінки ефективності функціонування такого механізму доцільна за кількома основними напрямами:

1. Оперативно-технічний напрям, у межах якого відбувається постійний моніторинг технічного стану об’єктів критичної інфраструктури, оцінка відповідності нормативно-технічним регламентам, виявлення потенційних ризиків, здійснення своєчасного реагування з боку органів державної влади та реалізація стабілізаційних заходів у випадку виявлення критичних порушень у роботі інфраструктурних елементів;

2. Стратегічно-планувальний напрям, який передбачає формування довгострокових сценаріїв трансформації інфраструктури, розроблення державної та регіональних політик модернізації, формування оновлених інфраструктурних карт, а також забезпечення координації дій між центральними і місцевими органами влади, галузевими експертами, громадськими структурами та представниками бізнесу [52];

3. Інтеграційно-аналітичний напрям, що полягає у побудові узгоджених моделей трансформації, формуванні системних стратегій модернізації з урахуванням потреб національної безпеки, соціально-економічних пріоритетів та загроз техногенного і природного характеру, а також у забезпеченні збалансованого розподілу управлінських та технічних ресурсів, що є особливо важливим в умовах високої концентрації ризиків для об’єктів критичної інфраструктури (табл. 2.6).



Рис. 2.7. Організаційно-управлінська взаємодія органів державної влади при забезпеченні роботи об'єктів критичної інфраструктури у системі публічного управління* *Джерело: власна розробка автора

Таблиця 2.6

Структура завдань у системі управління трансформацією об’єктів критичної інфраструктури*

№	Завдання 1 рівня (Поточні)	Завдання 2 рівня (Стратегічні)	Завдання 3 рівня (Загальні)
1	Виявлення та систематизація особливостей функціонування об’єктів критичної інфраструктури, таких як енергетичні мережі чи транспортні системи, на рівні окремих громад та регіонів для визначення їхнього поточного стану та потреб у модернізації	Складання прогнозних планів розвитку об’єктів критичної інфраструктури, таких як водопостачання чи телекомунікаційні об’єкти, з урахуванням регіональних особливостей та перспектив їхнього вдосконалення	Розробка комплексу превентивних заходів для забезпечення ефективного оновлення об’єктів критичної інфраструктури на національному та регіональному рівнях
2	Аналіз стану об’єктів критичної інфраструктури, таких як транспортні вузли чи інформаційні мережі, на рівні громад і регіонів для оцінки їхньої готовності до трансформаційних змін	Розробка програм, спрямованих на підвищення ефективності трансформації об’єктів критичної інфраструктури, таких як енергетичні системи чи водопостачання, з урахуванням місцевих потреб і ресурсів	Створення планів для вдосконалення об’єктів критичної інфраструктури, які сприяють їхній адаптації до нових технологій і потреб громад
3	Оцінка рівня готовності об’єктів критичної інфраструктури, таких як телекомунікаційні мережі чи транспортні артерії, до реалізації проєктів модернізації на рівні регіонів	Формування стратегічних планів розвитку ключових об’єктів критичної інфраструктури, таких як енергетичні об’єкти чи водопостачальні системи, з урахуванням регіональних особливостей і потенціалу	Визначення напрямів розвитку об’єктів критичної інфраструктури, які підтримують їхню стійкість і функціональність на різних рівнях
4	Ранжування регіонів за станом об’єктів критичної інфраструктури, таких як транспортні мережі чи системи водопостачання, для пріоритетного планування їхньої трансформації	Розробка комплексних програм розвитку інноваційних підходів до трансформації об’єктів критичної інфраструктури, таких як телекомунікаційні системи чи енергетичні мережі, з урахуванням регіональних ресурсів	Формування резервів для забезпечення безперервного вдосконалення об’єктів критичної інфраструктури на рівні громад і регіонів
5	Оцінка ефективності реалізації проєктів трансформації об’єктів критичної інфраструктури, таких як водопостачання чи транспортні системи, на рівні громад і регіонів	Прогнозування сценаріїв розвитку об’єктів критичної інфраструктури, таких як енергетичні мережі чи телекомунікаційні об’єкти, на основі впровадження інноваційних підходів до управління	Визначення зон пріоритетного розвитку об’єктів критичної інфраструктури для їхньої модернізації на національному та регіональному рівнях

*Джерело: власна розробка автора

Враховуючи, що ключовими об’єктами критичної інфраструктури залишаються енергетичні мережі, транспортні вузли, водопровідні системи, телекомунікаційні структури, а також об’єкти цифрової інфраструктури, органи державної влади, залучені до процесів управління цими системами, повинні діяти в тісній міжвідомчій взаємодії, застосовуючи інтегрований аналіз ефективності публічного управління. Дослідження, спрямоване на оцінку результативності управління в Україні, включає кілька логічних і послідовних етапів аналізу, які дають змогу визначити потенціал для покращення трансформації об’єктів критичної інфраструктури на різних рівнях, а отримані висновки узагальнюються в стратегічному документі, що використовується для коригування ключових напрямів розвитку, як це продемонстровано на рис. 2.8., відображаючи системний підхід до поєднання зусиль у загальному процесі управління.

Виокремимо три основні взаємопов’язані етапи оцінки функціонування відповідних підсистем, а саме: підготовчий, аналітичний та проєктний, кожен з яких передбачає реалізацію певної сукупності управлінських дій, що спираються на актуальну, достовірну інформаційну базу, забезпечуючи таким чином умови для точного виявлення реального стану об’єктів критичної інфраструктури й формування дієвих рішень щодо їх оновлення як у межах окремих територіальних громад, так і на рівні регіональних об’єднань [59].

Підготовчий етап включає організацію збору первинних даних із залученням відповідних державних органів виконавчої влади, органів місцевого самоврядування, галузевих регуляторів, а також операторів об’єктів критичної інфраструктури, що уможливлює створення комплексної інформаційної основи для подальших аналітичних процедур. У свою чергу, аналітичний етап передбачає проведення систематизованого аналізу зовнішнього середовища, в межах якого оцінюються політичні, соціальні, технологічні та інституційні чинники, що безпосередньо чи опосередковано впливають на функціонування та модернізацію критичної інфраструктури, а також дозволяє ідентифікувати вузькі місця та вразливості в наявних моделях управління [47].

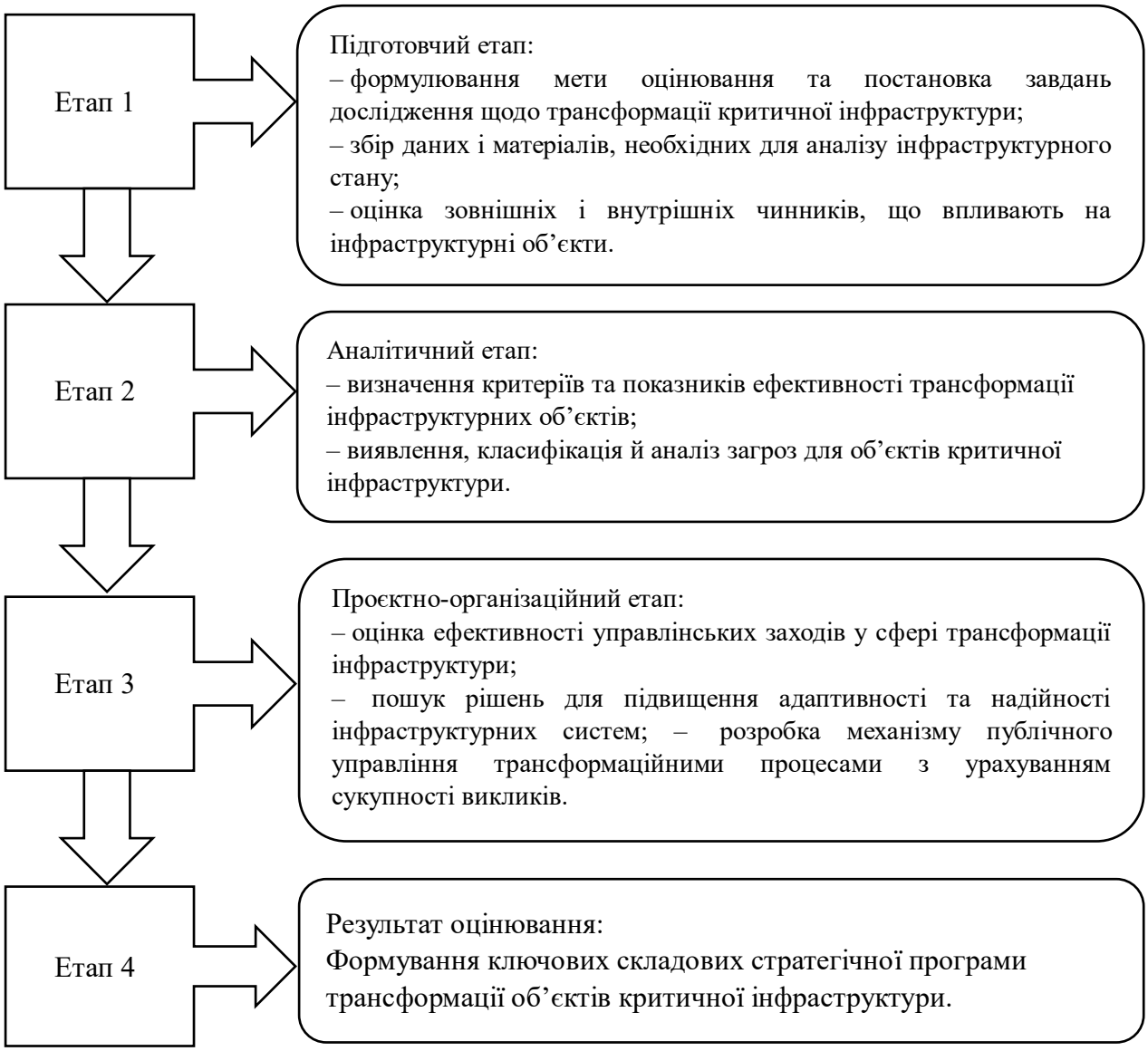


Рис. 2.8. Етапи публічного управління процесом трансформації об'єктів критичної інфраструктури України *

*Джерело: власна розробка автора

Результати аналітичної фази, отримані за активної взаємодії між різними рівнями влади, включаючи центральні органи виконавчої влади (наприклад, Міністерство з питань стратегічних галузей промисловості, Міністерство енергетики, Державну службу спеціального зв'язку та захисту інформації України) та місцеві адміністрації, формують основу для переходу до проєктного етапу, що передбачає розробку конкретних заходів, спрямованих на підвищення функціональної, технічної та управлінської ефективності об'єктів критичної інфраструктури. Ці заходи ґрунтуються на принципах міжвідомчої координації,

чіткої ієрархії відповідальності та ефективного розподілу ресурсів, що уможливлює досягнення синергії між управлінськими структурами різного рівня [54].

Водночас, у процесі здійснення аналітичної оцінки, особливого значення набуває узгоджена діяльність усіх суб'єктів, які беруть участь в управлінні трансформаційними процесами в інфраструктурному секторі, включаючи не лише державні інституції, а й представників приватного сектору, експертних організацій та громадянського суспільства, що забезпечує комплексний і багатогранний підхід до виявлення реальних потреб та можливостей об'єктів критичної інфраструктури в умовах динамічних змін безпекового, техногенного та економічного характеру [59].

Аналіз ефективності публічного управління трансформацією об'єктів критичної інфраструктури ускладнюється неоднорідністю самих об'єктів, що належать до різних секторів, таких як енергетика, транспорт, водопостачання чи телекомунікації, що вимагає диференційованого підходу до взаємодії органів державної влади, з урахуванням технічної специфіки, рівня зносу, географічного положення та важливості конкретного об'єкта для забезпечення національної безпеки. У цьому контексті важливою умовою є координація дій між уповноваженими органами на центральному рівні, зокрема Кабінетом Міністрів України, Радою національної безпеки і оборони України та відповідними профільними міністерствами, і їх територіальними підрозділами, які безпосередньо взаємодіють з об'єктами на місцях. У межах організаційно-управлінського забезпечення трансформації об'єктів критичної інфраструктури слід зазначити необхідність впровадження системи регулярного міжвідомчого обміну інформацією, що дає змогу не лише вчасно реагувати на потенційні загрози, але й формувати обґрунтовані рішення з урахуванням реальної ситуації у відповідній галузі чи регіоні. Така інформаційна взаємодія забезпечується, зокрема, через реалізацію положень Постанови Кабінету Міністрів України від 14 жовтня 2022 року № 1174 «Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури» [59].

Узгодженість дій між усіма ланками управлінської вертикалі відіграє свою роль у забезпеченні ефективності трансформації критичної інфраструктури, оскільки саме від якості та злагодженості організаційної взаємодії залежить здатність своєчасно виявити проблемні ділянки, ефективно мобілізувати ресурси та реалізувати технічні й організаційні заходи, спрямовані на підвищення рівня стійкості й безпеки таких об’єктів (рис. 2.7). Саме тому всі етапи оцінки та впровадження заходів мають відбуватись у тісному координаційному зв’язку між центральними органами виконавчої влади, обласними державними адміністраціями, органами місцевого самоврядування, а також уповноваженими технічними операторами об’єктів критичної інфраструктури, які несуть відповідальність за їх технічний та експлуатаційний стан [47].

Крім того, ефективне організаційно-управлінське забезпечення вимагає постійного вдосконалення нормативно-правового регулювання взаємодії між суб’єктами управління, зокрема шляхом оновлення механізмів контролю, звітності та оцінювання ефективності дій, а також шляхом зміцнення інституційної спроможності органів влади через впровадження стандартів електронного урядування, автоматизованих систем моніторингу та управління ризиками, що дозволяє підвищити швидкість реагування на критичні ситуації та забезпечити безперервність функціонування інфраструктурних об’єктів [59].

Ключового значення набуває врахування не лише фактичного технічного стану інфраструктурних систем, а й рівня налагодженості управлінської координації між різними гілками та рівнями державної влади, включаючи центральні органи виконавчої влади, обласні адміністрації, структурні підрозділи місцевого самоврядування, а також спеціалізовані агентства, які безпосередньо відповідають за експлуатацію та безпеку відповідних об’єктів [56] (рис. 2.9.).

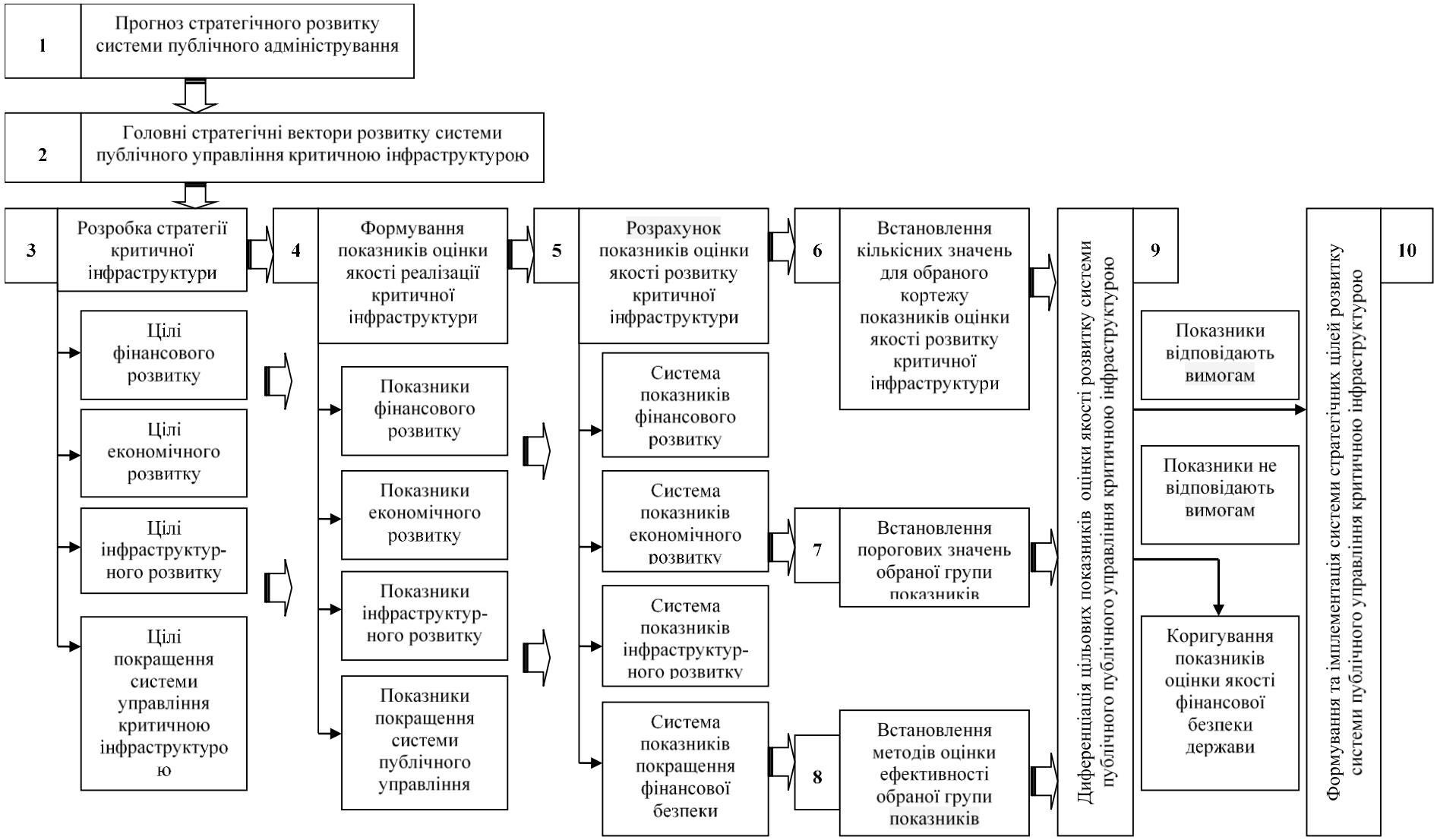


Рис. 2.9. Структурно-логічна модель стратегічного управління в системі адміністрування трансформації об’єктів критичної інфраструктури* *Джерело: власна розробка автора

Формування єдиного управлінського контексту у сфері трансформації критичної інфраструктури потребує розробки цілісної системи заходів, які, окрім врахування технічного зношення, фізичних і кіберзагроз, повинні передбачати встановлення постійних каналів комунікації між усіма зацікавленими суб’єктами державного управління для забезпечення безперебійного обміну інформацією та оперативного реагування на зовнішні виклики. При цьому особлива увага приділяється спроможності регіональних і муніципальних управлінських структур самостійно реалізовувати покладені на них завдання в межах повноважень, що вимагає налагоджених механізмів вертикальної та горизонтальної взаємодії в межах єдиної системи управління [56].

На практичному рівні організаційно-управлінське забезпечення функціонування об’єктів критичної інфраструктури передбачає чітку регламентацію дій органів виконавчої влади у випадках порушення стабільності роботи об’єкта, введення тимчасових режимів управління, організацію технічної підтримки, а також мобілізацію ресурсів через спеціально уповноважені державні органи, такі як Державна служба з надзвичайних ситуацій, Держспецзв'язку, Державна служба енергетичного нагляду тощо [26].

Система публічного управління у зазначеній сфері базується на постійній адаптації управлінських підходів до нових умов, що виникають унаслідок внутрішніх змін (наприклад, структурна деградація об'єктів) або зовнішніх факторів (збройна агресія, технологічні катастрофи, кібератаки), і передбачає відповідну трансформацію методів взаємодії між центральними та місцевими органами влади, а також зміцнення спроможності публічних інституцій реагувати на загрози в реальному часі [26].

Особливість управління об’єктами критичної інфраструктури полягає в необхідності чіткого дотримання міжвідомчих протоколів і функціонального узгодження дій між представниками органів влади різних сфер — зокрема, оборони, енергетики, цифрової трансформації, внутрішніх справ і охорони здоров’я, що забезпечується через спільні наради, координаційні центри, обмін ситуаційними звітами та участь у спільних навчаннях із моделюванням кризових ситуацій. Підвищення ефективності публічного управління в сфері трансформації

критичної інфраструктури неможливе без оновлення організаційних механізмів, зокрема розширення функціональних повноважень оперативних центрів, створення інтегрованих ситуаційних платформ, що забезпечують постійний моніторинг стану об'єктів, а також впровадження цифрових інструментів для автоматизованого аналізу даних і прогнозування критичних ситуацій із подальшим оперативним інформуванням відповідальних органів [11].

Найвищий рівень організаційної структури регіону у контексті управління критичною інфраструктурою репрезентується через систему публічного управління, яка втілює інституційну сутність території та реалізує управлінський вплив через формування програм трансформації, модернізації або переоснащення об'єктів, що мають вирішальне значення для життєдіяльності населення та функціонування базових сервісів (тал. 2.7).

Таблиця 2.7

Основні характеристики управління трансформацією об'єктів критичної інфраструктури в межах регіонального публічного адміністрування*

№	Регіон (область, територія)	Структури, що займаються трансформацією об'єктів критичної інфраструктури
1	Об'єкт управління	Сукупність регіонально розташованих об'єктів критичної інфраструктури, до складу яких входять енергетичні установки, транспортні вузли, системи водопостачання, телекомунікаційні мережі, а також елементи інженерної інфраструктури громадського призначення, управління якими здійснюється у тісній взаємодії між центральними органами виконавчої влади, регіональними адміністраціями та спеціалізованими службами.
2	Предмет управління	Забезпечення безперервної та безпечної експлуатації, модернізації та функціонального вдосконалення об'єктів критичної інфраструктури шляхом скоординованих дій між центральними державними структурами (Кабінет Міністрів України, відповідні міністерства), обласними військовими адміністраціями, місцевими органами самоврядування та територіальними підрозділами спеціалізованих інфраструктурних операторів.
3	Засоби управління	Організаційно-управлінські інструменти, до яких належать регламенти, міжвідомчі протоколи, положення про взаємодію органів влади, а також механізми міжрівневої координації, які забезпечують реалізацію функцій управління об'єктами критичної інфраструктури через взаємодію центральних та місцевих державних органів, структур цивільного захисту, комунальних служб і представників приватного сектора.

№	Регіон (область, територія)	Структури, що займаються трансформацією об’єктів критичної інфраструктури
4	Хронологічні межі управління	Період, протягом якого реалізується комплекс організаційно-управлінських рішень щодо трансформації об’єктів критичної інфраструктури в умовах багаторівневої взаємодії між державними структурами; зазвичай охоплює середньо- та довгострокові часові рамки (від 5 до 10 років), протягом яких здійснюється моніторинг, оцінювання стану об’єктів, узгодження ресурсного забезпечення та оперативне реагування на виклики і загрози.

*Джерело: власна розробка автора

Публічне управління, яке спрямоване на забезпечення трансформацію об’єктів критичної інфраструктури, передбачає необхідність чіткого визначення стратегічної візії розвитку, формулювання тактичних цілей, визначення ресурсного забезпечення, а також формування множини альтернативних сценаріїв розвитку кожного окремого об’єкта або інфраструктурного комплексу залежно від рівня його критичності та стану зносу. Управління в межах системи (*Y*) здійснюється за схемою:

$$Y \leftrightarrow \left| T \rightarrow S \rightarrow F \right|, \tag{2.1}$$

де: Т – цілі розвитку критичної інфраструктури; *S* – сукупність способів, засобів впливів, за допомогою яких формуються цілі розвитку; *F* – факт досягнення мети.

Незважаючи на проведені та триваючі дослідження у сфері функціонування критичної інфраструктури, існує нагальна потреба у подальшому вдосконаленні підходів до комплексного врахування багатофакторного впливу, що охоплює інфраструктурні, технічні, організаційні та нормативні аспекти, необхідні для ефективної підтримки процесів ухвалення управлінських рішень під час експлуатації та трансформації об’єктів критичної інфраструктури.

Ускладнення процесів функціонування інфраструктурних систем, що супроводжуються зростанням значущості взаємозалежності окремих елементів критичної інфраструктури, особливої ваги набуває забезпечення ефективної взаємодії між державними інституціями різних рівнів, які відповідають за

координацію, контроль і підтримку цілісності функціонування відповідних об’єктів, при цьому проблема ускладнюється відсутністю належного рівня розвитку регуляторних механізмів та методичних інструментів, які дозволяли б ідентифікувати та аналітично оцінювати міжелементні взаємозв’язки в межах єдиної системи публічного управління [16, с. 78-79].

Одним із ключових засобів практичного впровадження управлінських рішень у сфері трансформації об’єктів критичної інфраструктури виступає регіональна політика, яка формується з урахуванням потенціалу території, включаючи наявність кваліфікованого кадрового ресурсу, інноваційних і технологічних можливостей, інфраструктурної бази та реалізується через інструменти міжвідомчої взаємодії між органами державної влади, місцевого самоврядування, галузевими службами та уповноваженими технічними структурами.

Сучасна практика реалізації публічного управління у зазначеній сфері потребує переорієнтації з жорстко ієрархічного адміністрування на моделі горизонтальної взаємодії, за яких функції з прийняття рішень та їх реалізації розподіляються між кількома центрами, що представляють інтереси держави, регіону та громад, і які здатні узгоджено координувати дії, адаптуючи інфраструктурні системи до викликів сьогодення. У цьому контексті аналіз управлінських процесів, що стосуються трансформації критичної інфраструктури, має передбачати поглиблене вивчення зовнішніх і внутрішніх характеристик регіонального середовища, зокрема оцінку технічного стану об’єктів, їхньої вразливості до ризиків, функціонального ресурсу та ступеня готовності місцевих управлінських структур до оперативного реагування на потенційні загрози.

Визначення ролі та функцій органів державної влади у межах такого аналізу дозволяє чітко окреслити зони відповідальності та напрямки спільної роботи щодо підвищення ефективності управління об’єктами критичної інфраструктури, включаючи взаємодію з Державною службою з надзвичайних ситуацій, Державним агентством енергетичної ефективності, центральними

органами виконавчої влади, відповідальними за окремі інфраструктурні сегменти, а також з регіональними і місцевими адміністраціями [5].

Процедури оцінювання результативності спільної роботи державних органів передбачають поетапний підхід: спочатку виконується глибокий аналіз стану інфраструктурного комплексу на регіональному рівні, далі визначаються функціональні пріоритети у взаємодії між органами влади, після чого розробляються й реалізуються спільні заходи щодо технічного або організаційного оновлення об’єктів, а на завершальному етапі здійснюється моніторинг і контроль за досягнутими результатами на основі чітко встановлених індикаторів.

Описаний цикл управлінських дій формує своєрідну логіку координації, яка забезпечує не лише своєчасну реакцію на ризики, що виникають у критичній інфраструктурі, але й підвищує адаптивність державного управління до складних ситуацій шляхом залучення міжвідомчих комунікаційних механізмів, інтеграції цифрових інструментів обміну інформацією та створення єдиних інформаційно-аналітичних платформ для використання у процесі ухвалення рішень.

У підсумку, належне організаційно-управлінське забезпечення публічного управління у сфері трансформації об’єктів критичної інфраструктури повинне ґрунтуватися на моделі багатоаспектної взаємодії державних органів, яка передбачає гнучкий розподіл функцій, спільне використання ресурсів, уніфіковану нормативно-правову базу, а також здатність до колективного вироблення рішень у відповідь на виклики, які мають потенційний вплив на стабільність і життєздатність інфраструктурного середовища [5].

До управлінських компонентів, які мають бути інтегровані в систему організаційно-управлінського забезпечення публічного управління у сфері трансформації об’єктів критичної інфраструктури, належать кілька функціональних форматів, що охоплюють усі аспекти взаємодії державних органів, з урахуванням як їхньої адміністративної вертикалі, так і горизонтальної координації між структурами національного, регіонального й муніципального рівнів.

Насамперед, інституційно-координаційний формат управління передбачає налагодження цілісної системи погодження дій між усіма учасниками публічного адміністрування, що залучені до процесу зміни та адаптації об’єктів критичної інфраструктури. Йдеться, зокрема, про забезпечення узгодженості рішень, прийнятих на рівні центральних органів виконавчої влади, із позиціями профільних регіональних адміністрацій, а також про створення дієвих механізмів інформаційного обміну та спільного моніторингу реалізації заходів із технічного вдосконалення інфраструктурних систем, з огляду на новітні загрози як природного, так і техногенного чи військового характеру [22, с. 172].

У межах функціонально-інфраструктурного формату здійснюється комплексне оцінювання технічної спроможності об’єктів до виконання критичних функцій за умов ускладненої експлуатації або часткової деструкції. Органи державної влади, що здійснюють регуляцію у сфері інфраструктури, мають забезпечити системну інвентаризацію ключових об’єктів, визначаючи їх адаптивний потенціал, здатність до масштабування, гнучкість конфігурацій та рівень резервного забезпечення у випадку аварій або надзвичайних ситуацій.

Не менш важливим є кадрово-освітній формат, у межах якого повинно бути забезпечено формування якісного людського капіталу, здатного ефективно реалізовувати заходи з управління інфраструктурними трансформаціями. До обов’язків органів державної влади у цій площині входить розробка програм підготовки й підвищення кваліфікації фахівців, які працюють на перетині інженерного, управлінського та технологічного профілів, зокрема спеціалістів із технічного обслуговування об’єктів, інженерів з безпеки та аналітиків інфраструктурних систем. У свою чергу, екологічно-ресурсний формат акцентує увагу на необхідності інтеграції екологічних стандартів і норм природокористування у всі етапи процесу трансформації, що має на меті забезпечення екологічної безпеки та зменшення техногенного впливу об’єктів критичної інфраструктури на навколишнє середовище. Це передбачає, зокрема, впровадження регенеративних технологій, формування циклів замкненого використання ресурсів, а також модернізацію застарілих систем із метою досягнення енергоефективності та зниження викидів шкідливих речовин.

Просторово-інженерний формат охоплює аспекти раціонального планування територій, зайнятих об’єктами критичної інфраструктури. Тут органи публічного управління мають забезпечити інтеграцію інфраструктурних рішень із потребами міської забудови, логістики та з урахуванням норм сучасної урбаністики. Важливим є оптимальне розміщення виробничих, транспортних, комунальних та захисних об’єктів, з огляду на вимоги безпеки, доступності та сталого розвитку.

Останній із ключових форматів це технологічно-інноваційний, який утворює активне впровадження новітніх цифрових платформ управління, інтелектуальних систем прогнозування та автоматизованих моделей діагностики. Центральні й регіональні органи державної влади мають координувати заходи з упровадження інновацій у сфері експлуатації, обслуговування й реконструкції інфраструктурних об’єктів, сприяти розвитку вітчизняних розробок та адаптації передових технологій.

Таким чином, ефективне організаційно-управлінське забезпечення процесу трансформації об’єктів критичної інфраструктури вимагає побудови міжсекторальної координації, у межах якої кожен з наведених форматів має чітке функціональне призначення й взаємодіє з іншими через створення єдиної системи інформаційної підтримки, спільного нормативного поля та ієрархічно узгоджених механізмів прийняття управлінських рішень. У результаті такої системної взаємодії органів державної влади створюється цілісне інституційне середовище, здатне реагувати на нові виклики, забезпечувати надійність функціонування інфраструктурних об’єктів і забезпечувати їх цілеспрямовану модернізацію в інтересах безпеки та сталого розвитку країни [22, с. 172].

Висновки до розділу 2

1. Встановлено, що ефективне управління трансформаційними процесами в сфері критичної інфраструктури має ґрунтуватися на багаторівневій інтеграції, від стратегічного планування на рівні держави до конкретних оперативних

заходів на локальному рівні, що враховує регіональні особливості та специфіку навантажень на інфраструктуру. Обґрунтовано доцільність створення інтегрованої моделі публічного управління, яка поєднає стратегічну спрямованість центральних органів влади з гнучкістю регіональних структур та здатністю швидко реагувати на внутрішні й зовнішні загрози. Розроблено концептуальну модель взаємодії суб'єктів управління, побудовану на принципах синергії, вертикальної відповідальності та цільової результативності, що забезпечує узгодження інтересів усіх сторін, задіяних у модернізації. Також запропоновано новий набір показників ефективності управління, який враховує не лише економічні та технічні параметри, але й рівень адаптивності, цифрової зрілості, швидкості реакції на зміни та наявність стратегічних резервів.

2. У ході аналізу нормативно-правового регулювання сфери публічного управління критичною інфраструктурою (включно з її захистом, безпекою, стійкістю та трансформацією) виявлено суттєві зрушення в правовій сфері України, серед яких ключовим стало прийняття Закону України «Про критичну інфраструктуру» №1882-IX. Нормативний документ створив інституційну основу для формування національної політики в даній області. Досліджено, що ефективність правового механізму залежить від здатності нормативних актів об'єднати секторальні правила, кризове управління, кібербезпеку, стратегічне планування та міжвідомчу взаємодію в єдину систему гнучкого управління. Проаналізовано передбачені законодавством процедури категоризації, моніторингу, модернізації та захисту критичних об'єктів, особливо в надзвичайних ситуаціях, таких як воєнний стан або техногенні катастрофи. Визначено провідну роль Національної комісії з питань захисту критичної інфраструктури як ключового координуючого органу. Обґрунтовано необхідність подальшого наближення українського законодавства до європейських стандартів, зокрема Директиви ЄС 2008/114/ЄС, що дасть змогу активніше інтегруватися до систем безпеки ЄС та НАТО. Запропоновано концептуальну модель правового забезпечення, засновану на принципах багаторівневої взаємодії, гнучкості нормативного регулювання, чіткої інституційної відповідальності та відкритості до міжнародної практики.

3. У результаті проведеного дослідження деталізовано складові структури інтегрованого комплексного механізму публічного управління у сфері трансформації об’єктів критичної інфраструктури, до складу якого входять: нормативно-правовий, інституційний, організаційно-інформаційний, фінансово-економічний, технологічний та цифровий механізми. У межах механізму виділено взаємопов’язані блоки: а) блок стратегічного планування, б) блок координації та в) блок операційного реагування. Додатково виділені прогностично-планувальний, координаційний та контрольно-наглядовий механізми. Ключовими принципами комплексного механізму публічного управління у сфері трансформації об’єктів критичної інфраструктури виступають: системність; ризик-орієнтованість; безперервність управління; вертикальна та горизонтальна координація; прозорість; адаптивність. Метою функціонування механізму – є: забезпечення стійкості, захищеності та безперервності функціонування об’єктів критичної інфраструктури країни в умовах трансформації.

4. З точки зору ефективності, метою комплексного механізму є – забезпечення належного рівня ефективності управлінських рішень у процесі функціонування об’єктів критичної інфраструктури. Принципами є: системність управлінських дій; урахування обмеженості ресурсів; баланс інтересів територій і рівнів влади; пріоритетність захисту життя населення; адаптивність до змін зовнішнього середовища; безперервність управління; орієнтація на соціальну безпеку та екологічну стійкість.

РОЗДІЛ 3
МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ, ЗАХИСТУ ТА БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ЗАРУБІЖНИЙ ДОСВІД

3.1. Досвід держав-членів ЄС щодо публічного управління у сфері трансформації об'єктів критичної інфраструктури

У європейських країнах на національному рівні захист критичної інфраструктури здійснюється через розвинену нормативно-правову базу, яка доповнюється державними стратегіями та спеціалізованими планами щодо охорони критичної інфраструктури. Дані документи визначають ключові завдання, спрямовані на забезпечення безпеки та стійкості відповідних об'єктів, а також конкретні повноваження органів влади, відповідальних за управління ризиками та загрозами, що можуть вплинути на критичну інфраструктуру. Водночас існує різноманітність підходів до управління в даній сфері. Окремі дослідники акцентують на тому, що управління критичною інфраструктурою має бути комплексним, гнучким та оперативним, що дозволяє адекватно реагувати на динамічні виклики [193; 270]. Важливо також зазначити думку М. Нейкової (M. Neikova) [279] щодо нової Директиви Ради Європи від 5 квітня 2022 року [186], що як і її попередня версія не обмежує компетенцію держав-членів та їхніх органів у питаннях адміністративної автономії, відповідальності за забезпечення національної безпеки та оборони, а також їхньої здатності захищати інші важливі функції держави, особливо в контексті громадської безпеки, територіальної цілісності та підтримання правопорядку. На його думку виключення органів державного управління з дії цієї директиви має стосуватися суб'єктів, чия діяльність переважно пов'язана з національною безпекою, громадською безпекою, обороною або правоохоронною діяльністю, включаючи розслідування, виявлення та переслідування кримінальних правопорушень. Однак органи державного управління, чия діяльність лише незначною мірою пов'язана з цими

сферами, мають бути включені в обсяг цієї директиви. Для забезпечення комплексного підходу до стійкості критичних суб'єктів кожна держава-член повинна мати стратегію, спрямовану на підвищення стійкості критичних суб'єктів. Натомість інші автори зосереджують увагу на проблемах міжвідомчої координації та на складності співпраці між державними й приватними суб'єктами, що діють у сфері критичної інфраструктури [234; 270; 308]. Така взаємодія ускладнюється через поділ відповідальності між різними державними органами, кожен з яких курує окремі сектори критичної інфраструктури, що часто породжує проблеми у координації та ефективному управлінні ризиками. У зв’язку з цим постає необхідність запровадження нових підходів та інструментів публічного управління, які дозволять оптимізувати процеси взаємодії на різних рівнях та підвищити загальну стійкість критичної інфраструктури до сучасних викликів і загроз [213; 291]. Зокрема, у європейських країнах розроблено сім основних елементів публічного управління, які спрямовані на підвищення стійкості критичної інфраструктури на основі політики захисту та забезпечення її функціонування, що наведено у Таблиці 3.1.

Таблиця 3.1.

Політика публічного управління ЄС щодо підтримки стійкості при трансформації критичної інфраструктури*

Компонент публічного управління	Приклади впровадження елементів політики публічного управління стійкістю критичної інфраструктури країн-членів ЄС
Формування багатогалузевої системи управління для підвищення стійкості критичної інфраструктури	У Франції Генеральний секретаріат з питань оборони та національної безпеки під керівництвом прем'єр-міністра здійснює координацію національної політики стійкості інфраструктури, що охоплює 12 секторів у 8 галузевих міністерствах. Такий підхід забезпечує комплексну оцінку потенційних загроз і вразливостей, що дозволяє знизити ризики збоїв у функціонуванні критично важливих об’єктів.
Оцінка складних взаємозалежностей та вразливостей інфраструктури для визначення першочергових заходів стійкості	У Нідерландах Національний координатор з питань безпеки та протидії тероризму (NCTV) впровадив трирівневу методологію, яка допомагає ідентифікувати та класифікувати критичні інфраструктури за рівнем їхньої значущості (категорії А або В). Дана система також передбачає оцінку вразливостей до різноманітних загроз та встановлення пріоритетів для інвестицій у підвищення їхньої стійкості на підставі детального аналізу ризиків.
Розробка механізмів взаємодії та довіри між державою та	У Великій Британії створено Центр даних та аналітики національної інфраструктури (DAFNI), який використовує інтегровані платформи для збору даних і моделювання, що

операторами критичної інфраструктури через обмін інформацією про ризики	дозволяє ефективно аналізувати інфраструктурні системи, оцінювати їхню продуктивність і приймати обґрунтовані рішення щодо інвестицій у збереження їхньої стійкості на всіх етапах життєвого циклу.
Побудова партнерства для узгодження спільного бачення стійкості інфраструктури між державою та приватним сектором	У Швейцарії національна стратегія захисту критичної інфраструктури (CIP), координована Федеральним відомством цивільного захисту, базується на партнерських відносинах із операторами об'єктів інфраструктури та субнаціональними органами влади. У рамках цього партнерства реалізуються спільні платформи для аналізу ризиків, обміну інформацією та визначення цілей стійкості, що дозволяє ефективніше протидіяти загрозам і забезпечувати тривалу життєздатність інфраструктури.
Встановлення стратегічних політичних заходів для оцінки економічної ефективності та довгострокової стійкості інфраструктури	У Фінляндії Управління з питань енергетики впроваджує вимоги щодо стандартів надійності й безперервності роботи в секторі електроенергії. Додатково Національне агентство аварійного постачання розробляє рекомендації та інструменти для операторів інфраструктури, щоб забезпечити дотримання цих стандартів. Подібним чином, у Франції заходи зі стійкості інфраструктури до ризику великої повені в Парижі передбачають обмін інформацією між державою, місцевими органами влади та операторами, підвищення готовності до надзвичайних ситуацій і мінімізацію вразливості інфраструктури.
Моніторинг впровадження політики стійкості та забезпечення підзвітності	Після прийняття Директиви 2008/114/ЕС про європейську критичну інфраструктуру Європейська комісія здійснює періодичний контроль і оцінку її впровадження. Даний процес дозволяє визначати, наскільки ефективною є політика стійкості, і коригувати заходи для підвищення їхньої актуальності в умовах нових загроз.
Транскордонний вимір забезпечення стійкості інфраструктурних систем	Європейська програма захисту критичної інфраструктури (EPCIP) передбачає координацію на рівні ЄС з урахуванням міжнародних аспектів. Програма включає регулярні зустрічі національних координаторів із захисту інфраструктури та розширюється за рахунок співпраці з сусідніми державами, що дозволяє забезпечувати комплексний і системний підхід до захисту та стійкості критичних об'єктів.

*Джерело: сформовано автором на основі [225].

Налагодження дієвих механізмів взаємодії між органами державної влади та операторами критичної інфраструктури вимагає створення комплексної системи обміну інформацією щодо загроз і ризиків, що стосуються стійкості цих об’єктів. Центральна влада несе пряму відповідальність за впровадження інформаційних платформ, які дозволяють операторам інфраструктури ділитися релевантними даними, необхідними для повноцінного аналізу вразливостей та розробки заходів для підвищення рівня стійкості критичних об’єктів. У даному контексті важливою є не лише технічна та організаційна складова, але й розвиток

стратегічного партнерства, що забезпечує узгодженість цілей і підходів до захисту інфраструктури між державними структурами та приватними операторами.

Ключовим аспектом державної політики є створення єдиного бачення із залученням усіх зацікавлених сторін, що дозволяє ефективно реалізовувати національні програми безпеки. Співпраця державного і приватного секторів у межах такої програми спрямована на формування системної стійкості критичної інфраструктури. Водночас важливим чинником є врахування очікувань суспільства щодо можливої втрати основних послуг у разі виникнення збоїв у роботі інфраструктури, що дозволяє побудувати відкритий діалог між урядом, операторами та громадськістю, спрямований на зниження рівня ризиків.

Формування стратегії та політичних заходів з метою визначення їх пріоритетності за критеріями економічної доцільності є ключовим завданням у сфері забезпечення стійкості критичної інфраструктури. Досвід різних держав демонструє необхідність розробки всеохоплюючої національної стратегії розвитку, яка передбачає зміцнення стійкості інфраструктури до зовнішніх загроз. На центральному рівні формуються відповідні політичні інструменти, спрямовані на стимулювання інвестицій з боку операторів критичних об'єктів у їхню довгострокову стійкість. Дані заходи повинні охоплювати весь життєвий цикл інфраструктурних об'єктів: від початкового етапу планування до експлуатації, обслуговування, оновлення та модернізації.

Пріоритетність заходів з підвищення стійкості, що визначається урядом конкретної держави, має базуватися на ретельному аналізі рентабельності, враховуючи можливі наслідки для економіки та вартості наданих послуг. Крім того, держава повинна забезпечити ефективні механізми підзвітності та контролю за впровадженням політики у сфері стійкості критичної інфраструктури, що включає визначення чітких рамок підзвітності для операторів критичних об'єктів.

Політика Польщі у сфері управління та захисту критичної інфраструктури ґрунтується на інтегрованій системі, яка охоплює визначення, управління, моніторинг та захист важливих об'єктів, що мають ключове значення для

національної безпеки. Відповідно до Закону «Про кризове управління» від 26 квітня 2007 року (Ustawa o zarządzaniu kryzysowym) [358], директор Урядового центру безпеки відповідає за складання переліку елементів критичної інфраструктури, особливо в енергетичному секторі, до якого входять об'єкти, системи, пристрої та послуги, пов'язані з постачанням енергії та палива. Зазначений закон регламентує класифікацію інфраструктури за такими категоріями, як енергетика, нафтогазовий сектор і газопостачання, що охоплює видобуток, переробку, зберігання, транспортування та управління терміналами для зрідженого природного газу. Для забезпечення належного рівня захисту Польща запровадила функцію зв'язкової особи відповідно до положень Закону «Про особливі права Державного казначейства» від 3 червня 2005 року (Ustawa o szczególnych uprawnieniach Skarbu Państwa i ich wykonywaniu w spółkach) [357]. Зв’язкова особа відповідає за моніторинг діяльності партнерств у сфері захисту критичної інфраструктури, зокрема підготовку регулярних звітів про стан захисту об'єктів, які подаються Міністру державної скарбниці та директору Урядового центру безпеки для подальшого аналізу.

Національна програма захисту критичної інфраструктури, затверджена Радою Міністрів Польщі, має на меті створення умов для підвищення безпеки ключових об'єктів через запобігання порушенням їх функціонування, підготовку до кризових ситуацій, реагування на них та відновлення інфраструктури після можливих загроз. Програма, розроблена відповідно до вимог Директиви ЄС 2022/542 від 5 квітня 2022 року [186], встановлює національні пріоритети, цілі, вимоги та стандарти для забезпечення ефективного функціонування критичної інфраструктури. Також визначено чіткі критерії для ідентифікації об'єктів і систем, які мають стратегічне значення для безперебійного функціонування держави. Крім того, Польща підтримує діалог із власниками та операторами критичної інфраструктури на національному та європейському рівнях, що сприяє обміну інформацією та формуванню єдиних підходів до забезпечення безпеки [229]. На міжнародному рівні Польща бере участь у створенні мережі раннього попередження про загрози, згідно з положеннями Постанови Ради Міністрів про захист критичної інфраструктури від 30 квітня 2010 року (Rozporządzenie Rady

Ministrów w sprawie ochrony infrastruktury krytycznej) [312], яка спрямована на забезпечення високої стійкості та захисту телекомунікаційної інфраструктури, критично важливої для функціонування інших секторів економіки.

Стійкість критичної інфраструктури ЄС визначається її спроможністю ефективно реагувати на екзогенні чинники, здійснювати відновлення після інцидентів негативного характеру та адаптуватися до динамічних умов, що є наслідком активізації процесів цифрової трансформації та глобалізації, при цьому зберігаючи основні функції. Дане визначення акцентує увагу на здатності інфраструктури до стійкості у відповідь на інциденти без значної втрати функціональності, обмежуючи тривалість перерв у наданні послуг та мінімізуючи час, необхідний для її відновлення. Таким чином, в умовах поширення ризиків, досягнення цілей стійкості можна оцінити за двома вимірами: обмеженням масштабу завданих пошкоджень та скороченням тривалості перерв у наданні послуг, що виникають унаслідок цих пошкоджень.

Слід зазначити, що процес відновлення не обов’язково передбачає повернення до попереднього стану, який існував до інциденту; він може включати елементи зміни, адаптації до нових умов, а також покращення функціональності системи з плином часу, що забезпечує її подальшу ефективність та стійкість. У даному контексті зазначена раніше директива 2008/114/ЄС також вказує на необхідність створення загальноєвропейських механізмів для забезпечення захисту інфраструктурних об’єктів, а також координації між державами-членами з метою мінімізації ризиків та підвищення стійкості критичної інфраструктури до зовнішніх і внутрішніх загроз [19], що визначені на рис. 3.1.

З огляду на кількість та масштаби сучасних загроз визначальним аспектом забезпечення стійкості критично важливої інфраструктури є ідентифікація перебоїв в її функціонуванні та збоїв в ланцюгах постачання, що можуть викликати перехресний вплив на інші сектори економіки та географічні території.



Рис. 3.1. Загрози стійкості критичної інфраструктури країн-членів ЄС*

*Джерело: сформовано автором на основі [19, 312, 357]

Даний процес потребує розробки комплексу фіскальних і регуляторних механізмів, орієнтованих на створення резервних потужностей, диверсифікацію ресурсів або впровадження альтернативних систем, що сприятиме зменшенню ризику виникнення збоїв та тривалих перерв у функціонуванні критичної інфраструктури. Крім того, необхідним напрямком для забезпечення стійкості є координація у проєктуванні мереж критично важливої інфраструктури (зокрема енергетичних, транспортних, телекомунікаційних та інформаційних систем) з політикою містобудування та управління територіями, а використання потенціалу приватного сектора для побудови стійкої інфраструктури підвищує ефективність зазначених ініціатив.

Заохочення підприємств до реалізації заходів, спрямованих на забезпечення безперервності бізнес-процесів, становить ще один ключовий елемент у цьому процесі, що, головним чином, стосується операторів критичної інфраструктури, які також потребують розробки відповідних стандартів та інструментів, спрямовані на управління ризиками, які можуть загрожувати їхній діяльності або наданню основних послуг. Натомість забезпечення функціонування критично важливої інфраструктури, інформаційних систем і мереж після виникнення ризику передбачає наявність і реалізацію планів реагування на надзвичайні ситуації, що дозволяє оперативно реагувати на інциденти, здатні порушити роботу мереж критично важливої інфраструктури, з метою швидкого відновлення їх функціонування.

Норми законодавства ЄС у сфері захисту критичної інфраструктури були сформовані на основі особливості окремих секторів та використання відповідних інструментів. Висновки Європейської Ради, що стосуються запобігання терористичним загрозам та готовності до них, а також «Програма солідарності ЄС у відповідь на терористичні атаки», відображають програму Європейської Комісії до розробки нових політик. При цій Європейській програмі захисту критичної інфраструктури підтримана ініціатива створення в рамках європейських управлінських структур спеціалізованої інформаційної мережі, що зосереджується на питаннях критичної інфраструктури. Зазначена програма містить ключові принципи, процеси та інструменти, які забезпечують реалізацію механізму управління системами захисту об'єктів критичної інфраструктури. Реалізація цих проектів доповнюється специфічними аспектами, які враховують особливості сектору комунікацій, та описують підходи Комісії до вирішення конкретних питань, пов’язаних із критичною інфраструктурою. Таким чином, структурні елементи захисту об’єктів критичної інфраструктури ЄС включають заходи, що спрямовані на ідентифікацію та підтримку критичної інфраструктури країн-членів союзу, удосконалення систем їх захисту тощо (рис. 3.2.).

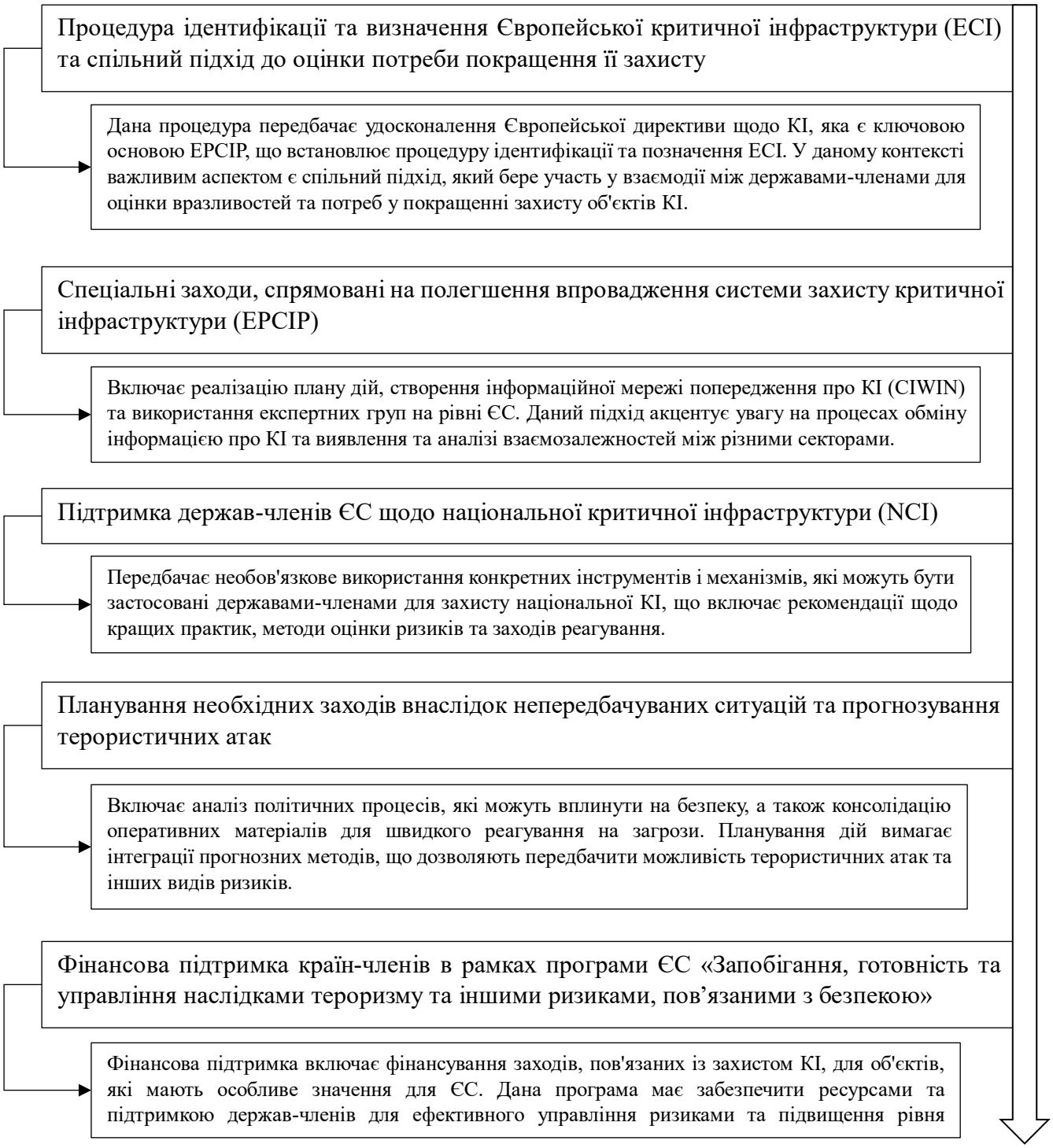


Рис. 3.2.Структурні елементи захисту об’єктів критичної інфраструктури ЄС Джерело: сформовано автором на основі*

*Джерело: сформовано автором на основі [228].

Проте, стійкість критичної інфраструктури також значною мірою залежить від ефективної співпраці між урядами та операторами інфраструктурних систем, що представляють як державний, так і приватний сектори. Хоча всі сторони визнають необхідність захисту критично важливих активів і підтримки

відповідних послуг, існують відмінності в їхніх уявленнях щодо необхідного рівня стійкості, шляхів її досягнення та регуляторних норм, які слід застосовувати. Визначені аспекти мають фінансові наслідки та піднімають питання про те, хто нестиме додаткові витрати, пов’язані з інвестиціями у забезпечення стійкості. Державно-приватне партнерство (ДПП) між урядами та операторами є важливим для сприяння конструктивному діалогу щодо вказаних питань. Таке партнерство є основою для спільної розробки та впровадження політик, спрямованих на забезпечення стійкості та безпеки критичної інфраструктури. Ключовими завданнями у даному контексті є встановлення довіри, забезпечення надійного обміну інформацією, розробка механізмів фінансового розподілу витрат та зміцнення міжнародного співробітництва, які вимагають відповідних управлінських стратегій. Проте, виявлений М. Нейковою факт, що окремі держави-члени ЄС встановлюють менш жорсткі вимоги безпеки для відповідних суб'єктів, не лише спричиняє неоднорідність рівнів стійкості, а й може негативно вплинути на забезпечення життєво важливих соціальних функцій та економічної діяльності у рамках ЄС, що в кінцевому підсумку створює перешкоди для належного функціонування внутрішнього ринку [279].

У даному контексті слід відзначити досвід Норвегії, як найбільш розвиненої держави у контексті інфраструктурного забезпечення та сталого розвитку, де система публічного управління критичною інфраструктурою ґрунтується на тісній взаємодії, державно-приватному партнерстві, а також активному залученні представників державних установ та різних зацікавлених сторін із приватного сектору до процесу управління. Ключові структурні елементи управління критичною інфраструктурою в Норвегії охоплюють, перш за все, процеси перетворення та розвитку критичної інфраструктури, що зобов’язують державу до формування законодавчого середовища, яке стане основою для нагляду та регулювання різних секторів критичної інфраструктури. Відповідні закони, директиви та інші нормативно-правові акти чітко окреслюють повноваження та обов’язки органів влади та зацікавлених сторін, які відповідають за захист і управління критичною інфраструктурою, зокрема до них належать Закон «Про безпеку» [107], Закон «Про таємниці оборони», Закон «Про

оборонні винаходи», а також Угода про сертифікацію інформаційних систем і продуктів (SERTIT) [247].

По-друге, розподіл повноважень та завдань між урядовими установами, відповідальними за різні сектори критичної інфраструктури в Норвегії, є важливим аспектом забезпечення їх ефективного функціонування та безпеки. Норвезький уряд чітко визначив сфери відповідальності спеціалізованих агентств та уповноважених органів, які здійснюють нагляд за окремими сегментами критичної інфраструктури, що дозволяє реалізувати комплексний підхід до управління. Наприклад, Норвезьке управління водних ресурсів та енергетики виконує функцію контролю за інфраструктурою енергетичного сектора. Основними завданнями Норвезького управління водних ресурсів та енергетики є проведення аналізу стану енергетичних об'єктів, забезпечення їхньої безпеки та готовності до можливих надзвичайних ситуацій, а також розвиток стратегій сталого використання енергетичних ресурсів [283]. У свою чергу, Норвезьке управління зв'язку відповідає за регулювання та контроль у секторі телекомунікацій. Як виконавчий орган державної влади, дане управління не лише здійснює нагляд за якістю та доступністю зв'язку, але й активно працює над впровадженням новітніх технологій у галузі комунікацій. Воно також відповідає за розвиток політики у сфері електронних комунікацій, захисту прав споживачів та забезпечення кібербезпеки в телекомунікаційних мережах [281].

Крім того, державно-приватне партнерство у Норвегії є одним з ключових механізмів для оптимізації управлінських процесів у сфері критичної інфраструктури, що базується на інтеграції державних і приватних суб'єктів. Урядова підтримка ДПП має на меті підвищення стійкості критичних об'єктів, удосконалення інформаційного обміну між ключовими акторами, а також координацію дій у відповідь на потенційні загрози. Зокрема, у Норвегії зростає значення співпраці з приватними компаніями у контексті кіберзахисту критичної інфраструктури, що зумовлено переважанням приватної власності та обмеженими можливостями державного фінансування. У даному контексті транснаціональна природа кіберризиків вимагає не лише активізації внутрішнього співробітництва в рамках ДПП, але й залучення міжнародних і

регіональних організацій [224]. Таким чином, міжнародне співробітництво в умовах зростаючої взаємозалежності різних секторів критичної інфраструктури в Європі є критично важливим для спільного вирішення актуальних проблем, оптимізації ресурсів і обміну досвідом. Співпраця між державами на національному та регіональному рівнях сприяє підвищенню ефективності реагування на виклики. Країна активно бере участь у міжнародних форумах, зокрема в заходах, організованих Агентством ЄС з кібербезпеки (ENISA) і Радою міністрів Північних країн, що забезпечує обмін передовими практиками та координацію дій у відповідь на загрози, пов'язані з критичною інфраструктурою.

Натомість у Франції основні загрози, що стосуються критичної інфраструктури, зосереджені навколо кіберзагроз і терористичних ризиків. Для ефективної протидії цим викликам функціонує Генеральний секретаріат з питань оборони та національної безпеки (SGDSN) [328], що виконує ключову роль у забезпеченні безпеки критичних об’єктів, здійснюючи аналіз відкритих джерел інформації та розвідувальних даних, що стосуються захисту критичної інфраструктури. Також SGDSN відповідає за моніторинг загроз, що можуть виникнути як з внутрішніх, так і з зовнішніх джерел. У межах своєї діяльності секретаріат займається виявленням потенційних ризиків і забезпечує рекомендації для підвищення рівня захисту критичних об'єктів, що включає як кібернетичні системи, так і фізичні інфраструктури. Зокрема, в умовах цифровізації та розвитку технологій паралельним явищем є зростання масштабів кіберзлочинності, SGDSN спрямовує свої зусилля на вдосконалення механізмів захисту від можливих кібератак, які мають катастрофічні наслідки для національної безпеки. Крім того, секретаріат аналізує ймовірні терористичні загрози, що можуть поставити під загрозу життєво важливі функції держави, включаючи енергетичну, транспортну та інформаційну інфраструктури.

У свою чергу Данія та Нідерланди, незважаючи на їхню географічну близькість і спільні культурні традиції, демонструють відмінності у підходах до управління загрозами для критичної інфраструктури, що відображає специфіку їхніх національних контекстів. Так, у Данії основні загрози, що стосуються критичної інфраструктури, зосереджуються на надзвичайних ситуаціях, таких як

аварії, катастрофи та стихійні лиха. У цьому контексті ключову роль відіграє Данське агентство з управління надзвичайними ситуаціями (DEMA), яке відповідає за забезпечення неперервності функціонування важливих державних і суспільних служб у випадках криз. Отже, підхід до публічного управління у сфері критичної інфраструктури Данії зосереджується на готовності до реагування на природні та техногенні ризики, акцентуючи значення превентивних заходів і координації дій у разі надзвичайних ситуацій [302]. Водночас у Нідерландах основні загрози для критичної інфраструктури визначаються через національну оцінку ризиків, яка включає тероризм, кіберзагрози та аспекти національної безпеки. Слід зазначити, що у цій країні важливу роль виконує Національний координаційний центр із питань боротьби з тероризмом та забезпечення безпеки (NCTV), який координує діяльність різних установ, включаючи поліцію, судову владу та служби безпеки. Нідерландський підхід, головним чином, акцентує увагу на антропогенних загрозах, розробляючи комплексні стратегії реагування на терористичні акти та кіберзлочини [216].

Таким чином, досвід держав ЄС у сфері управління трансформацією об’єктів критичної інфраструктури відзначається ретельним підходом до створення комплексних регуляторних механізмів, які сприяють зміцненню стійкості таких об’єктів у відповідь на сучасні виклики та загрози. Важливим аспектом також є системна інтеграція приватного сектора, оскільки значна частина критично важливих об’єктів належить до приватної власності, що вимагає від держав розробки багаторівневих стратегій захисту, які забезпечують належну координацію між державними установами та приватними операторами. Крім того, акцент на публічно-приватне партнерство та міжвідомчу координацію підкреслює необхідність спільного бачення у сфері стійкості критичної інфраструктури, що вимагає, перш за все, узгодження зусиль, а також постійного моніторингу та оцінки ефективності впроваджених стратегій.

3.2. Реалізація загальної системи управління та захисту об’єктів критичної інфраструктури в ЄС

У директиві Ради Європи від 8 грудня 2008 року викладено результати діяльності Комісії, спрямованої на розробку єдиного підходу до ідентифікації та класифікації об’єктів європейської критичної інфраструктури (ECI) [19]. Даний документ визначає критичну інфраструктуру як об'єкти, системи або їхні елементи, розташовані на території держав-членів ЄС, що мають вирішальне значення для забезпечення життєво важливих суспільних функцій, охорони здоров'я, громадської безпеки, економічної стабільності або соціального добробуту населення. Зокрема, наголошується на тому, що пошкодження або руйнування таких об'єктів може призвести до серйозних наслідків для держави-члена ЄС через неможливість продовжувати надання важливих послуг, що впливає на функціонування основних секторів економіки та безпеки.

Окрім загального визначення, директива приділяє увагу терміну «європейська критична інфраструктура» (ECI), який охоплює об'єкти, розташовані в державах-членах, руйнування або пошкодження яких може спричинити значний вплив не тільки в одній країні, а щонайменше в двох або більше державах-членах [19]. Такий підхід до класифікації критичних об'єктів підкреслює важливість їхньої безпеки для міждержавної співпраці в рамках ЄС, оскільки порушення функціонування одного об'єкта може спричинити ланцюгові наслідки, що вплинуть на загальноєвропейську інфраструктуру, а також на стабільність європейського суспільства в цілому.

Особливістю державної стратегії щодо функціонування критичної інфраструктури у країнах-членах ЄС є створення таких регуляторних механізмів, які в умовах надзвичайних ситуацій забезпечать ефективність контролю за її основними функціями, навіть в умовах тимчасового припинення дії ринкових економічних законів, що реалізовується лише за рахунок ефективного впровадження державно-приватного партнерства . Слід зазначити, що у країнах ЄС значна частина критичної інфраструктури перебуває у власності приватного

сектора, що ставить перед урядами завдання розробки комплексної нормативно-правової бази, що має бути спрямована на зміцнення стійкості таких об'єктів до різних типів загроз, включно з природними катаклізмами, техногенними аваріями та терористичними атаками. У даному випадку державні органи виконавчої влади несуть пряму відповідальність за розробку стратегічних планів захисту критичної інфраструктури, які охоплюють усі сектори, та за впровадження відповідних заходів в рамках політики безпеки і, крім того, держава бере на себе політичну відповідальність за наслідки реалізації цих стратегій у випадку загроз або кризових ситуацій.

Незважаючи на те, що програмні документи держав-членів ЄС мають певні відмінності у ідентифікації та класифікації об’єктів критичної інфраструктури. Наприклад, у Польщі «медичне транспортування» є сектором, який зазвичай поділяється на транспортний та охорону здоров'я [19]. З огляду на це, важливо забезпечити гармонізацію підходів до ідентифікації та класифікації об’єктів критичної інфраструктури на міждержавному рівні, що сприятиме ефективній координації заходів з їх захисту та підвищенню стійкості загальноєвропейської інфраструктури. Відсутність уніфікованих критеріїв визначення критичної інфраструктури в різних країнах-членах ЄС може створювати прогалини в системі загальної безпеки, що, в умовах зростання глобальних загроз, потребує спільного підходу та стандартизації основних принципів захисту ключових об'єктів. Систематизація наявних секторів критичної інфраструктури серед країн-членів ЄС наведена на Рис.3.3. Аналіз критичної інфраструктури серед країн Європи свідчить про високий рівень усвідомлення важливості захисту національних секторів. Зокрема, 95% європейських країн (42 із 44) мають офіційно визначений перелік секторів критичної інфраструктури, що є основою для розробки національних стратегій безпеки. Серед них сектор енергетики є пріоритетним, адже всі 42 країни включили його до свого переліку критичних об'єктів, що відображає критичну залежність Європи від стабільності постачання зовнішніх джерел енергії, зокрема російського викопного палива, та важливість енергетичної безпеки для економіки і суспільства.



Рис. 3.3. Мапа критичності інфраструктури ЄС*

*Джерело: сформовано автором на основі [364].

Натомість сфера досліджень та освіти залишається найменш згадуваною категорією критичної інфраструктури, охоплюючи лише 12% європейських країн, що свідчить про недостатню увагу до цих напрямів у контексті національної безпеки.

Для комплексного вирішення питань стійкості суб’єктів, що мають вирішальне значення для нормального функціонування внутрішнього ринку, Директива (ЄС) 2022/2557 щодо стійкості критичних суб’єктів встановлює загальний підхід, що охоплює їх стійкість стосовно всіх видів небезпек, включаючи природні, антропогенні, випадкові та навмисні загрози. Критичні суб’єкти повинні мати всебічне розуміння тих ризиків, яким вони можуть бути піддані, і зобов’язані проводити ретельний аналіз цих ризиків. Відповідно до зазначених вимог, вони повинні здійснювати оцінку ризиків, орієнтуючись на специфіку своїх обставин та можливу еволюцію цих загроз. Оцінка має проводитися принаймні раз на чотири роки, що дає змогу виявити всі значущі ризики, здатні порушити надання їхніх основних послуг. Така оцінка ризиків є

обов’язковою для кожного критичного суб’єкта і є важливим елементом для забезпечення стійкості інфраструктури та безперервності важливих функцій. На Рис. 3.4. представлено характеристику та взаємозалежності різних типів об’єктів критичної інфраструктури, що відповідно до статті 2 Директиви (ЄС) 2022/2557 [197] визначаються як такі, що мають вирішальне значення для збереження функціонування суспільства в цілому.

Сучасна політика Європейського Союзу у сфері захисту критичної інфраструктури, закріплена в Директиві Ради Європи 2022/542 від 5 квітня 2022 року [186] спрямована на забезпечення надійного функціонування життєво важливих суспільних функцій, громадської безпеки та стабільності економіки і соціальної сфери. Незважаючи на виклики, пов’язані з ефективністю цієї політики, її практична цінність полягає у виявленні і зниженні ризиків, що виникають через взаємозалежність держав-членів у таких ключових секторах, як енергетика, інформаційно-комунікаційні технології, транспорт, водопостачання, охорона здоров’я, фінансова сфера, хімічна промисловість та оборонна інфраструктура. ЄС розглядає взаємозалежність критичної інфраструктури у двох основних вимірах: міждержавному та міжсекторальному; що означає, що порушення у функціонуванні одного з секторів або в межах однієї країни може призвести до суттєвих наслідків для інших країн та галузей, створюючи загрозу для системної стабільності та безпеки. Одним із актуальних прикладів транскордонної взаємодії є створення Європейської мережі передачі електроенергії (ENTSO-E), в яку входять більшість країн ЄС. Завдяки цьому об'єднанню забезпечується інтеграція електричних мереж Європи, що оперативно перенаправляє енергію під час локальних збоїв. Водночас синхронізація таких мереж створює ризики каскадних відключень: наприклад, збій у Франції або Німеччині може швидко вплинути на інші країни. Однак країни, які не входять до синхронної мережі, зокрема Велика Британія після Brexit, мають асинхронні зв’язки з Європою, що дозволяє їм зберігати автономність і менше залежати від континентальних енергетичних коливань, що забезпечує підвищену стійкість до зовнішніх ризиків, хоча і може обмежити їхню здатність отримувати підтримку в разі кризи [359].

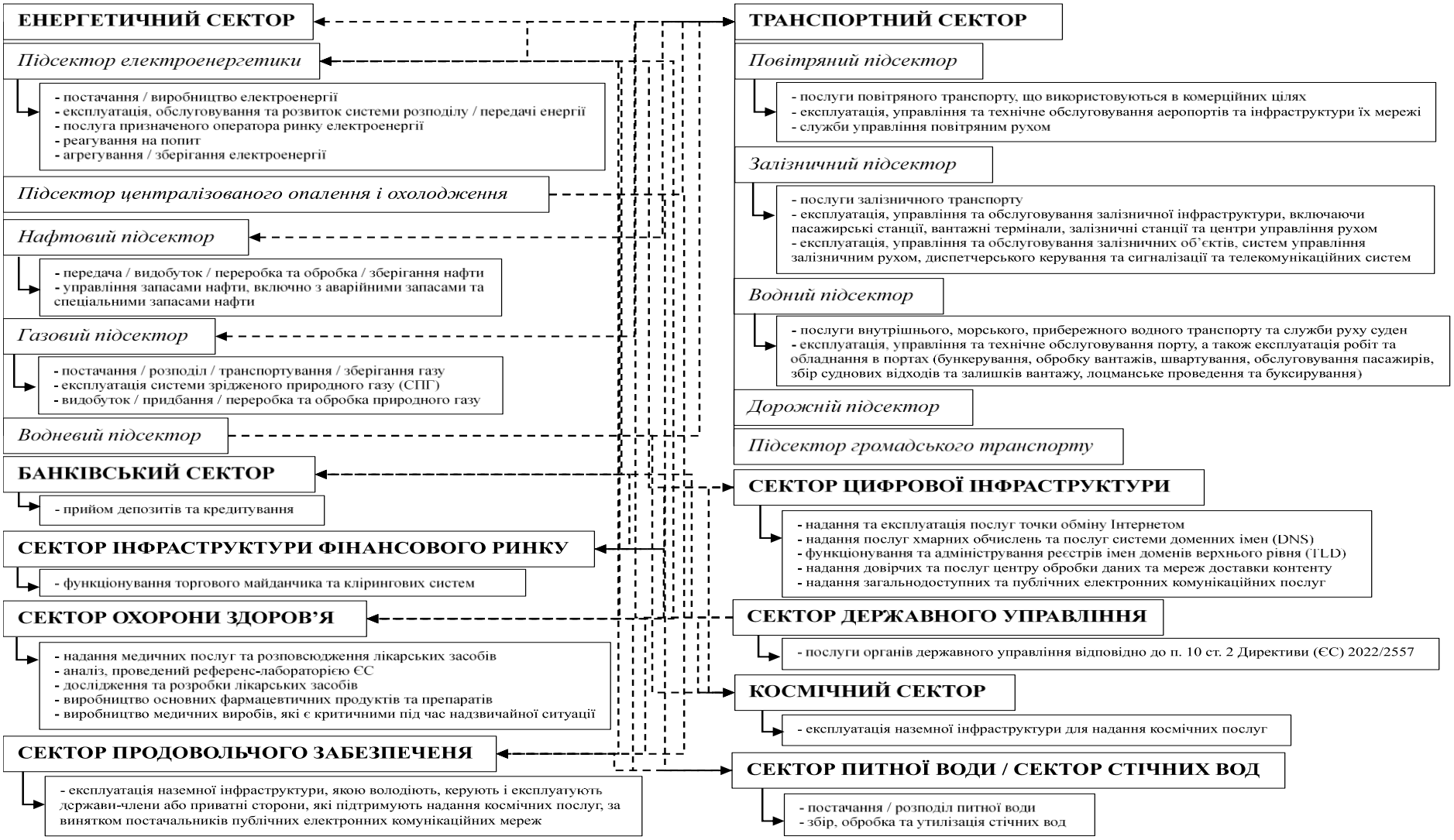


Рис. 3.4. Класифікація та система взаємозалежностей між об'єктами критичної інфраструктури ЄС*

*Джерело: власна розробка автора

Подібний підхід до управління транскордонною інфраструктурою застосовується й у сфері цифрової безпеки, де ЄС активно впроваджує нові стандарти кіберзахисту. Програма «Цифрова Європа» [130] стимулює співпрацю держав-членів у розвитку інструментів для запобігання кіберзагрозам, а також зменшує залежність від постачальників технологій з-за меж ЄС. Така стратегія посилює стійкість цифрової інфраструктури Європи в умовах потенційних кібератак. Отже, політика ЄС спрямована на побудову більш стійкої та інтегрованої інфраструктури, яка одночасно залишається достатньо гнучкою, щоб враховувати особливості і потреби окремих країн, мінімізуючи транскордонні ризики і створюючи надійну основу для захисту взаємозалежних систем у часи глобальних викликів.

Міжгалузеві зв’язки в критичній інфраструктурі сьогодні мають ще більше значення для забезпечення стійкості суспільства, оскільки сучасні кризи можуть швидко дестабілізувати різні сектори. Наприклад, перебої в енергопостачанні чи збої у функціонуванні інформаційно-комунікаційних технологій (ІКТ) здатні паралізувати роботу державних і приватних структур, медичних закладів та критичних фінансових операцій, що залежить від електронних систем [244]. Дослідження показують, що такі зв’язки поглибилися за останні десятиліття через постійне вдосконалення технологій та цифровізації суспільства.

Одним із найяскравіших прикладів є фінансова система, яка сьогодні повністю залежить від ІКТ. Із розширенням Інтернету фінансові установи перейшли до онлайн-банкінгу, що забезпечує доступ клієнтів до рахунків та автоматичні платежі. Особливо з початком пандемії COVID-19 в 2020 році, банківські послуги зазнали потужного поштовху до цифровізації, спричинивши ще глибшу інтеграцію фінансового сектора з ІКТ [221]. Крім того, взаємозалежність енергетичної інфраструктури з важкою промисловістю також зазнала значного оновлення. На тлі переходу до відновлювальних джерел енергії та реалізації заходів для зменшення викидів і переходу на відновлювані джерела енергії, великі промислові підприємства почали поступово інтегрувати у власні процеси технології енергозбереження, використовуючи, наприклад, біогаз та

інші альтернативні джерела. Зокрема, енергетична криза в Європі 2022 року, спричинена, головним чином, необхідністю відмови від викопних джерел палива з росії на тлі її агресії на території України, підкреслила важливість енергетичної незалежності і водночас показали критичність доступу до традиційних енергоресурсів, таких як газопроводи й танкери з нафтопродуктами [223].

Щодо зеленої інфраструктури, важливість її захисту відображається у сучасних ініціативах, таких як Європейська зелена угода 2019 року [329] та її подальше впровадження, яке включає розвиток транснаціональних екологічних коридорів і мереж для підтримки біорізноманіття та стійкості екосистем. Відновлення зелених зон і природних середовищ стало пріоритетом у багатьох країнах, і в 2021-2022 роках значна частина національних стратегій країн-членів ЄС включала формування екологічних мереж, що об'єднують між собою природні заповідники. Збереження таких територій є критично важливим для захисту екологічних ресурсів і запобігання екологічним ризикам, таким як деградація земель та втрата біорізноманіття. Таким чином, сучасні міжгалузеві зв'язки критичної інфраструктури стали більш вразливими, але водночас критично важливими для функціонування суспільства, особливо на фоні новітніх викликів, таких як цифровізація, перехід на екологічні технології та глобальні екологічні ініціативи.

Отже, підвищення стійкості критичної інфраструктури є ключовим завданням для урядів у всьому світі, що зумовлено ескалацією нових типів загроз, включаючи нетрадиційні атаки, які виходять за межі звичних методів оцінки ризиків і традиційних заходів з їх мінімізації. Деякі загрози залишаються складними для прогнозування, а зниження їхнього впливу з економічної точки зору не виправдане, що зумовлює зсув акценту з класичної оцінки ризиків на забезпечення стійкості, спрямованої на підтримання безперервності надання послуг навіть у випадках непередбачуваних і руйнівних подій.

З метою ефективного аналізу технологічних систем з урахуванням їхньої міжсекторальної та транскордонної взаємозалежності, а також для кількісного вимірювання економічного впливу збоїв у роботі критичної інфраструктури на суспільство, Спільний дослідницький центр (JRC) розробив низку інструментів і

методологій, що підкріплені серією наукових публікацій [125; 288; 373], стали основою для комплексного оцінювання стійкості критичної інфраструктури, зокрема її здатності до швидкого відновлення після дестабілізуючих інцидентів. Характеристика етапів реалізації заходів JRC щодо стійкості критичної інфраструктури наведено на Рис.3.5.

Європейська програма із захисту критичної інфраструктури (EPCIP) є основою, відповідно до якої різні заходи спрямовані разом на покращення захисту критичної інфраструктури в ЄС. Дані заходи включають створення Європейської еталонної мережі захисту критичної інфраструктури (ERNCIP), яку координує JRC. З метою підвищення рівня захисту критичної інфраструктури та зменшення її вразливості, EPCIP, що є комплексом політичних та технічних заходів, спрямованих на забезпечення цілісності, надійності та стійкості таких об'єктів. EPCIP охоплює різні економічні сектори та всі держави-члени ЄС, формуючи спільні стандарти та підходи до захисту інфраструктури, що є критично важливою для функціонування суспільства. Крім того, ЄС реалізує Ініціативу щодо захисту критичної інформаційної інфраструктури (CIIP), основним завданням якої є підвищення безпеки ІКТ як невід'ємного елемента сучасної критичної інфраструктури. CIIP сприяє зміцненню стійкості цих систем, оскільки вони забезпечують стабільне функціонування не лише комунікацій, але й низки інших життєвоважливих галузей.

Для підтримки заходів ЄС у сфері захисту критичної інфраструктури, Спільний дослідницький центр (JRC) координує діяльність Європейської довідкової мережі захисту критичної інфраструктури (ERNCIP), яка забезпечує технічну підтримку для реалізації Директиви про європейську критичну інфраструктуру. JRC здійснює наукові дослідження, спрямовані на розвиток інноваційних методів та інструментів для кібербезпеки, підвищення стійкості мережевої інфраструктури до впливу екстремальних космічних погодних умов, а також на оцінку здатності будівель та транспортних систем витримувати вибухові впливи.

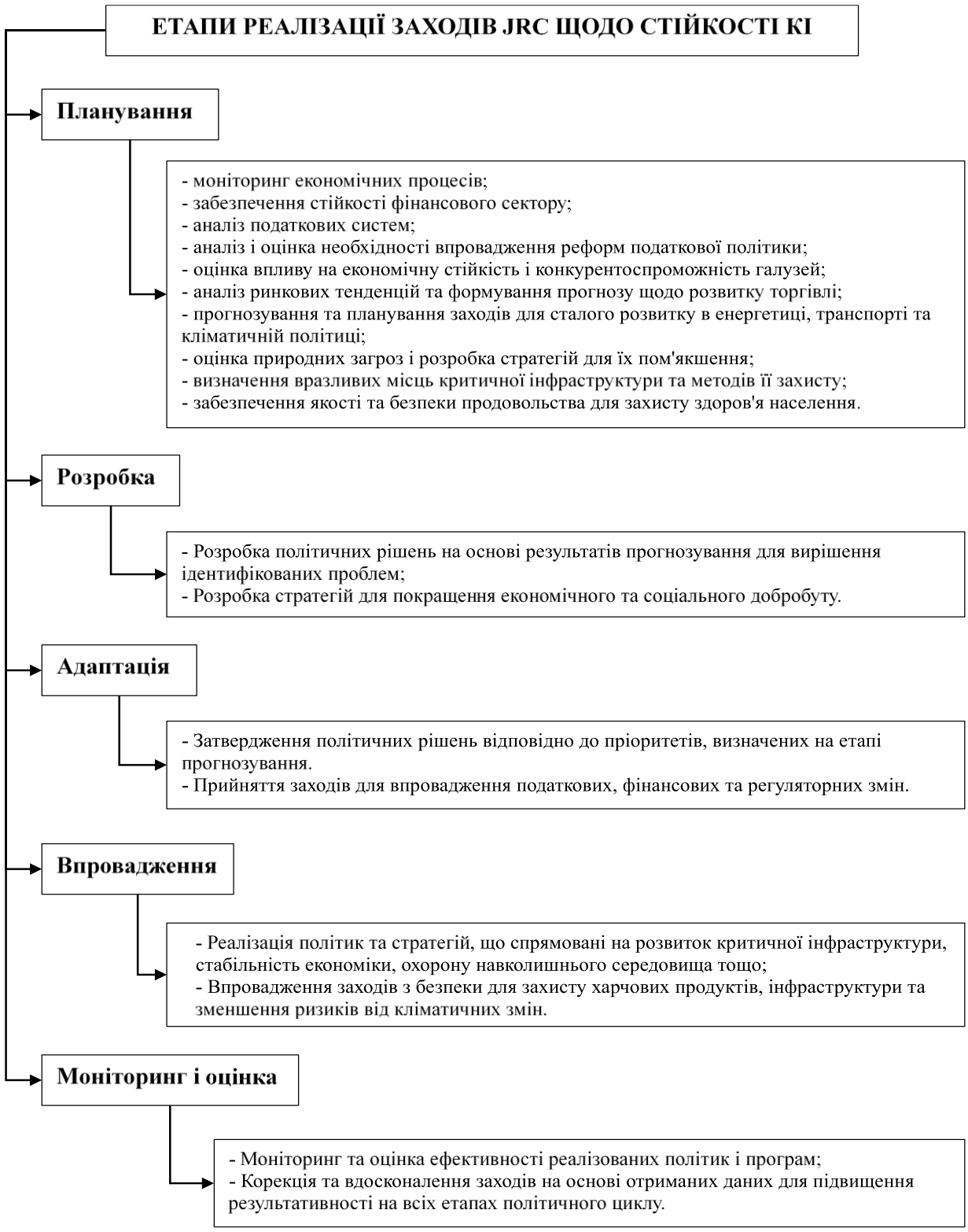


Рис. 3.5. Характеристика етапів реалізації заходів об’єднаного дослідницького центру щодо стійкості критичної інфраструктури*

*Джерело: власна розробка автора

Таким чином, система управління та захисту об'єктів критичної інфраструктури в ЄС є комплексним механізмом, що поєднує інноваційні підходи

до забезпечення безпеки, міждержавне співробітництво та технічну підтримку. Її основною метою є зменшення вразливості ключових секторів суспільної та економічної діяльності до сучасних загроз, таких як терористичні атаки, природні катастрофи та кібернетичні інциденти. Європейська комісія, ініціювавши EPCIP та Ініціативу щодо CIIP, сприяє створенню єдиної нормативно-правової та організаційної платформи, яка забезпечує гармонізацію підходів до захисту об'єктів у державах-членах ЄС. Важливою складовою цієї системи є ERNCIP, діяльність якої координує JRC з метою розробки нових методів та інструментів для підвищення стійкості як окремих об’єктів критичної інфраструктури, так і їх взаємопов’язаних ланцюгів. Отже, реалізація системи управління та захисту критичної інфраструктури в ЄС сприяє підвищенню безпеки та стійкості суспільства в умовах зростаючих загроз, а також забезпечує стабільне функціонування життєво важливих об'єктів, знижує ризик виникнення потенційних проблем та сприяє збереженню економічної стабільності, усуваючи прогалини та вразливості в управлінні, регулюванні та захисті критичної інфраструктури від сучасних викликів і загроз в ЄС.

3.3. Практика управління та захисту критичної інфраструктури США та Канади

Головним нормативно-правовим актом, який регламентує питання управління та захисту критичної інфраструктури у Сполучених штатах є USA PATRIOT Act [356], згідно до якого критична інфраструктура охоплює як матеріальні, так і цифрові системи та ресурси, від яких значною мірою залежить стабільність та безпека США. Такі об'єкти та системи є настільки важливими, що будь-які порушення їхньої роботи чи знищення можуть призвести до суттєвих і довгострокових наслідків у кількох ключових сферах, що стосується не лише загроз національній безпеці, але й економічної стійкості, захисту здоров'я населення та підтримки соціальної стабільності. Крім того, критичні об'єкти є основою національної життєздатності, оскільки їхній вихід з ладу може

викликати масштабні збої в роботі інших систем та інфраструктурних об’єктів, породжуючи складні взаємопов’язані ризики, які вимагають високої координації та швидкої реакції.

В оновленій Національній стратегії безпеки США до 2022 року акцент зроблено на захисті критичної інфраструктури як на одному з шести головних національних пріоритетів. Таке рішення є відповіддю на зростаючі ризики, зумовлені новими видами загроз, включаючи терористичні атаки, кіберзагрози та інші виклики, які можуть вплинути на безпеку, стабільність економіки та добробут суспільства. Стратегія передбачає посилену координацію між державними та приватними секторами, вдосконалення методів оцінки ризиків і розширення можливостей для оперативного реагування та відновлення в разі надзвичайних ситуацій, що робить критичну інфраструктуру одним з основних елементів національної безпеки.

У Публічному законі 107-296 [300] уряд США особливо підкреслює важливість захисту критичної інформаційної інфраструктури як ключової складової національної безпеки та економічної стабільності. Відповідно до цього нормативного документа, критичні інформаційні інфраструктури включають системи та мережі, інформація в яких має обмежений доступ, оскільки вона безпосередньо стосується безпеки стратегічно важливих об’єктів і базових функцій інших життєво важливих структур. Дані об’єкти інфраструктури охоплюють інформаційно-комунікаційні технології, які підтримують основні канали передачі даних, мережеві структури та інтерфейси, необхідні для безпечного й оперативного передавання конфіденційної інформації. Інформаційні системи критичної інфраструктури забезпечують надійність і стійкість у функціонуванні таких сфер, як енергетика, транспорт, охорона здоров'я та фінансова галузь, що вимагає чітко визначеної системи управління ризиками та безпеки інформації, яка враховує специфіку каналів зв’язку та структуру мережевих топологій, завдяки чому підтримується безперервний захист і стійкість до можливих загроз, що можуть вплинути на життєво важливі ресурси країни.

У рамках Закону про інформацію про критичну інфраструктуру (CII Act) від 2002 року [188] Конгрес США започаткував Програму захисту інформації про критичну інфраструктуру (PCII), що забезпечує захист інформації, яку суб'єкти приватного сектору та місцеві органи влади добровільно надають уряду. Дана програма розроблена з метою посилення безпеки стратегічних об'єктів через надання гарантій щодо збереження конфіденційності наданої інформації, яка є важливою для охорони критичної інфраструктури.

Відповідно до CII Act та положень про його імплементацію, зокрема 6 CFR частина 29 «Процедури обробки інформації про критичну інфраструктуру» (Procedures for Handling Critical Infrastructure Information) [375] встановлено стандартизовані правила щодо отримання, перевірки, обробки, зберігання, маркування та використання інформації, що надходить до Агентства з кібербезпеки та інфраструктури безпеки (CISA), яке діє під егідою Департаменту внутрішньої безпеки (DHS). Зазначене положення зобов’язує CISA забезпечувати особливі умови для роботи з інформацією, щоб уникнути ризику її несанкціонованого розголошення.

Програма PCII також сприяє активізації обміну інформацією між операторами критичної інфраструктури та державними структурами, гарантуючи захист конфіденційних даних від загроз витоку та несанкціонованого доступу. Така форма захисту сприяє зміцненню довіри між державою та приватними операторами, дозволяючи ефективніше координувати дії щодо забезпечення національної безпеки та безперебійного функціонування життєво важливих об’єктів. Структуру та основні рівні було складено відповідно до 6 CFR частини 29 пункту 4 PCII та представлено у вигляді ієрархічної схеми на Рис.3.6.

Директор CISA призначається відповідальним за управління Програмою PCII, здійснюючи контроль через його Виконавчого помічника. Таким чином, керівництво та адміністрування Програми PCII через CISA охоплює визначення загального напряму програми, координацію дій між відповідними відомствами та надання організаційної підтримки для досягнення цілей захисту критичної інформації.

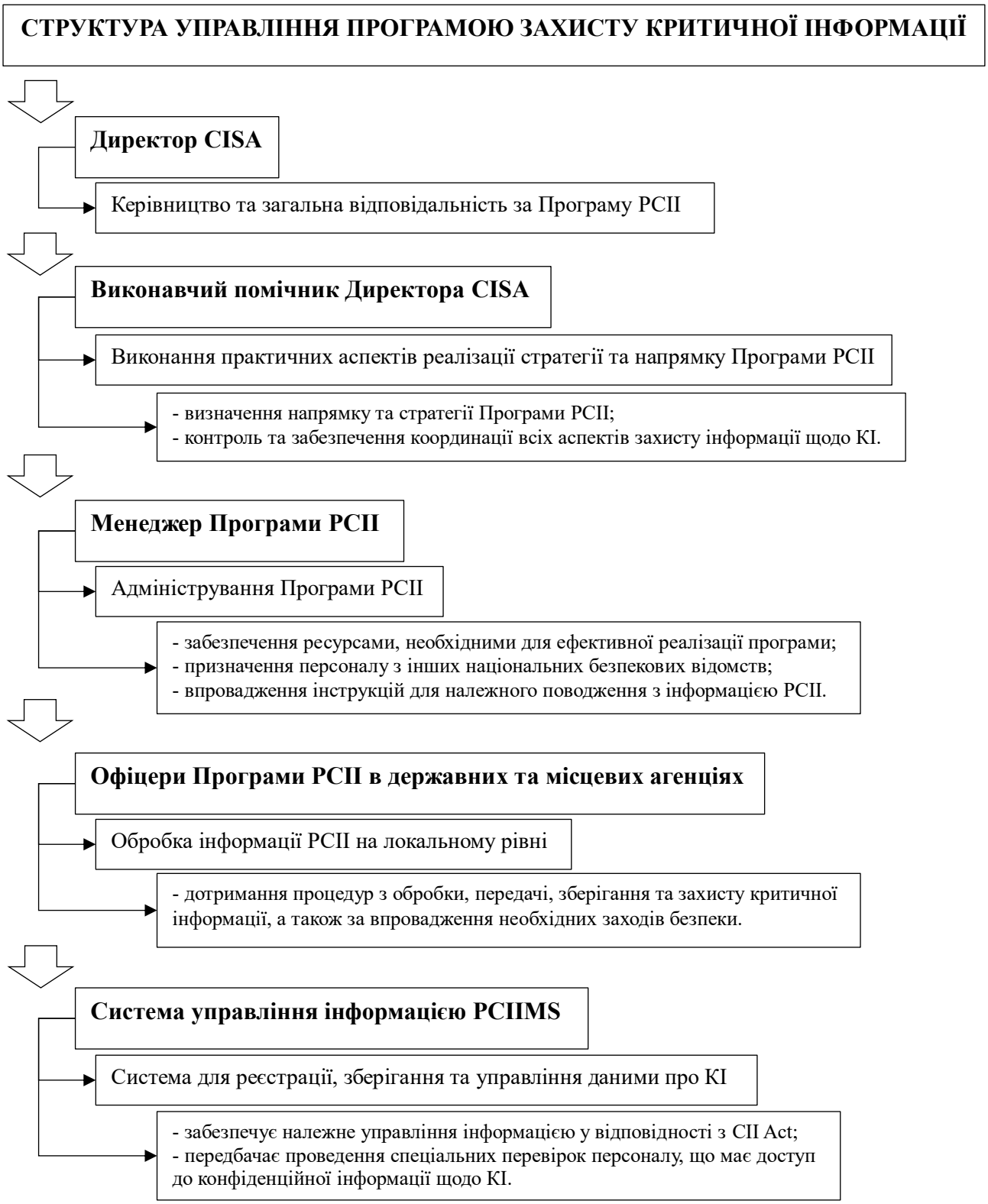


Рис. 3.6. Структура та рівні управління програмою захисту критичної інформації у США*

*Джерело: власна розробка автора

До обов’язків Директора CISA входить призначення менеджера Програми РСІІ, який працює під керівництвом Виконавчого помічника та несе основну

відповідальність за управління програмою. Обов’язки менеджера включають забезпечення ресурсами, необхідними для ефективної реалізації програми, призначення персоналу з інших національних безпекових відомств та впровадження інструкцій для належного поводження з інформацією PCII.

У свою чергу менеджер Програми зобов’язується призначити офіцерів PCII у всіх відповідних урядових агенціях, які працюють з інформацією PCII. Офіцери відповідають за дотримання процедур з обробки, передачі та зберігання цієї інформації, а також за впровадження необхідних заходів безпеки. Призначення офіцерів сприяє уніфікації дій та дозволяє підтримувати високу якість захисту інформації. Основні обов’язки офіцерів включають контроль за поводженням з інформацією PCII, забезпечення захищеного обміну інформацією з відповідними органами, створення внутрішніх перевірок для контролю за дотриманням норм і запровадження додаткових заходів для запобігання несанкціонованому доступу до PCII. Офіцери також координують дії з менеджером програми щодо запитів чи скарг, що виникають під час реалізації цих процедур.

Менеджер Програми PCII створює електронну базу даних для управління захищеною інформацією критичної інфраструктури PCIIMS з метою реєстрації всіх процесів, що пов'язані з отриманням, підтвердженням, зберіганням або знищенням, передачею або обміном та захистом інформації PCII. Система PCIIMS забезпечує належне управління інформацією у відповідності з Законом про критичну інфраструктуру, а також може передбачати проведення спеціальних перевірок персоналу, що має доступ до цієї інформації. За рахунок правильного розподілу повноважень та своєчасного виконання покладених на учасників процесу управління Програмою PCII функцій дана система забезпечує надійний захист критичної інформації. Такий підхід дозволяє забезпечити стійкість критичної інфраструктури, зокрема інформаційної, для протидії потенційним загрозам та забезпечення безпеки національних інтересів через чітке розподілення обов'язків, ефективну координацію між рівнями управління та використання спеціалізованих інструментів для моніторингу і контролю інформації.

Управління та захист критичної інформаційної інфраструктури Канади є ключовими елементами національної стратегії кібербезпеки, що спрямована на забезпечення захисту державних і приватних кіберсистем від зростаючих загроз у цифровому середовищі, яке згідно до Звіту щодо Цифрових амбіцій Канади у 2022 році (Canada's Digital Ambition) [162] характеризується безпрецедентними темпами та масштабами змін. Стратегія кібербезпеки Канади 2010 року (Canada's Cyber Security Strategy) [161] ґрунтується на трьох базових принципах, спрямованих на забезпечення стійкості інформаційних систем, підтримку економічного розвитку та захист канадських громадян:

I. Забезпечення довіри громадян до державних інформаційних систем передбачає захист персональної та корпоративної інформації громадян з боку канадського уряду, а також забезпечує високий рівень кібербезпеки електронних послуг. Захист суверенітету держави та кібербезпека національних інтересів є стратегічними пріоритетами, які вимагають значних інвестицій у створення відповідних структур та залучення висококваліфікованого персоналу, що спрямовано на підтримку кіберстійкості в окремих секторах, таких як охорона здоров'я, енергетика та транспорт [161];

II. Формування партнерств для захисту важливих кіберсистем за межами державного сектору передбачає функціонування системи співробітництва між урядом, місцевою владою та приватним сектором, що дає змогу координувати заходи щодо кібербезпеки та розвивати стратегії для зміцнення критичної інфраструктури. В рамках стратегії здійснюється прогнозування, виявлення та реалізація заходів з реагування на кіберзагрози, забезпечення національних інтересів та оптимізації використання кіберпростору [227];

III. Міжнародне співробітництво в галузі кібербезпеки включає участь Канади у глобальних ініціативах з розробки та впровадження міжнародних стандартів кіберзахисту, які сприяють підвищенню безпеки не тільки в країні, але й у всьому світі. Участь у проектах підвищення потенціалу системи кіберзахисту в країнах, що розвиваються, дозволяє Канаді спільно з міжнародними партнерами зміцнювати кіберстійкість глобальної системи, запобігаючи використанню слабких ланок для здійснення атак [275].

У межах забезпечення громадської безпеки Канадський центр реагування на кібератаки (Canadian Centre for Cyber Security) [163] виконує функцію координації моніторингу кіберзагроз, а також надає консультаційну допомогу щодо розробки та впровадження заходів з пом’якшення їх впливу. Одним із пріоритетів діяльності Центру є формування національної стратегії ефективного реагування на кіберзлочини, яка передбачає створення механізмів оперативного втручання при виникненні загроз у кіберпросторі. Служба громадської безпеки Канади (Public Safety Canada) [301] веде активну інформаційно-пропагандистську діяльність щодо потенційних ризиків, спрямованих на інформування громадян про потенційні ризики, які можуть виникнути в результаті кіберзагроз. Отже, запровадження національної системи безпечного зв’язку сприяє значному посиленню можливостей щодо своєчасного виявлення та реагування на загрози, забезпечуючи ефективність роботи органів зовнішньої розвідки та служби кібербезпеки. Здійснення комплексної підтримки повсюдної діяльності проти кіберзагроз дозволяє запобігти можливим збоям, які можуть призвести до серйозних політичних та економічних наслідків, а також підірвати довіру громадян до органів державної влади [18].

Натомість національний план захисту інфраструктури США (NIPP), розроблений Міністерством внутрішньої безпеки (DHS), визначає низку додаткових критичних секторів, що становлять особливу важливість для функціонування держави та безпеки національного масштабу. Дані сектори є невід'ємною частиною інфраструктурної стійкості, і їх захист є необхідною умовою для забезпечення національної безпеки, економічної стабільності та соціальної згуртованості. До таких критичних секторів відносяться: національні пам'ятники та ікони (пам'ятники, фізичні споруди, об'єкти та географічні місця, які представляють національну культуру або мають релігійне чи історичне значення); комерційні об'єкти (великі торговельні та бізнес-центри, офісні будівлі, спортивні стадіони та інші об'єкти, що вміщують велику кількість людей); критичне виробництво (підприємства, що здійснюють перетворення матеріалів на готову продукцію для інших галузей економіки, включаючи усі етапи виробництва і транспортування; база оборонної промисловості

(підприємства та об'єкти, що спеціалізуються на виробництві військових ресурсів, таких як зброя, техніка, літаки, кораблі, а також на забезпеченні основних служб національної безпеки) [112].

Міністерство внутрішньої безпеки США [187] виконує ключову роль у координації та інтеграції національних зусиль, спрямованих на захист критичної інфраструктури та ключових ресурсів (CIKR), зокрема шляхом розробки та впровадження комплексних багаторівневих програм управління ризиками. Такі програми передбачають методології, які дозволяють системно оцінювати та мінімізувати ризики на всіх етапах, охоплюючи як окремі сектори, так і міжсекторальні та міжюрисдикційні зв’язки. Основні зусилля DHS полягають у формулюванні настанов та рекомендацій щодо оптимізації заходів захисту, які враховують специфіку кожного сектору, що наведені на Рис., а також взаємодію різних юрисдикцій.

Ключові обов’язки DHS, які мають вирішальне значення у контексті реагування на надзвичайні ситуації, зокрема орієнтовані на забезпечення безпеки національно критичних активів, систем і мереж, передбачають проведення комплексної ідентифікації, пріоритизації та координації федеральних дій. У даному контексті особлива увага приділяється тим елементам інфраструктури, що можуть бути використані для нанесення катастрофічних наслідків, які за своєю руйнівною силою можуть бути порівнянні із застосуванням зброї масового знищення.

Слід також наголосити, що в межах взаємозалежних інформаційних структур важливою складовою є формування та підтримка з боку DHS динамічної багаторівневої мережі обміну інформацією, яка надає своєчасні та оперативно цінні дані про загрози, оцінки та попередження учасникам з державного та приватного секторів. До основних компонентів критичної інформаційної інфраструктури відносяться інформаційні системи, мережі зв'язку, бази даних, програмне забезпечення, а також організаційні структури, що забезпечують їх безпечне функціонування, в межах критичних секторів (Рис.3.7.), зокрема енергетики, транспорту, охорони здоров’я тощо.



Рис. 3.7. Характеристика об'єктів критичної інформаційної інфраструктури*

*Джерело: сформовано автором на основі [112, 187]

Формування мережі інформаційних структур вимагає від DHS забезпечення належного захисту конфіденційної інформації, що надходить від приватних компаній, а також створення ефективних механізмів і систем для обміну інформацією в межах окремих секторів та між секторами. Важливою частиною діяльності DHS є координація та впровадження комплексних програм оцінки ризиків для інфраструктури високого рівня критичності, що включає визначення пріоритетних напрямів захисту та інтеграцію захисних програм з підходами управління усіма загрозами (HSPD-5). Крім того, DHS визначає плани та процедури для посилення захисних заходів на основі виявлених загроз, які

відповідно коригуються в залежності від рівня загрози, що фіксується через систему внутрішньої безпеки США (HSAS) [187].

Промислові системи керування (ICS) є центральною ланкою у структурі критичної інформаційної інфраструктури, адже вони забезпечують відстеження та регулювання процесів на об'єктах стратегічного значення, включно з енергетичними станціями, системами передачі та розподілу електроенергії, водоочисними об'єктами, газо- та нафтопроводами, а також хімічними й нафтопереробними заводами [249]. ICS побудовані з використанням комунікаційної архітектури, які з’єднують головні керуючі центри з віддаленими об’єктами через автоматизовані підстанції. Важливими компонентами цих підстанцій є віддалені термінальні пристрої (RTU), оснащені сенсорами для моніторингу параметрів середовища та технічних процесів. Дані, зібрані RTU, передаються до центру управління, де відбувається їх аналіз і приймаються керуючі рішення, що реалізуються за допомогою виконавчих пристроїв.

Системи ICS складаються з кількох важливих типів: диспетчерські системи збору даних та управління (SCADA) і розподілені системи управління (DCS). SCADA є розподіленою мережею, що у процесі керування подіями поєднує географічно віддалені об’єкти через керуючий центр, підстанції та корпоративну мережу, охоплюючи всю структуру системи. Диспетчерський центр здійснює оперативне управління процесами, використовуючи сервери SCADA і сховища даних для збереження та обробки інформації. Безпека доступу до цих елементів забезпечується багаторівневим захистом, включно з брандмауерами, демілітаризованими зонами (DMZ), системами виявлення та запобігання вторгненням (IDS/IPS), а також антивірусним захистом. Слід зазначити, що розподілені системи управління (DCS) відрізняються від SCADA локальним характером, що є оптимальними саме для управління процесами в рамках однієї території або виробничого майданчика. Таким чином, DCS забезпечують високу ефективність керування окремими виробничими циклами без потреби у складній мережевій інфраструктурі, орієнтуючись переважно на інтеграцію технологічних процесів на конкретних виробничих об’єктах [112].

На сучасному етапі більшість SCADA-систем встановлюються для вищезазначених об’єктів критичної інформаційної інфраструктури з метою автоматизації процесів управління різними системами та їх підсистемами. SCADA-системи представляють собою складні електронні системи управління, головною функцією яких є збирання, моніторинг і аналіз даних у реальному часі. Завдяки цим системам забезпечується ефективне функціонування та координація діяльності критично важливих об’єктів, що робить SCADA незамінною основою сучасної інфраструктури. Тому можливі збої в роботі SCADA-систем потенційно становлять значну загрозу, яка може мати серйозні наслідки для забезпечення безпеки і стабільності всієї системи критичної інфраструктури [217].

Вразливість критичної інфраструктури зростає в умовах підвищених ризиків як природного, так і антропогенного характеру. Природні катаклізми, такі як землетруси та цунамі, можуть серйозно порушувати функціонування транспортної системи, тоді як антропогенні загрози, серед яких особливе місце посідають кібератаки, несуть потенціал руйнування ще більшого масштабу. У випадку успішної кібератаки можливе порушення безперервності надання критичних послуг, що в свою чергу загрожує суттєвими економічними та соціальними втратами для суспільства [370].

Наразі внаслідок стрімкого розширення бізнес-процесів та зростаючої необхідності централізованого моніторингу розподілених програмних засобів, SCADA-системи зазнали суттєвих трансформацій, еволюціонуючи до складних відкритих структур, інтегрованих із глобальною мережею за допомогою передових інформаційно-комунікаційних технологій [173]. Завдяки стабільному підключенню до Інтернету SCADA-системи забезпечують моніторинг та управління процесами на віддалених або топографічно важкодоступних об’єктах. Однак така інтеграція спричинила підвищення вразливості цих систем до потенційних зовнішніх атак, що можуть здійснюватися з будь-якої точки світу, створюючи серйозні ризики для їх безпеки.

Модернізація SCADA-систем, стандартизація протоколів зв’язку, а також зростання рівня взаємопов’язаності їхніх компонентів спричинили значне збільшення кількості цілеспрямованих кібератак на зазначені системи. Такі атаки

стають дедалі витонченішими, застосовуючи не лише методи традиційної кіберзлочинності, але й механізми кібершпигунства та промислового саботажу. Забезпечення безперервної та достовірної роботи SCADA-систем є стратегічним пріоритетом для промислових підприємств, оскільки вихід з ладу даних систем здатний призвести до тяжких наслідків, включно з масштабними фінансовими збитками, шкодою довкіллю та втратами людських життів [176].

У даному контексті особливу небезпеку становить потенційна кібератака на атомні електростанції, здатна викликати глобальні екологічні та економічні наслідки, виходячи за межі локального впливу. Аналогічно, порушення кібербезпеки у невеликих комунальних мережах може призвести до суттєвих фінансових збитків та втрати критичних послуг для населення, що підкреслює необхідність багаторівневих механізмів кіберзахисту, які здатні забезпечити стабільну та безпечну роботу SCADA-систем, що функціонують у критично важливих галузях економіки.

Оскільки різні об’єкти критичної інфраструктури є взаємозалежними, атака або порушення функціонування одного з них може спричинити ланцюгову реакцію, що вплине на інші системи. Одним із ключових напрямків діяльності DHS є саме здійснення моделювання та симуляція аналітики взаємозалежностей між секторами, що дозволяє виявити потенційні ризики на міжсекторальному та міжрегіональному рівнях, зокрема в контексті кіберзагроз. Крім того, DHS активно здійснює обмін результатами проведених досліджень і симуляцій із відповідними партнерами з безпеки для подальшого розвитку та вдосконалення механізмів захисту [187].

За результатами досліджень DHS визначаються напрямки запобігання виникненню збоїв в межах взаємозалежних секторів, що підкреслює необхідність комплексного підходу до захисту критичної інфраструктури. Приклад зазначених взаємозалежностей між різними елементами критичної інфраструктури, що ілюструє можливі наслідки відсутності захисту одного з її компонентів для загальної стійкості системи наведено на рис. 3.8.

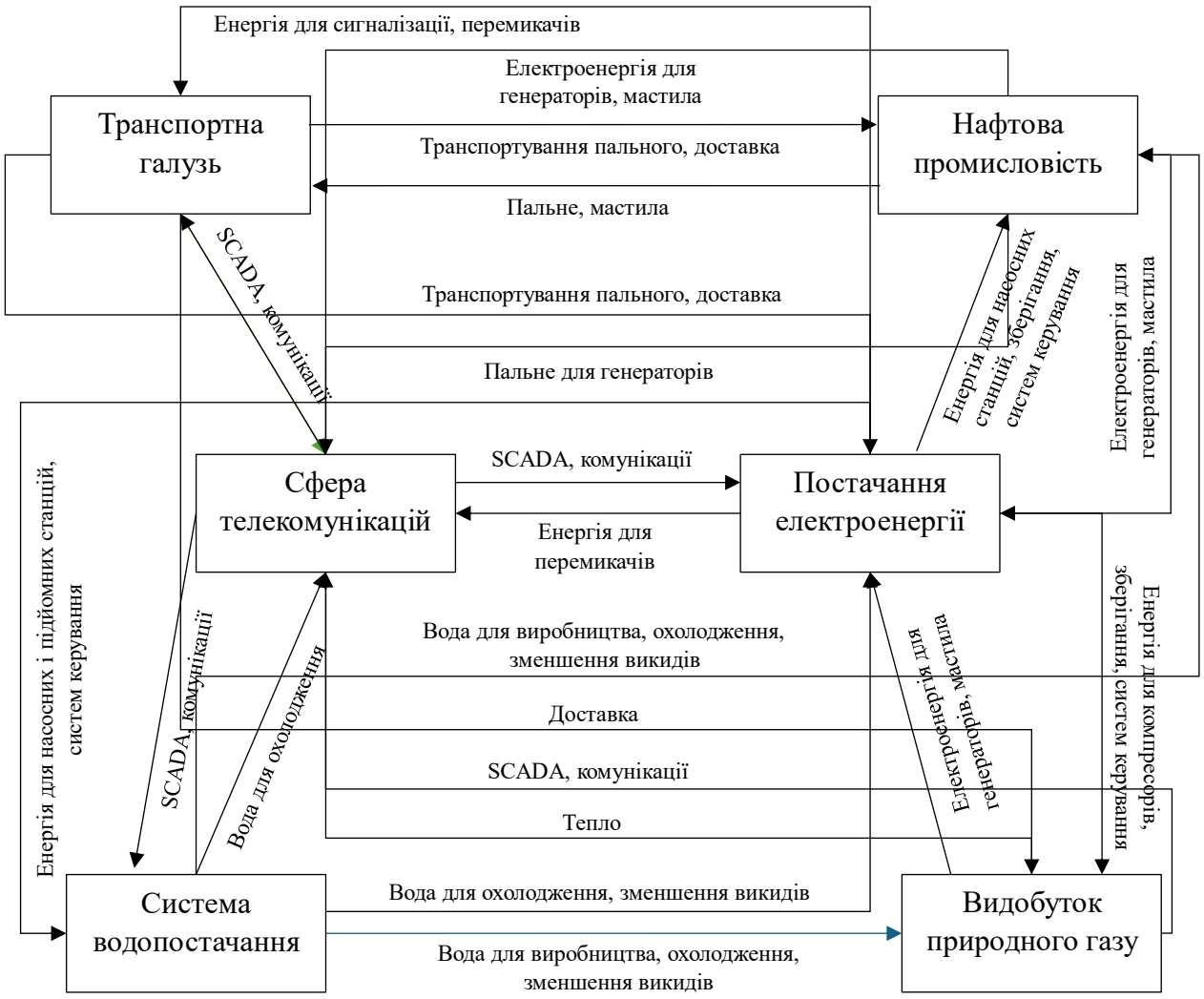


Рис. 3.8. Взаємозалежності критичної інфраструктури з встановленими системами SCADA*

*Джерело: сформовано автором на основі [187]

Таким чином, для безперервного функціонування систем, таких як водопостачання, необхідного для охолодження природного газу, необхідні сталі потоки ресурсів, включаючи запаси нафти та моторних олив (як пального, так і мастильних матеріалів), а також стабільне енергопостачання для насосних станцій. Крім того, підтримка працездатності системи SCADA потребує безперебійного функціонування управлінських і телекомунікаційних систем, які забезпечують передачу та обробку даних, необхідних для контролю та моніторингу. Для захисту цих систем від загроз, зокрема кібератак, необхідно впроваджувати спеціалізовані запобіжні заходи, спрямовані на підвищення безпеки кожного з компонентів.

З огляду на це, DHS активно співпрацює з міжнародними партнерами для зміцнення стійкості інфраструктури в умовах зростаючих глобальних ризиків, таких як зміна клімату, кіберзагрози, тероризм та інші, що ставлять під загрозу безпеку та функціонування ключових систем у всьому світі. У даному контексті співпраця є важливою складовою стратегії глобальної безпеки, адже в умовах сучасних глобалізаційних процесів та взаємозалежності різних національних систем, забезпечення надійного захисту критичної інфраструктури не обмежується суто внутрішньо національними процесами.

Взаємодія з міжнародними партнерами реалізується через механізми, що включають Міністерство закордонних справ США, а також взаємодію з іншими державними структурами, приватними установами та міжнародними організаціями, які займаються питаннями безпеки. Таке співробітництво охоплює міжсекторальні та міжгалузеві зв'язки, що сприяють обміну знаннями, досвідом та технологіями для забезпечення комплексного підходу до захисту критичної інфраструктури на глобальному рівні. Міжнародні партнерства також передбачають створення спільних платформ для обміну інформацією та координації дій у разі виникнення кризових ситуацій, таких як кіберзагрози або природні катастрофи, що можуть торкнутися не лише окремих країн, але й мати транснаціональний характер. Оскільки критичні інфраструктури мають тісні взаємозв'язки, порушення або відмова в роботі одного з елементів спричиняє ризики для функціонування інших, що потенційно здатне призвести до масштабних наслідків і дестабілізації системи в цілому.

3.4. Міжнародний досвід забезпечення кібербезпеки критичної інфраструктури

Сьогодні частота та масштаби кібератак на критичні об’єкти інфраструктури по всьому світу зростає, і багато країн шукають нові та ефективні методи захисту критично важливих ресурсів, таких як вода, електроенергія та газ, а також об’єктів, які виробляють, розподіляють та зберігають енергію. Згідно із

The Global Risks Report 2020 [330], кібератаки на об’єкти критичної інфраструктури займають почали з'являтися у цьому рейтингу після 2012 року, коли технологічні загрози набули більшого значення, і протягом останніх років перебувають на високих позиціях, займаючи у 2018-2019 роках п’яте місце за ймовірністю та сьоме місце за впливом, що відображає їхню здатність завдавати значної шкоди урядам, бізнесу та суспільству. Таким чином, кібератаки поступово закріплюються серед ключових ризиків, особливо за ймовірністю, що підкреслює потребу в заходах із кібербезпеки та посилення стійкості до таких загроз на міжнародному рівні. Тому міжнародний досвід забезпечення кібербезпеки критичної інфраструктури є надзвичайно актуальним в українському контексті з огляду на масштабність сучасних загроз та їх багатовимірний характер на тлі мінливої геополітичної ситуації.

Масштабне застосування кібернетичних засобів у ході агресії російської федерації проти України є необхідністю з огляду на супутню кібервійну росії, що увійшла в активну фазу після 24 лютого 2022 року, де кібератаки відіграють суттєву роль у дестабілізації української критичної інфраструктури [41]. Сучасні умови війни вимагають активної протидії з боку українських фахівців з кібербезпеки, а також розробки чіткої правової бази для регулювання процесів захисту критичної інфраструктури. Отже, внаслідок зростання складності та масштабів кібернетичних атак, спрямованих на критичні об'єкти, актуальним питанням національної безпеки стає кібербезпека, що має стратегічне значення для захисту національної інфраструктури, державних установ, а також цивільних та комерційних систем. Кібервійна, як новітній вимір гібридного конфлікту, здатна завдати значної шкоди, обходячи традиційні механізми оборони, і тому вимагає врахування можливостей та розробок глобального середовища для реалізації відповідних безпекових заходів.

Аналогічні ризики у сфері кібербезпеки спостерігаються у Ізраїлі. У жовтні 2023 року під час спільного наступу палестинської групи Hamas проти Ізраїлю поряд з кінетичними атаками спостерігалася інтенсивна кібернетична агресія з боку угруповань, пов’язаних з Hamas, Хезболлою, Іраном і Росією. Зазначені кібератаки були спрямовані на критичні інформаційні системи в урядовому,

комерційному та промисловому секторах Ізраїлю, що продемонструвало вразливість навіть найбільш захищених інфраструктурних об’єктів країни. Незважаючи на те, що Ізраїль витримав кібератаку «Цифрового 7 жовтня», такий досвід спричинив хвилю дискусій щодо необхідності переосмислення підходів до кіберзахисту на національному та глобальному рівнях, особливо щодо громадянського суспільства та інфраструктури.

В Ізраїлі критична національна інфраструктура перебуває під особливою загрозою кібернетичних атак, що зумовлено складною архітектурою та технологічними особливостями промислових систем керування. Такі системи функціонують на основі застарілого обладнання і специфічних промислових протоколів, таких як ICS/SCADA, які були розроблені без урахування сучасних вимог до кібербезпеки. Отже, захист даних і процесів у таких мережах вимагає унікальних технологій кібербезпеки, орієнтованих саме на вразливості операційних технологій (ОТ). У даному контексті основною проблемою є процес конвергенції мереж ОТ та ІТ, коли традиційні ІТ-додатки, зокрема інтерфейси людино-машинної взаємодії (HMI), отримують доступ до пристроїв і мереж ОТ. Даний процес сприяє формуванню нових векторів атак, оскільки зловмисники можуть використовувати ІТ-мережі як проміжні шлюзи для проникнення в критичні ОТ-системи. Подібне переплетіння ІТ та ОТ, з одного боку, покращує ефективність та інтеграцію процесів, але водночас відкриває нові точки уразливості, оскільки ІТ-інфраструктура часто не має достатнього рівня захисту для забезпечення безпеки критичних ОТ-компонентів.

Атаки на критичну інфраструктуру, в тому числі на промислові системи управління, все частіше включають початкове компрометування ІТ-компонентів для подальшого поширення в ОТ-мережі. Така стратегія використовується для обходу класичних захисних бар’єрів, що фокусуються виключно на ОТ-рівні, і вказує на необхідність розробки інтегрованих багаторівневих систем захисту, здатних забезпечити високий рівень кіберстійкості. Тому для Ізраїлю актуальним стає формування глибоко ешелонованого підходу до кіберзахисту критичної інфраструктури, який би враховував як особливості ОТ, так і вимоги до ІТ-безпеки. Такий підхід передбачає комплексне зміцнення кібербезпеки шляхом

синергії між технологіями захисту операційних і інформаційних систем, що є критично важливим у контексті зростання кіберзагроз та розвитку гібридних форм агресії.

Наразі Ізраїль має чітко визначену політику в галузі кібербезпеки критичної інфраструктури, яка пройшла кілька етапів розвитку, від початкової участі оборонного відомства до створення національної політики захисту комп'ютеризованих систем. Сучасна стратегія кіберзахисту Ізраїлю є комплексною системою заходів, спрямованих на захист національних інтересів у цифровій сфері та забезпечення стійкості країни до сучасних кіберзагроз (Рис.3.9.). Дана стратегія охоплює міжнародну співпрацю, національні ініціативи, захист критичної інфраструктури, обмін інформацією, а також просування новітніх технологій кібербезпеки. Особливо увага приділяється ідентифікації та протидії перед стійким загрозам (APT), які можуть є високоризикованими для держави. Крім того, стратегія сконцентрована на підвищенні обізнаності громадськості, створенні ефективного регулювання та розвитку технологічної інфраструктури, що сприяє систематичному зміцненню та розвитку кібербезпеки критичної інфраструктури.

Першим важливим нормативно-правовим актом, що посприяв формуванню зазначеної політики, стала Спеціальна резолюція B/84, прийнята Міністерським комітетом з національної безпеки 11 грудня 2002 року [324].

Резолюція B/84 визначила відповідальність за захист комп’ютеризованих систем, що стали частиною національної стратегії кібербезпеки, і є основою для розробки інших правових актів у сфері захисту критичної інфраструктури Ізраїлю. Основні положення цієї резолюції зазначають, що «кіберпростір» не є окремим простором, а є частиною фізичних просторів, що потребує інтегрованої стратегії кіберзахисту.

Також важливим аспектом є розмежування «інформаційних» та «контрольних» систем, де інформаційні системи відповідають за обробку та передачу даних, а контрольні системи здійснюють нагляд за технологічними процесами в межах інформаційних систем.

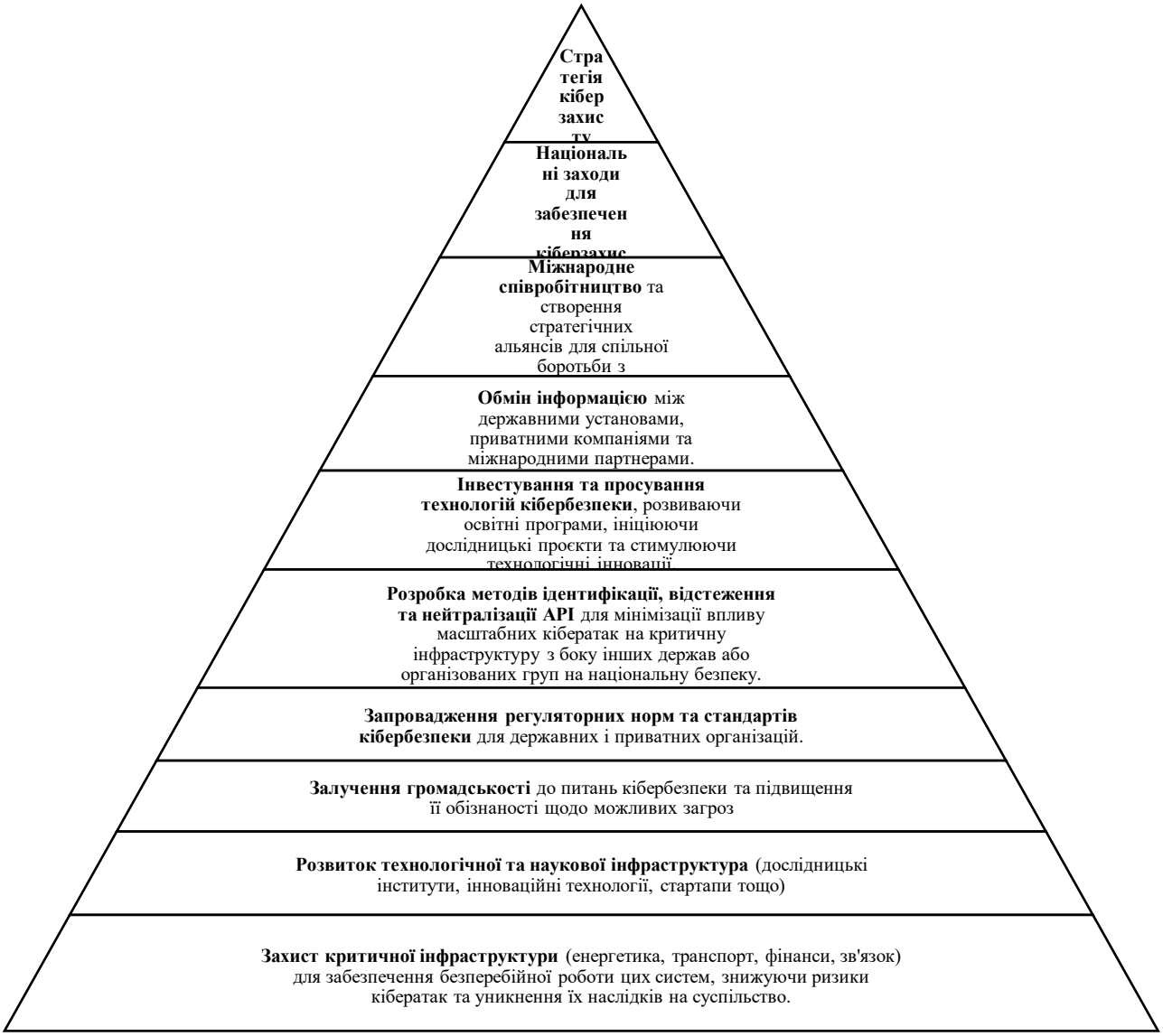


Рис. 3.9. Складові стратегії забезпечення кібербезпеки критичної інфраструктури Ізраїлю*

*Джерело: сформовано автором на основі [330, 324]

Додатково до резолюції B/84, на рівні законодавства Ізраїлю були прийняті інші нормативно-правові акти, що регулюють питання кібербезпеки та захисту критичної інфраструктури: Закон про кібербезпеку 2018 року (Cybersecurity Law, 2018) створює правові основи для координації заходів щодо кіберзахисту критичних секторів економіки та управління кіберзагрозами в Ізраїлі, а також визначає обов'язки організацій щодо забезпечення кібербезпеки та передбачає санкції за порушення [305]; та Закон про безпеку інформації в державних органах 2007 року (PPL 5741-1981), що визначає вимоги до захисту державних

інформаційних систем і установ, а також уточнює роль різних державних органів у забезпеченні безпеки даних [332].

Згідно з цими нормативно-правовими актами, відповідальність за захист критичних комп'ютеризованих систем покладається на організації, які здійснюють контроль і управління цими системами, а також на державних регуляторів, серед яких є Міністерство комунікацій (захист телекомунікаційних мереж), Міністерство фінансів (для фінансових установ) та інші відповідальні органи. Одним із важливих органів, що здійснює нагляд, є Національна інформаційна служба безпеки (NISA), яка відповідно до Спеціальної резолюції B/84 має ряд обов’язків, серед яких оцінка загроз кібербезпеки, розробка захисних стратегій, інтеграція розвідки та підтримка досліджень у галузі кіберзахисту. Особливе значення має також Міністерство оборони (MoD) та його підрозділ Maƒ’at (Оборонний директорат наукових досліджень і розвитку), який ініціював роботу з розробки національної стратегії з кібербезпеки та надав підтримку в створенні відповідних нормативно-правових актів [324].

Зокрема, Закон про кібербезпеку, ухвалений в 2018 році має на меті створення Ізраїльського національного кіберуправління (INCD), яке отримало розширені повноваження у питаннях кібербезпеки на національному рівні. INCD стане центральним органом для розробки національних політик і інструкцій щодо кіберзахисту для критично важливих інфраструктурних секторів, таких як фінанси, охорона здоров’я, енергетика, транспорт і зв’язок. Зазначені повноваження часто виходять за межі традиційних ролей органів безпеки та військових, що значно розширює обсяг контролю в сфері кібербезпеки. Однією з важливих інновацій цього законопроекту є те, що INCD має підзвітність безпосередньо перед прем’єр-міністром, який визначатиме стратегічні пріоритети щодо кіберзагроз і політики кібербезпеки [320]. Такий підхід дозволяє країні оперативно реагувати на швидко змінювані загрози в кіберпросторі. На відміну від традиційних інституцій, що відповідають за безпеку в інших сферах, INCD наділяється значними юридичними повноваженнями для активного впливу на діяльність як приватних, так і державних організацій, включаючи безпосереднє втручання в інфраструктуру,

яка може бути визнана загрозою для національної безпеки. Проте, незважаючи на значні переваги в сфері національної безпеки, даний Закон став предметом дискусій, оскільки на думку правозахисних організацій, зокрема 7amleh, його положення можуть суперечити основним демократичним принципам, таким як право на приватність, свободу вираження думок та доступ до правосуддя. Водночас його реалізація уможливлює ефективне управління національною кібербезпекою, що є важливим фактором у сучасному глобалізованому та цифровому світі [332].

Наразі в Австралії створена багаторівневу систему регуляторного нагляду за критичною інфраструктурою, що спрямована на забезпечення національної безпеки, ефективності та відповідності державного управління. Основними нормативно-правовими актами, що регулюють управління критичною інфраструктурою, є Закон про державне управління, ефективність і підзвітність 2013 року (Закон PGPA), який сприяє повноваженню державних суб'єктів господарювання, та низка делегованих законодавчих актів, зокрема Правила державного управління, ефективності та підзвітності 2014 року (Правила PGPA), Правила закупівель Співдружності та Політика Співдружності щодо управління ризиками.

І. Закон про безпеку критичної інфраструктури 2018 року (SOCI) [315] встановлює юридичні вимоги для організацій, які володіють, керують або мають інтереси в активах критичної інфраструктури Австралії. Даний закон спрямований на зміцнення безпеки в одинадцяти ключових секторах, серед яких комунікації, фінансові послуги, оборона, енергетика, охорона здоров'я, транспорт, водопостачання та інші важливі сфери, забезпечення функціонування яких є критичним для національного добробуту та безпеки країни. Закон забезпечує державну підтримку у разі інцидентів, що загрожують функціонуванню критичних об'єктів, і дозволяє швидко реагувати для мінімізації впливу на основні послуги та економіку.

Закон SOCI зобов'язує операторів критичної інфраструктури виконувати три основні вимоги: надавати інформацію про власників активів для національного реєстру, повідомляти Австралійський центр кібербезпеки про

інциденти, що впливають на основні послуги, та підтримувати листи програми управління ризиками. Крім того, для активів, що мають національне значення, діють додаткові вимоги: розробка планів реагування на кіберзлочини, проведення навчання, оцінка вразливостей та регулярне оновлення інформації для забезпечення своєчасного реагування на загрози. Закон SOCI також передбачає повноваження держави допомогти операторам критичної інфраструктури у випадках кіберінцидентів, які мають серйозний вплив на безпеку та добробут країни. Також даний закон встановлює чіткі вимоги щодо конфіденційності інформації про критичні об'єкти, обмежуючи доступ до неї відповідно до встановлених нормативів. У межах нормативної позиції 2024-2025 років передбачено збалансованість між навчанням, підвищення обізнаності операторів та забезпечення відповідності їх діяльності вимогам закону, що сприятиме більш ефективному забезпеченню національної кібербезпеки та стійкості інфраструктури.

II. Нормативно-правове регулювання критичної інфраструктури в Австралії обґрунтовується на комплексній системі законодавчих актів, що спрямовані на забезпечення ефективного, прозорого та підзвітного управління. Основні положення цієї системи закріплені в Законі PGPA 2013 року [294], які визначають повноваження та обов'язки державних суб'єктів господарювання. Важливими елементами цього законодавства є також делеговані нормативні акти, такі як Правила PGPA 2014 року [298], Правила закупівель Співдружності 2024 року (CPRs) [179] та Політика Співдружності щодо управління ризиками 2022 року [180]. Дані нормативно-правові акти встановлюють рамкові стандарти, відповідно до яких суб'єкти критичної інфраструктури мають здійснювати свою діяльність з урахування.

III. Ефективність урядового регулювання в Австралії посилюється за допомогою Структури ефективності регуляторної політики [306; 307], впровадженої в жовтні 2014 року, що спрямовує державних регуляторів на досягнення поставлених цілей, забезпечуючи баланс між дотриманням вимог та мінімізацією адміністративного тиску на регульовані організації. Проте, з 1 липня 2021 року в рамках Посібник з ефективності регуляторних органів

Співдружності (CRPG) [306], що замінив попередню рамку 2014 року, було впроваджено перехідний період для адаптації нових принципів регулювання. посібник закладає нові стандарти та інструменти для оцінки діяльності регуляторів, дозволяючи їм коригувати свої стратегії для забезпечення високої якості державного нагляду.

IV. Найголовнішим нормативно-правовим актом для забезпечення кібербезпеки критичної інфраструктури Австралії Закон про безпеку критичної інфраструктури 2018 року (SOCI) [315], що формує правові основи забезпечення кібербезпеки та зниження ризиків для критичних об’єктів. Проте, Програма управління ризиками критичної інфраструктури (CIRMP) [189] встановила конкретні вимоги, які мають бути виконані до серпня 2024 року, таким чином, забезпечивши високий рівень безпеки та стандартизації кіберзахисту в національному масштабі. Такі компанії, як Industrial Defender, надають австралійським операторам критичної інфраструктури засоби для підтримки зазначених вимог, зміцнюючи їхню готовність до кіберзагроз і забезпечуючи відповідність стандартам, як Система кібербезпеки енергетичного сектору (AESCSF).

Інноваційний підхід до забезпечення кібербезпеки критичної інфраструктури Австралії полягає у розробці заходів щодо стратегічного партнерства між компанією Google та національним науковим агентством CSIRO у 2024 році [289], орієнтованому на створення цифрових рішень для автоматизованого виявлення та усунення вразливостей у програмному забезпеченні. Розроблені інструменти, розроблені з урахуванням вимог місцевих регуляторів, забезпечують адаптацію безпекових систем для таких критично важливих секторів, як охорона здоров'я, оборони та енергетики. Впровадження цього програмного забезпечення сприятиме підвищенню стійкості до кіберзагроз, що набуває особливого значення з огляду на збільшення кількості кібератак, які призвели до компрометації персональних даних значної частини критичних об’єктів Австралії.

Співробітництво між Google та CSIRO забезпечує об'єднання штучного інтелекту та бази даних про вразливість з відкритим кодом, що забезпечує

комплексний підхід до виявлення кіберзагроз і захист цифрових систем. Такий підхід відповідає довгостроковій стратегії щодо інвестування Google у кібербезпеку Австралії, спрямованій на зміцнення цифрової безпеки національних інфраструктурних об’єктів та забезпечення відповідності вимогам місцевого регуляторного середовища, що підвищує рівень кібербезпеки та надійності інфраструктурних систем. Дана ініціатива є частиною багаторівневої інвестиційної програми Google, яка передбачає виділення 1 млрд. дол. на розвиток цифрових технологій в Австралії. Таким чином, уряд активізував свою діяльність у сфері обороноздатності критично важливої інфраструктури, а також забезпечує відповідність національним та міжнародним стандартам кіберзахисту, знижуючи ризики кіберзагрози в усіх сферах, де безпека є важливою складовою.

Висновки до розділу 3

1. Аналіз досвіду провідних країн ЄС, зокрема Франції, Нідерландів та Великобританії, демонструють успішні приклади координації національної політики, застосування трирівневих методологій оцінки ризиків та створення інтегрованої платформи для обміну інформацією. Важливим елементом є також розробка стратегічних політичних заходів, які базуються на аналізі економічної доцільності та довгострокової стійкості інфраструктури. Стійкість критичної інфраструктури розглядається не тільки як здатність до відновлення після інцидентів, але й як можливість адаптації до нових умов і збереження основних функцій, що потребує ефективної взаємодії між державними структурами та приватними операторами, що у своїй програмі формує довіру та спільні цілі у забезпеченні безпеки. Важливою є також роль державно-приватного партнерства, яке сприяє конструктивному діалогу, створюючи умови для спільної розробки політики. Водночас виявлені різниці в рівнях вимог безпеки між державами-членами можуть призвести до неоднорідності стійкості та негативно вплинути на функціонування внутрішнього ринку ЄС. Таким чином, досвід держави ЄС у сфері управління трансформацією критичної інфраструктури підкреслює

потребу в інтегрованому підході, який охоплює взаємодію між усіма зацікавленими сторонами, чітке визначення позицій, стратегічне планування та забезпечення механізмів підзвітності для досягнення високих стандартів стійкості.

2. Стратегія ЄС щодо захисту критичної інфраструктури забезпечує широку міждержавну та міжсекторальну взаємодію, враховуючи, що значна частина таких об’єктів перебуває у приватній власності; що обумовлює створення комплексної нормативно-правової бази, яка сприяє державно-приватному партнерству та підвищує стійкість до різноманітних загроз, зокрема природних катастроф, техногенних аварій та терористичних атак. У зв’язку зі зростанням глобальних загроз, в ЄС активно розробляються заходи для гармонізації підходів до класифікації критичної інфраструктури, що посилює координацію заходів з її захисту у країнах-членах ЄС. Зважаючи на євроінтеграційну політику України синхронізація підходів до управління критичною інфраструктурою з європейськими стандартами, враховуючи специфіку національної безпеки, дозволить побудувати надійну систему захисту критичних об’єктів та підвищити стійкість держави до потенційних загроз та поточних ризиків в умовах війни.

3. Дослідження управлінських практик та захисту критичної інформаційної інфраструктури в США та Канаді демонструє високий рівень організації та міжсекторальної співпраці у захисті критичних ресурсів, що має особливу актуальність для України. У США, зокрема, створена система чітко визначених нормативно-правових актів, що охоплюють такі аспекти критичної інфраструктури, як управління фізичними та цифровими об’єктами критичної інфраструктури, захист інформації критичної інфраструктури, підтримка довіри між державними та приватними операторами та покращує захист від кіберзагроз за рахунок чітко визначених відповідальних осіб. Натомість канадський підхід передбачає стабільне функціонування критичної інфраструктури за рахунок забезпечення кіберстійкості, партнерства між державним і приватним секторами та міжнародного співробітництва. У даному контексті в українському контексті доцільно адаптувати принципи міжвідомчої координації, партнерства між

державою та бізнесом, а також управлінські та організаційні підходи до захисту конфіденційних даних, що забезпечують ефективний захист від кіберзагроз, підтримку економічної стабільності та стійкості національних інтересів в умовах сучасних викликів.

4. Аналіз нормативно-правової бази щодо забезпечення кібербезпеки критичної інфраструктури на прикладі Ізраїлю та Австралії демонструє, що ефективний захист критично важливих об’єктів у кіберпросторі вимагає всебічного підходу, який охоплює нормативно-правові, організаційні, технологічні та координаційні аспекти. Досвід Ізраїлю свідчить про важливість оновлення стандартів кібербезпеки та потребу у зміцненні стійкості критичної інфраструктури, включаючи цивільні сектори. Зростаюча кількість і комплексність кібератак підкреслюють важливість міжнародного співробітництва, обміну інформацією та спільної розробки нормативно-правових актів, які б відповідали сучасним загрозам. Боротьба з кіберзагрозами вимагає не лише вдосконалення технічних засобів захисту, а й формування єдиного правового поля та політик, що сприятимуть підвищенню рівня захищеності критичної інфраструктури у глобальному масштабі. Австралія, у свою чергу, приділяє значну увагу створенню нормативно-правової бази для захисту критичної інфраструктури, що забезпечує активне залучення приватного сектору до управління кібербезпекою та розробки технологій для посилення стійкості національних мереж. З огляду на виявлені тенденції розвитку практики кібербезпеки критичної інфраструктури для України використання ізраїльської моделі централізованої координації дозволить оперативно реагувати на кіберзагрози, а австралійський підхід до регулювання та залучення бізнесу посприяє формуванню стійкої та гнучкої системи захисту.

РОЗДІЛ 4
ЕФЕКТИВНІСТЬ ПУБЛІЧНОГО УПРАВЛІННЯ ТРАНСФОРМАЦІЄЮ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВІЙСЬКОВОГО СТАНУ ТА ЇЇ ВІДНОВЛЕННЯ В ПОВОЄННОМУ ПЕРІОДІ

4.1. Стан пошкодження та руйнувань об'єктів критичної інфраструктури у період війни

Стан об'єктів, що належать до критичної інфраструктури, (таких як об'єкти сфери енергетики, телекомунікації, комунального господарства транспорту, охорони здоров'я) під час війни суттєво погіршився. Саме об'єкти інфраструктури стали однією з мішень найбільших атак з боку російського агресора. Має місце руйнування та пошкодження суттєвої кількості таких об'єктів в результаті бойових дій. Російські атаки завдали значної шкоди численним об'єктам енергетичної інфраструктури, транспортним вузлам, водопровідним системам та іншій критично важливій інфраструктурі. Це спричинило суттєві труднощі з доступом до електроенергії, водопостачання та транспортних маршрутів для населення, що підтверджують статистичні дані, зібрані впродовж останніх років. Відповідно до цих даних, більше половини об'єктів критичної інфраструктури України зазнали руйнувань або серйозних пошкоджень [53].

Для оцінювання стану та зруйнованості об'єктів критичної інфраструктури пропонуємо власну методику. Загалом методика складається зі кількох напрямків оцінювання: I. Втрата функціональності об'єкта (F); II. Фізичні пошкодження (D); III. Строк можливого відновлення функціональності об'єкта (T); IV. Ступінь критичності порушення (K); V. Негативний вплив на галузі економіки (E), див. табл. 4.1. Перші три є базовими й характеризують стан самого об'єкта Дві інші є контекстними й характеризують значущість порушення для системи загалом.

Таблиця 4.1.

Параметри та індикатори класифікації стану пошкодження та руйнувань об’єктів критичної інфраструктури у період воєнного стану*

№пп	Класифікаційна ознака	Характеристика
1	Втрата функціональності об’єкта (F)	Бальна оцінка 0: функцію збережено; 1: часткове зниження, до 25 %; 2: суттєве зниження, 25–60 %; 3: критичне зниження, 60–90 %; 4: повна втрата функції, понад 90 %
2	Фізичні пошкодження (D)	Бальна оцінка 0: пошкоджень немає; 1: поверхневі, лише ненесучі елементи; 2: помірні, окремі несучі елементи чи обладнання, придатні до ремонту; 3: значні, несучі конструкції чи ключове обладнання потребують заміни; 4: руйнування, потрібне нове будівництво
3	Строк можливого відновлення функціональності об’єкта (T)	Бальна оцінка 0: відновлення до 72 год; 1: відновлення до 30 діб; 2: відновлення до 1–6 міс.; 3: відновлення до 6–24 міс.; 4: відновлення понад 24 міс.
4	Ступінь критичності порушення (K)	Відповідно до категорії критичності об'єкта (I–IV) з урахуванням можливості резервування чи заміщення послуги (від 1 до 4 балів)
5	Негативний вплив на галузі економіки (E)	Локальний → муніципальний → регіональний → міжрегіональний → національний; кількість залежних секторів, де виникли збої (від 1 до 4 балів)

*Джерело: власна розробка автора

Оцінювання здійснюється за таким алгоритмом:

Етап I. Ідентифікація та первинна фіксація пошкоджень. Використовуються дані операторів ДСНС, органів місцевої влади, дистанційного зондування та обстежень;

Етап II. Оцінювання за базовими ознаками і розрахунок базового індексу пошкодження;

Етап III. Визначення критичності порушення та масштабу впливу з урахуванням категорії об'єкта та наявності резервних потужностей;

Етап IV. Аналіз каскадних ефектів на основі матриці міжсекторних залежностей: визначається кількість суміжних секторів, у яких виникли або прогнозуються збої;

Етап V. Урахування просторових чинників, які впливають на ризик повторного ураження та реальні строки відновлення;

Етап VI. Визначення інтегрального класу стану об'єкта та пріоритету його відновлення;

Етап VII. Ухвалення управлінського рішення та моніторинг. Клас періодично переглядається за результатами повторних уражень або завершення етапів відновлення.

Базовий індекс пошкодження може визначатись за такою формулою 4.1:

$$Id = 0,35*F + 0,35*D + 0,3*T \quad (4.1)$$

де, Id – Інтегральний індекс стану класифікації стану пошкодження та руйнувань об’єктів критичної інфраструктури/

Інтегральний індекс стану класифікації стану пошкодження та руйнувань об’єктів критичної інфраструктури у період воєнного стану з врахуванням критичності, може мати такий вигляд:

$$Iid = Id * K \quad (4.2)$$

де, Iid – Інтегральний індекс стану класифікації стану пошкодження та руйнувань об’єктів критичної інфраструктури у період воєнного стану з врахуванням критичності, K – коефіцієнт критичності: категорія I = 1,5; II = 1,3; III = 1,15; IV = 1,0;

Вагові коефіцієнти й порогові значення визначаються експертним методом і можуть калібруватися для окремих секторів КІ.

Відповідно, стан пошкодження може мати такі класи і значення:

Клас I (значення Iid < 1,0) Мінімальні пошкодження, функцію збережено. Стратегія Планове відновлення силами оператора в межах поточного бюджету. Пропозиції до фінансування: власні кошти оператора, підрядники.

Клас II. (значення Iid 1,0–2,0) Обмежені пошкодження, часткові функціональні втрати без значних каскадних ефектів Стратегія відбудови. Відновлення оператором за координації місцевих органів влади, строк до 30 діб. Пропозиції до фінансування: оператор, місцеві бюджети, малі гранти, гуманітарне обладнання, підрядники, спонсорська допомога.

Клас III. (значення Iid 2,0–3,5) Суттєві пошкодження з регіональними наслідками Стратегія Залучення регіональних ресурсів, тимчасові схеми

резервування, державна підтримка. Пропозиції до фінансування: обласні бюджети, Фонд ліквідації наслідків збройної агресії, співфінансування, страхові виплати.

Клас IV. (значення Iid 3,5–5,0) Критичні пошкодження з міжсекторними наслідками Стратегія Першочергове відновлення, міжвідомча координація, мобілізація державних і донорських ресурсів нальних ресурсів, тимчасові схеми резервування, державна підтримка. Пропозиції до фінансування: Державний бюджет, цільові програми Ukraine Facility, МФО (ЄБРР, ЄІБ, Світовий банк)

Клас V. (значення Iid > 5,0) Катастрофічні руйнування з національним масштабом впливу Стратегія Невідкладні рішення на рівні КМУ, тимчасове заміщення функції, ухвалення рішення щодо відновлення чи нового будівництва з урахуванням принципу «build back better» і безпекових ризиків. Пропозиції до фінансування: Пакетне донорське фінансування.

Реєстр пошкоджених об'єктів може складатись по паспортах об’єктів. Структура паспорта об'єкта:

1. Ідентифікація об’єкта та його первинні характеристики: код, сектор і підсектор КІ, оператор, точка геолокаї, клас критичності.
2. Характеристика пошкоджень та руйнувань: дата, година руйнування, причина, ступінь фізичних руйнувань, фото- і відеофіксація, акт обстеження.
3. Функціональний блок: втрачена потужність (%), кількість споживачів без послуги, наявність резерву.
4. Вплив на інші об’єкти: вплив на об’єкти КІ і економіку.
5. Безпека: типи небезпеки та загрози для об’єкта КІ в майбутньому.
6. Фінансування: попередня оцінка та розрахунок збитків, кошторис для відновлення функціонування та пропозиції щодо фінансування.
7. Статус: розрахований індекс Iid, клас, ранг, етап робіт, результати моніторингу.

Дослідження підкреслюють, що найбільшу частку загальних збитків становлять втрати у житловому секторі, які оцінюються приблизно в $55,9 млрд. Ця сума включає близько $1 млрд через затоплення та руйнування житлових будинків, спричинених підривом дамби Каховської ГЕС. Друге місце за

масштабами збитків посідає інфраструктурна сфера — транспортна, дорожня, залізнична, авіаційна та портова, із загальною сумою втрат у $36,6 млрд. [53].

Під час цієї війни українці зазнали значних збитків та втрат в енергетиці, тоді як Росія продовжує погрожувати посилити свої атаки. У цій ситуації населення України зазнало численних відключень електроенергії, а атаки Росії на українські генеруючі (тобто виробничі) потужності та мережу передачі електроенергії призвели до відключень електроенергії, про які повідомлялося навіть у сусідній Молдові. Однак Україні вдалося витримати всі російські ракетні атаки – протиповітряна оборона значно посилилася, велика підтримка була отримана від країн ЄС (включаючи Литву) та США, а також розпочалася децентралізація енергосистеми. Зменшення загального споживання електроенергії в країні внаслідок війни також допомогло збалансувати енергетичну систему.

Однак збитки, завдані енергетичній інфраструктурі внаслідок агресії Росії, оцінюються в мільярди євро. Повне відновлення енергетичної системи від втрат займе кілька років і вимагатиме значних ресурсів. Україна ставить перед собою мету не лише відновити зруйновану енергетичну інфраструктуру, а й відновити її за принципом «Відбудуємо краще» (Build Back Better). Саме тому актуально проаналізувати, які збитки зазнала енергосистема України, як вдалося відновити пошкоджену інфраструктуру, які є основні подальші виклики та можливості розвитку енергетичного сектору.

Зима 2022/2023 року стала найчутливішою для енергосистеми України під час цієї війни. Атаки були регулярними, з використанням типових російських крилатих та балістичних ракет, а також безпілотників (включаючи сумнозвісні іранські безпілотники «Шахид»), артилерії, розгорнутих уздовж кордонів та ліній фронту. Найбільшою слабкістю України на той час була нестача систем ППО та боєприпасів. Президент В. Зеленський неодноразово звертався до західних союзників з проханням надати підтримку системами ППО – не лише сучасними радарами чи ракетами NASAMS середньої дальності, платформами IRIS-T або SAMP/T Mamba та далекобійними американськими Patriot, але й збереженими системами ППО, такими як MIM 23 Hawk (технологія 1960 року)

або радянські С-125, С-200 чи С-300. Хоча ці системи старі та не мають можливостей сучасних систем ППО, їхньою найбільшою перевагою є наявність запасів боєприпасів.

З кінця зими 2022/2023 років атаки на українську енергетичну інфраструктуру значно зменшилися. Літо 2022 та 2023 років було менш сприятливим для таких атак. Найважливішою подією літа 2023 року стало руйнування дамби Нова Каховка поблизу міста Херсон, ймовірно, здійснене для зменшення можливостей українців здійснювати контратаку на лівому березі Дніпра. Дамба була важливим об'єктом не лише завдяки своїй генеруючій потужності, а й для формування ландшафту та екосистеми в регіоні. Збільшена течія скинула велику кількість брудної води та різного сміття в Чорне море, порушила не лише електропостачання, а й водопостачання значної частини півдня України (включаючи Крим, який забезпечувався водою з Каховського водосховища). Повені, що виникли після підриву дамби, затопили низку населених пунктів у Херсонській адміністративній області, як на контрольованій Україною, так і на контрольованій Росією частині. Водосховище, утворене дамбою, також мало важливе значення для забезпечення охолодження Запорізької атомної електростанції. Його знищення можна вважати найруйнівнішою окремою подією з початку вторгнення у лютому 2022 року.

Згідно з інформацією, наданою Повітряними силами України, до кінця 2023 року Росія випустила 7400 ракет та 3700 безпілотників «Шахед» по різних цілях в Україні. Однак ситуацію виправила підтримка України з боку Заходу – до тієї зими Україна придбала та інтегрувала більше систем протиповітряної оборони, що дозволило їй захищати найважливіші об'єкти. Таким чином, покращення ситуації в енергетичному секторі було зумовлене: 1) зміною тактики Росії; 2) посиленням української протиповітряної оборони після отримання більшої підтримки протиповітряної оборони від Заходу; 3) уроками, отриманими українцями, та зміцненням стійкості мережі, що дозволило країні запобігти масовим відключенням електроенергії.

Кілька міжнародних організацій, включаючи Світовий банк, підрахували грошові збитки, завдані Україні. Найбільше пошкоджень зазнали потужності з

виробництва електроенергії, мережі передачі та розподілу, а також нафтосховища. Газова інфраструктура також зазнала значних пошкоджень, але їх складніше виміряти, оскільки Україна не надає інформації про стан своїх газовидобувних потужностей. Однак, згідно з оцінкою Міжнародної хартії енергетики, російські війська контролюють 15% запасів природного газу України та щонайменше 150 газовидобувних об'єктів. Більшість із них не працювали в Харківській області через триваючі бойові дії в цьому регіоні. Український експерт з питань енергетики під час інтерв'ю заявив, що одна з українських компаній газового сектору вже зазнала збитків майну на суму 1 мільярд доларів США [310].

Згідно з оцінкою Світового банку, збитки, завдані газовому сектору (без урахування видобутку газу), склали 1,3 млрд доларів США. Тим часом найбільших збитків зазнав сектор електроенергетики – 7,5 млрд доларів США. Російські війська найбільше атакували потужності з виробництва та передачі електроенергії, тому розподільча мережа постраждала найменше. Постраждали вугільні та газові електростанції, зруйновані підстанції мережі передачі, а також підприємства з виробництва відновлюваних ресурсів (тобто вітрової та сонячної енергетики, а також зруйнована гребля Нова Каховка).

Збитки, завдані енергетичній інфраструктурі регіонів України в млрд доларів США (з 24.02.2022 по 31.12.2023), представлені на рис. 4.1. Згідно із загальною оцінкою у дослідженні Світового банку, Україна зазнала збитків енергетичній інфраструктурі (без урахування мереж теплопостачання) на суму 10,6 млрд доларів США. Додатково оцінюється, що через війну та її наслідки електроенергетика, видобуток газу, транспортування газу, видобуток вугілля, паливно-нафтовий сектори в Україні втратили доходи на суму 54 млрд доларів США. 47 млрд доларів США знадобиться протягом наступних 10 років для реконструкції енергетичної інфраструктури відповідно до принципу «Build Back Better», з яких 40 млрд доларів США знадобиться для відновлення генеруючих потужностей [310].

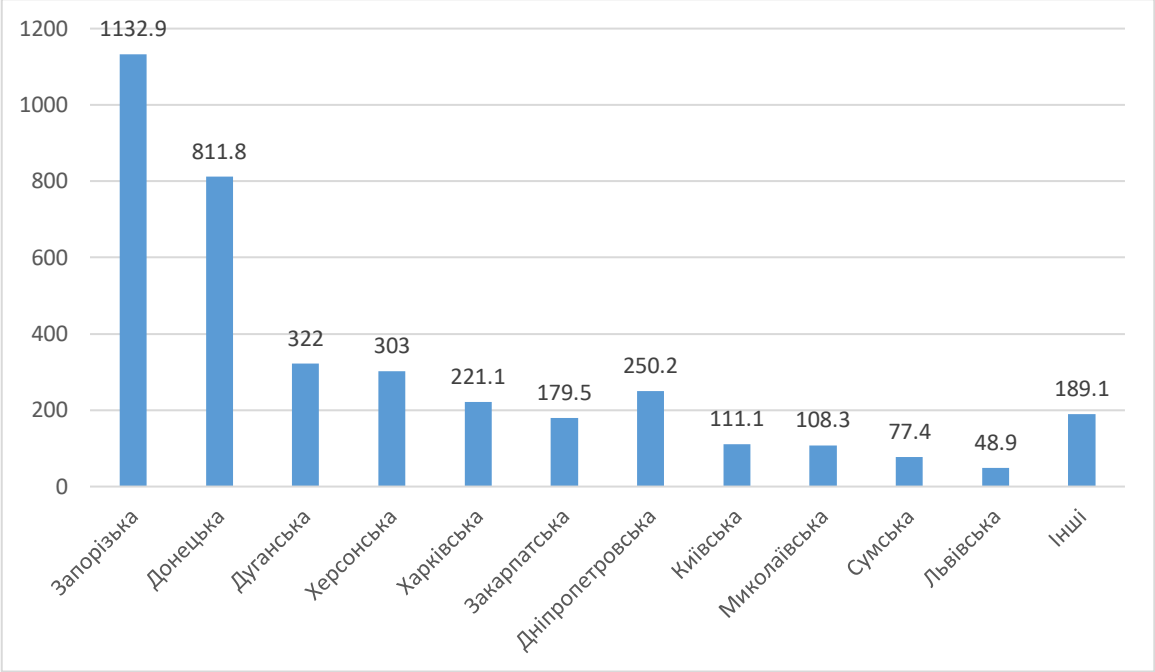


Рис. 4.1. Збитки, завдані енергетичній інфраструктурі регіонів України, у мільярдах доларів США (з 24.02.2022 по 31.12.2023)*

*Джерело: сформовано автором на основі [310]

Згідно розрахунків, представлених Київською школою економіки у співпраці з Міністерством розвитку громад та територій, розмір прямих збитків, завданих українській енергетиці, складає $14,6 млрд. Під час оцінювання збитків у сфері енергетики використовували як прямі, так і непрямі методи визначення вартості втрачених і пошкоджених об'єктів. Вартість пошкоджених об’єктів взята на основі первісної балансової вартості основних засобів, вартості поточних ремонтів, вартості відновлення (ринкова вартість заміщення зруйнованого). Ключова інформація щодо втрат у секторі енергетики надана військовими адміністраціями, Міністерством розвитку громад і територій та Міністерством енергетики. Для оцінки збитків на окремих великих об'єктах використовується індивідуальний підхід, базований на даних із відкритих джерел, а також на інформації від власників і керівників підприємств та центральних органів виконавчої влади. При цьому збір даних про збитки об'єктів електрогенерації відбувався в узагальненій формі, враховуючи високий ризик поширення чутливої інформації про детальні пошкодження об'єктів критичної інфраструктури.

Сектор виробництва та передачі електроенергії найбільше постраждав від військової агресії. У період з жовтня 2022 року до лютого 2023 року відбувалися цілеспрямовані та масштабні атаки на енергетичні об'єкти. У прифронтових регіонах продовжувалися регулярні та точкові обстріли енергетичної інфраструктури. За оцінками, загальні збитки для цих об'єктів перевищують 12 мільярдів доларів. В цілому, з початку вторгнення були уражені всі ТЕС, ГЕС та 20 теплоелектроцентралей (ТЕЦ), що знаходяться під контролем України.

Значні збитки спостерігаються у великих електрогенераційних об'єктах. Під час опалювального сезону 2022-2023 років, внаслідок одного з масованих обстрілів, було пошкоджено дев'ять блоків теплових електростанцій, а один з них зазнав повного знищення через пряме влучення ракети. Як вже згадувалося, на початку червня 2023 року Каховська ГЕС була повністю зруйнована, що призвело до прямих збитків у розмірі 586 мільйонів доларів.

З березня 2024 року масовані атаки, здійснені РФ, призвели до серйозних пошкоджень енергетичної генерації. Усі теплоелектростанції на підконтрольних територіях, що належать до групи оператора електростанцій ДТЕК, зазнали обстрілів. Зокрема, виведено з ладу енергоблоки Ладижинської та Бурштинської ТЕС потужністю понад 4 ГВт. Об’єкти в Харківській області зазнали значних руйнувань — Харківська ТЕЦ-5 та Зміївська ТЕС, що входять до складу «Центренерго», майже повністю знищені. Також у Київській області величезних пошкоджень зазнала Трипільська ТЕС, яка фактично перестала існувати.

Оцінка прямих поточних збитків теплової електрогенерації складає $3,8 млрд (ТЕС) та $1,6 млрд (ТЕЦ), гідроелектростанцій (ГЕС) та гідроакумулювальних електростанцій (ГАЕС) – $2,5 млрд. [2]. В той же час, з причин очевидного фізичного зносу та технологічної застарілості обладнання що було пошкоджено або знищено, вартість відновлення втрачених потужностей таких електростанцій може суттєво перевищувати оцінку збитків. Виробники альтернативної електроенергії також зазнають суттєвих збитків. Згідно з даними Секретаріату Енергетичної Хартії, 13% потужностей сонячної генерації розташовані на окупованих територіях, з яких 8% були пошкоджені або знищені. Приблизно 80% вітрових електростанцій також опинилися під контролем

окупантів, а частина з них постраждала від обстрілів. Щодо біоенергетичних потужностей, 2% знаходяться на окупованих територіях, і принаймні 4 біогазові заводи зазнали руйнувань. Прямі збитки для виробників електроенергії з відновлюваних джерел (за винятком великих гідроелектростанцій та гідроакумулюючих електростанцій) оцінюються в $281 млн.

Спостерігється також пошкодження і знищення об'єктів передачі та розподілу електроенергії. Згідно з попередніми оцінками, сума прямих збитків, завданих Оператору системи передачі електроенергії внаслідок повномасштабного вторгнення, становить приблизно 2,2 мільярда доларів, тоді як компаніям-операторам систем розподілу – близько 826 мільйонів доларів.

Також, в результаті бойових дій та масованих повітряних атак, 925 котельні було повністю зруйновано або частково пошкоджено, з них найбільше - у Харківській, Чернігівській, Київській, Донецькій та Миколаївській областях; 214 центральних теплових пунктів частково пошкоджено або повністю зруйновано, окрім того повного руйнування зазнали понад 354 погонних кілометри теплових мереж. В таблиці 4.2 представлено оцінку прямих втрат енергетики (розрахунки станом на листопад 2024 р.).

Таблиця 4.2.

Оцінка прямих втрат в секторі енергетики (розрахунки станом на листопад 2024 р.)*

Види втрат	Оцінка втрат, млрд дол. США
Електроенергетика, зокрема:	12,1
Генерація електроенергії	9,0
Передача електроенергії	2,2
Розподіл електроенергії	0,8
Нафтогазовий сектор, зокрема:	1,2
Транспортування газу	0,8
Розподіл газу	0,2
Зберігання нафти та нафтопродуктів	0,3
Вугледобувна промисловість	0,4
Теплопостачання	1,0
Всього	14,6

*Джерело сформовано автором на основі: [2]

Загальна сума прямих збитків завданих нерухомості, іншій інфраструктурі, транспортним засобам та запасам склала з початку вторгнення майже $170 млрд.

У порівнянні з попередньою оцінкою, станом на початок 2024 року, збільшення суми складає $12,6 млрд. (8%) [2]. Найбільша частка у загальному обсязі прямих збитків завдана житловим будівлям ($60,0 млрд) та транспортній інфраструктурі ($38,5 млрд). Розмір втрат сектору енергетики - $14,6 млрд, активів промисловості, послуг та будівництва - $14,4 млрд. Окрім того, прямі втрати аграрного сектору та земельних ресурсів внаслідок військових дій складають ще $10,3 млрд. Розмір сукупних прямих збитків від руйнувань та пошкоджень об'єктів громадського сектору (заклади освіти та науки, охорони здоров'я, соціальні об'єкти та установи, культурні споруди, спортивні об'єкти, адміністративні будівлі) складають близько $16,3 млрд. [2]. В таблиці 4.2 представлено загальну оцінку прямих збитків інфраструктури станом на листопад 2024 року. Встановлено, що найбільшого ураження зазнали енергетична, транспортна, житлово-комунальна та телекомунікаційна інфраструктура, що призвело до системних порушень функціонування базових життєзабезпечувальних систем держави. Доведено, що ключовим об'єктом цілеспрямованих атак стала енергетична система України, включаючи об'єкти генерації, передачі та розподілу електроенергії, а також нафтогазову та теплопостачальну інфраструктуру. Сукупні прямі втрати енергетичного сектору оцінено на рівні 14,6 млрд дол. США (2024р.) та 18,3 млрд дол. США (2026р.), тоді як загальний обсяг прямих втрат критичної інфраструктури перевищує 169 млрд дол. США (2024 р.), із найбільшою часткою у житловому та транспортному секторах. Просторовий розподіл втрат свідчить про їх концентрацію у прифронтових та окупованих регіонах. Найбільш критичні пошкодження зафіксовано в дорожній інфраструктурі, енергетичних об'єктах генерації та мережах електропостачання (табл. 4.3.).

Найбільше зростання збитків в абсолютному виразі спостерігається саме в енергетиці (+$4,6 млрд). Також фіксуються великі збитки в транспортній інфраструктурі, соціальних секторах, а також в активах підприємств. У відносному вимірі найбільша динаміка характерна для адміністративних будівель (+60%), а також для енергетики (+46%), охорони здоров'я (+32%), та культури/туризму/спорту (+29%).

Таблиця 4.3

Загальна оцінка прямих збитків, завданих інфраструктурі, станом на листопад 2024 р. та станом на лютий 2026 р.*

Тип майна	Оцінка прямих втрат станом на листопад 2024 р., $ млрд	Частка, %	Оцінка прямих втрат станом на лютий 2026 р., $ млрд	Частка, %	Динаміка, %
Житлові будівлі	60,0	35,3	65,9	33,4	+9,8
Інфраструктура	38,5	22,7	42,0	21,3	+9,1
Енергетика	14,6	8,6	18,3	9,3	+25,3
Активи підприємств, промисловість	14,4	8,5	18,4	9,3	+27,8
АПК та земельні ресурси	10,3	6,1	12,1	6,1	+17,5
Освіта	7,3	4,3	12,2	6,2	+67,1
Лісовий фонд	4,5	2,7	…	…	…
Охорона здоров’я	4,3	2,5	4,5	2,3	+4,7
Культура, туризм, спорт	4,0	2,3	4,5	2,3	+12,5
ЖКГ	3,5	2,0	3,8	1,9	+8,6
Транспортні засоби	3,5	2,0	…	…	…
Торгівля	2,8	1,7	…	…	…
Цифрова інфраструктура	1,2	0,7	1,8	0,9	+50,0
Адміністративні будівлі	0,8	0,4	…	…	…
Соціальна сфера	0,2	0,1	…	…	…
Разом	169,8	100	197,5	100	+16,3

*Джерело: сформовано автором на основі: [2]

В цифровій інфраструктурі зростання мало ще більшу динаміку. Що стосується географічного розподілу збитків, найбільшою мірою постраждали прифронтові регіони. На десять областей, які були окуповані і мають спільний кордон з РФ або вихід до моря, припадає більше ніж 90% загальної суми прямих збитків. Однак удари по активах продовжуються і в інших областях, зокрема серед сильно постраждалих регіонів — також Дніпропетровська область. На рис. 4.2 представлено карту розподілу прямих втрат за областями, $ млрд. [2].

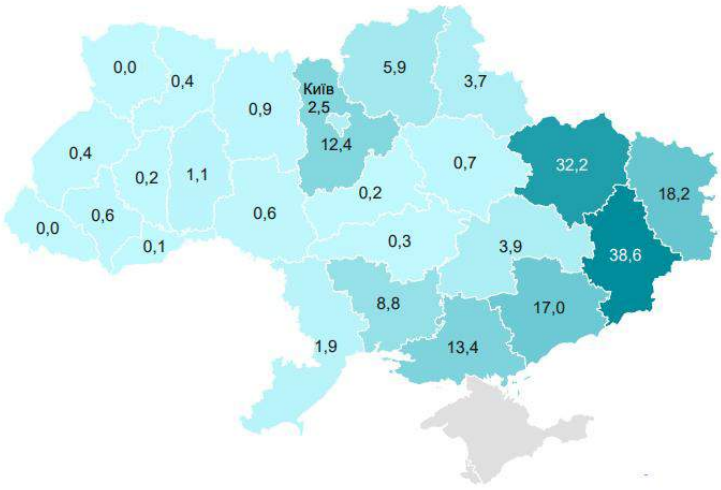


Рис. 4.2. Розподіл прямих втрат за областями, $ млрд у 2024 р.*

*Джерело: сформовано автором на основі: [2]

Серед усіх інфраструктурних об'єктів країни, найменше пошкоджень і руйнувань зафіксовано серед соціальних установ. Пошкоджені заклади соціального захисту знаходяться в Києві та областях: Донецькій, Херсонській, Сумській, Київській, Житомирській, Харківській, Дніпропетровській, Закарпатській, Запорізькій, Миколаївській, Одеській, і Чернігівській. Зруйновані об'єкти соціальної сфери виявлено в Донецькій, Луганській, Дніпропетровській, Запорізькій, Київській, Миколаївській, Сумській, Харківській, Херсонській і Чернігівській областях, а також у Києві.

Що стосується об’єктів транспортної інфраструктури, загальна величина прямих збитків склала $38,5 млрд. Також, у перші тижні війни, масованих обстрілів з боку російських військ зазнала авіаційна інфраструктура, передусім аеродроми, причому не лише військового, але й цивільного і військово-цивільного (подвійного) призначення. Пізніше об’єкти залізничної інфраструктури, зокрема електричні підстанції, стали головними цілями активних атак. Однак найбільших руйнувань як за масштабами, так і за вартісними показниками зазнала дорожня інфраструктура. Це пояснюється не лише тим, що в умовах воєнних дій дороги природно піддаються артилерійським обстрілам, а й тим, що російські танки значною мірою використовували українські дороги для пересування. Автомобільні шляхи слугували лініями

комунікацій між російськими військовими угрупованнями на території України та їхнім тилом у Росії та Білорусі. У таблиці 4.4 наведено оцінку прямих втрат транспортної інфраструктури, проведену Київською школою економіки у співпраці з Міністерством розвитку громад і територій.

Таблиця 4.4.

Оцінка прямих втрат транспортної інфраструктури у 2024 р.*

Види втрат	Одиниці виміру	Первісна кількість	Зруйновано/ пошкоджено	Оцінка втрат, $ млрд
Автомобільні дороги державного значення	км	47 000	9 298	9,9
Автомобільні дороги місцевого значення	км	120 000	9 056	9,6
Комунальні дороги (міст та ін. насел. пунктів)	км	270 000	8 277	8,8
Мости та мостові переходи	од.	11 076	344	2,6
Активи УЗ	X	X	X	4,5
Інфраструктура морських та річкових портів	X	X	X	1,0
Авіаційна галузь	од.	36	20	2,0
Майно поштових операторів	X	X	X	0,01
Всього	X	X	X	38,5

*Джерело: сформовано автором на основі: [2]

Руйнування зафіксовано на понад 26 тисячах кілометрів доріг та 344 мостах і мостових переходах державного, місцевого чи комунального значення. Перевірка стану дорожньої інфраструктури у деокупованих регіонах (Чернігівська, Київська, Сумська, Харківська області) підтвердила очікувані значні пошкодження, спричинені проходженням танків і важкої військової техніки. Це вказує на необхідність масштабної реконструкції пошкоджених доріг. Попередні оцінки свідчать, що рівень руйнувань сягає 95%, що в середньому становить близько 10% від загальної протяжності доріг у регіонах, які перебували під окупацією військ РФ або де велися чи тривають бойові дії.

З моменту вторгнення залізниця стала важливою частиною критичної інфраструктури, виконуючи ключову роль у безкоштовній евакуації мільйонів українських громадян і компаній із зон бойових дій. Крім того, вона забезпечувала перевезення життєво важливих матеріалів та обладнання в ці регіони. Природно, з огляду на цю роль, залізниця стала об'єктом для російських

обстрілів. Прямі збитки в цьому секторі оцінили у 4,3 мільярда доларів. Значні пошкодження зазнали залізничні полотна, вокзали та станції як на підконтрольних, так і на окупованих територіях. Більше 700 км залізничних колій перебувають на тимчасово окупованих територіях після 24 лютого 2024 року. Зруйновано або втрачено близько 10 тисяч будівель. Крім того, є підстави вважати повністю втраченим все рухоме майно Укрзалізниці, яке не встигли вивезти з цих територій, оскільки воно або знищене, або викрадене силами країни-агресора.

Оцінка прямих втрат в авіаційній галузі, яка охоплює аеропорти, аеродроми, авіаційну техніку та аеронавігаційне обладнання, становить близько 2 мільярдів доларів. З початком бойових дій російські війська активізували ракетні обстріли всіх основних аеродромів України, намагаючись знищити її можливості для забезпечення протиповітряної оборони. Внаслідок цих атак було пошкоджено 19 з 35 аеродромів, серед яких 12 цивільних та 7 аеродромів подвійного призначення (не враховуючи військові). Деякі з аеродромів зазнали повторних обстрілів.

Прямі збитки інфраструктури портів та пов'язаних з ними підприємств оцінюються в 0,85 мільярда доларів. Ця оцінка включає як інфраструктуру морських портів, так і об'єкти внутрішнього водного транспорту, які постраждали внаслідок війни. До загальних збитків також враховані втрати, завдані портовій інфраструктурі через аварію на Каховській ГЕС.

Після припинення дії зернового коридору, узгодженого з Росією, у період із липня по жовтень 2024 року лише в портах Одеської області було зафіксовано майже 60 нападів з боку ворога. Унаслідок цих атак пошкоджень і руйнувань зазнали майже 300 об’єктів інфраструктури, 177 транспортних засобів та 22 цивільні судна. Як зазначає Міністерство аграрної політики та продовольства, лише жовтневі обстріли портів спричинили збитки, що сягнули 30-40 мільйонів доларів. Уряд звинувачує ці дії у свідомому тероризмі з метою підриву експортного потенціалу України.

Прямі збитки, нанесені комунальним підприємствам та приватним перевізникам через зруйнований транспорт, становлять 830 мільйонів доларів.

Серед пошкодженого майна - тролейбуси, трамваї, автобуси. Оцінка втрат комунального транспорту проводилася як методами розрахунків на основі припущень, так і за допомогою аналізу точних даних про пошкоджене або зруйноване майно, які надали військові адміністрації.

Найбільше шкоди комунальному майну, зокрема й громадському транспорту, було завдано в Луганській та Донецькій областях, а також в Харкові. У результаті ударів важкого озброєння по цивільній інфраструктурі, ворог знищив близько 60% громадського транспорту на Донеччині та понад 70% – на Луганщині. У цих регіонах сфера надання послуг міського та приміського пасажирського транспорту фактично припинила своє існування. Найбільше втрат зазнали і власники приватних автомобілів, адже в цих східних областях багатьом громадянам їх довелося втратити.

Прямі збитки об’єктів водопостачання, водовідведення та сфер поводження з побутовими відходами сягають 3,5 мільярдів доларів. Житлово-комунальна інфраструктура регулярно піддавалася ракетним і артилерійським ударам Росії. Постійні обстріли та бойові дії ускладнювали або взагалі унеможливлювали ремонтні роботи, що спричинило тривалі відключення систем водопостачання. У деяких населених пунктах доступ громадян до житлово-комунальних послуг та питної води залишався обмеженим протягом тривалого часу, а подекуди ця проблема досі актуальна. Зокрема, через пошкодження водогону більшість районів Миколаєва довгий час залишалися без централізованого водопостачання. Тільки в листопаді 2022 року після звільнення Херсона вдалося частково відновити водогін. До цього у місті була доступна лише технічна вода, а питну доводилося доставляти з інших регіонів у пляшках. Крім того, значних руйнувань зазнала житлово-комунальна сфера міст, що перебувають під інтенсивними артилерійськими ударами. Оцінку прямих втрат житлово-комунального господарства представлено в таблиці 4.5.

Таблиця 4.5

Оцінка прямих втрат житлово-комунального господарства у 2024 р.*

Показники	Одиниці виміру	Первісна кількість	Зруйновано	Пошкоджено	Оцінка втрат, млрд дол. США
Водопровідні очисні споруди	од.	400	7	18	0,36
Каналізаційні очисні споруди	од.	967	23	28	1,03
Водопровідні насосні станції	од.	5 646	109	73	0,24
Каналізаційні насосні станції	од.	2 908	63	120	0,35
Водопровідні мережі	м пог.	98 076 470	1 947 026	0	0,54
Каналізаційні мережі	м пог.	37 053 200	582 863	0	0,75
Свердловин	од.	22 134	125	34	0,02
Лабораторії	од.	н.д.	4	2	0,001
Резервуари чистої води	од.	2 129	33	4	0,04
Водонапірні башти	од.	695	101	38	0,02
Контейнери для збирання побутових відходів	од.	н.д.	23 145	0	0,02
Сміттєвози	од.	3 669	222	0	0,05
Полігони для захоронення побутових відходів	од.	5 969	12	21	0,07
Сміттєсортувальні лінії	од.	34	3	2	0,01
Контейнерні майданчики	од.	н.д.	813	97	0,001
Біогазові установки	од.	21	3	0	0,01
Всього	X	X	X	X	3,47

*Джерело: сформовано автором на основі: [2]

Отже, загальний стан об'єктів критичної інфраструктури в Україні на цьому етапі воєнного протистояння вказує на потребу в терміновому відновленні та модернізації. Він також підкреслює важливість ефективної взаємодії національних і міжнародних структур для забезпечення сталого розвитку держави.

4.2. Ефективність публічного управління об'єктами критичної інфраструктури в Україні

Досягнення ефективності публічного управління об'єктами критичної інфраструктури в Україні є критично важливою для стабільності та безпеки

держави, особливо в умовах воєнного стану. Україна поступово розвиває систему управління критичною інфраструктурою, впроваджує реєстри та механізми захисту, але залишаються виклики, пов'язані з координацією дій, фінансуванням та кадровим забезпеченням. Ці виклики включають неефективне витрачання коштів, затримки з прийняттям рішень та відсутність координації, особливо в контексті триваючого воєнного конфлікту та необхідності реконструкції. Ситуація ще більше ускладнюється необхідністю адаптації до нових загроз безпеці та процесу децентралізації, що триває.

В цілому, проблематиці захисту критичної інфраструктури присвячено низку наукових праць вітчизняних авторів. Однією з основоположних наукових праць із проблематики забезпечення стійкості критичної інфраструктури є робота Д. Бобро [9]. Вчений систематизує загрози критичній інфраструктурі, визначає критерії її оцінювання. У статті Б. Богдана [10] йдеться про законодавче забезпечення формування системи захисту критичної інфраструктури в Україні.

У роботах Л. Мельничука [59], окрім аналізу методологічної складової моделювання процесів управління критичною інфраструктурою, запропоновано оригінальну модель системи управління критичною інфраструктурою на рівні регіону та схема її впровадження.

О. Суходоля та інші співробітники Національного інституту стратегічних досліджень [22] розглядають питання захисту критичної інфраструктури з точки зору забезпечення національної безпеки країни. В. О. Євсєєв [27] розглядає еволюційний аспект нормативно-правового забезпечення публічного управління у сфері захисту критичної інфраструктури. Однак фактично весь масив згаданих публікацій має суто описовий та декларативний характер, що викликає здивування з огляду на ситуацію війни та вкрай високих ризиків для критичної інфраструктури країни, тобто очевидної необхідності зосередження зусиль відповідних науковців на практичних питаннях захисту цієї інфраструктури.

Між тим, навіть до 2014 року, тобто ще до початку навіть гібрідної агресії з боку рф, було опубліковано грунтовну працю Д. С. Бірюкова та С. І. Кондратова «Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні» [7]. Автори згадують, що з-поміж пріоритетних напрямів підготовки

держави до збройного захисту національних інтересів у новій редакції Воєнної доктрини України (ст. 23) вказується «розвиток інфраструктури регіонів з урахуванням потреб підготовки території держави до оборони». На жаль, цей важливий елемент доктрини не був врахований ані в деталізованих документах (планах і т.п.), ані в діяльності з захисту критичної інфраструктури держави за весь період з 2014 року – диференціація регіонів за ступенем безпекової ситуації та ризиків не здійснювалась по відношенню до систем та об'єктів критичної інфраструктури. І це є саме одним з наслідків непродуманої системи показників ефективності, побудованої на базі наявного та перспективного (тобто такого що розглядається в динаміці) диференційованого середовища функціонування критичної інфраструктури.

Ще один можливий спосіб – це розробка альтернативних форм оцінки ефективності та бенчмаркінгу. Бенчмаркінг є відносно новим для державного сектору, оскільки був розроблений для використання в приватному секторі в 1970-х роках, але зараз широко поширений, особливо серед корпоратизованих установ, де його легше розділити на частини та виміряти. Значна частина цієї оцінки ефективності здійснюється «технократами» в кількох високоцентралізованих установах на Півночі, таких як Міжнародна організація зі стандартизації (ISO) [274; 296]. Стандартизовані вимірювання ефективності, спрямовані на підвищення прозорості та підзвітності шляхом забезпечення більшої доступності даних про ефективність для широкої громадськості, розробили спільні підходи до комунікації та систему оцінювання, які теоретично можна використовувати в будь-якій точці світу.

Критики стверджують, що ці схеми вимірювання призводять до зниження прозорості, враховуючи, що вони, як правило, проводяться «експертами» за зачиненими дверима та маніпулюються менеджерами та політиками, які хочуть «виробити правду» способами, які можуть бути відірвані від реалій на місцях [133]. Фактично, саме ця ситуація спостерігається в управлінні об'єктами критичної інфраструктури в Україні, тобто діяльності підприємств критичної інфраструктури таких як Укренерго [156].

Хоча інфраструктурні проекти в державному секторі стикаються з ризиками, що виникають протягом усього життєвого циклу, неефективне визначення ризиків та їх джерел протягом усього життєвого циклу проекту може призвести до низьких показників ефективності проектів та може призвести до можливих збоїв. Оцінка ризиків протягом усього життєвого циклу проекту може бути ефективним методом зробити його більш стійким і, як наслідок, більш прибутковим для всіх зацікавлених сторін.

Ще однією сферою, на яку варто звернути увагу, є можливість проведення належної перевірки (due diligence) підприємств критичної інфраструктури. У зарубіжній практиці дью дилідженс для державних підприємств – це підхід, що базується на оцінці ризиків, «без несподіванок», гнучкий та спритний. Застосування цього підходу для українських проектів критичної інфраструктури видається дуже доцільним. Гнучкість процесів та елементів due diligence дозволяє включити безпековий компонент та фактори диференціації регіонів України за рівнем поточної та прогнозованої безпеки/небезпеки, для визначення ступеню ефективності та прозорості функціонування об’єкту інфраструктури за цим показником. Відкритим, однак, залишається питання про суб’єкта виконання due dilligence. Найбільш доцільним видається поєднання зусиль державних регуляторів, незалежних антикорупційних органів, та залучення іноземних агенцій що надають послуги due dilligence у державному секторі.

Наявні методики оцінювання ефективності публічного управління критичною інфраструктурою (Ek) здебільшого мають один із двох недоліків. Одні зосереджуються лише на кінцевих результатах, як-от тривалість перебоїв чи обсяг втрат, і не пояснюють, чому ці результати саме такі. Інші оцінюють наявність нормативних актів, планів і структур, але не показують, наскільки вони реально працюють у кризовій ситуації. Крім того, ефективність зазвичай оцінюють «загалом», без розмежування рівнів управління. Через це важко зрозуміти, де саме виникають збої: в ухваленні рішень на національному рівні, у координації в регіоні чи у спроможності самого оператора об'єкта. Запропонований підхід поєднує три групи індикаторів (результативні, процесні та інституційні) і розглядає кожну з них окремо на трьох рівнях управління:

національному, регіональному та об'єктовому. Такий розподіл дає змогу не лише отримати загальну оцінку, а й визначити, які саме управлінські компоненти найбільше впливають на кінцевий результат.

Пропонуємо визначення трьох груп індикаторів для оцінювання ефективності публічного управління критичною інфраструктурою (див. табл. 4.6.):

Група І. *Індикатори результату* (об’єктивні). Ефективність роботи об’єктів, швидкість відновлення.

Група ІІ. *Індикатори процесу* (суб’єктивні). Демонструють як швидко приймаються рішень, наскільки ці рішення є злагодженими, чи забезпечується виконання плану заходів.

Група ІІІ. *Індикатори інституційного розвитку* (суб’єктивні). Характеризують повноту та ефективність правового забезпечення, організована діяльність інституцій публічного управління, налагодження механізмів взаємодії.

Етапи застосування методичного підходу:

Етап І. Формування переліку індикаторів для конкретного сектору КІ та рівнів управління.

Етап ІІ. Збирання вихідних даних від операторів КІ, органів влади, ДСНС України, звітів про виконання планів і програм.

Етап ІІІ. Нормування показників. Пропонуємо здійснювати за нормативними значеннями.

Етап IV. Визначення вагових коефіцієнтів. Пропонуємо визначення вагових коефіцієнтів на користь результативних показників, проте рівномірно.

Етап V. Розрахунок групових, рівневих та інтегрального показників.

Етап VI. Аналіз виявлених проблем «вузьких місць» та можливостей. Формування карти управлінських рішень на основі аналізу.

На нашу думку, елементами зважування усіх цих показників доцільно обрати нормативне зважування. Якщо для показника встановлено цільове значення (норматив, стандарт ЄС, показник довоєнного періоду), замість мінімуму й максимуму використовують відношення фактичного значення до

цільового за формулою, якщо показник демонструє позитивність тенденції (формула 4.3) та негативної тенденції(формула 4.4.):

Таблиця 4.6.

Система індикаторів оцінювання ефективності публічного управління критичною інфраструктурою*

№пп	Рівень	*Індикатори результату R*	*Індикатори процесу P*	*Індикатори інституційного розвитку Iir*
1	**Держава**	Тривалість безперебійного надання послуг об'єктами КІ; Загальний час, необхідний на відновлення функціонування об'єктів КІ; фінансові та економічні втрати від збоїв КІ	Швидкість реакції під час НС; виконання заходів та досягнення цілей стратегічних планів держави	Наявність потрібного і повного правового забезпечення для роботи; злагоджені механізми взаємовідносин органів влади; ефективні управлінські рішення, достатність фінансових ресурсів для функціонування КІ
2	**Регіон**	Частка населення та підприємств, які користуються послугами КІ; Загальний час відновлення роботи КІ; кількість населення та територій, де простежуються перебої	Швидкість реакції під час НС на регіональному рівні; кількість злагоджень та тренувань для фахівців, що забезпечують функціонування КІ	Робота координаційних регіональних структур в разі надзвичайних ситуацій; повнота інструкцій та положень для роботи; наявність матеріалів та обладнання; наявна потрібна кількість кадрів
3	**Об'єкт КІ**	Частка відновленої функції за нормативний строк	Час від виникнення до локалізації НС; дотримання розроблених раніше процедур реагування	Наявність резервних систем функціонування, розроблений план дій у разі надзвичайної ситуації

*Джерело: власна розробка автора

$$Xnorm = \frac{Xi}{X\,n} \tag{4.3}$$

$$Xnorm = \frac{X\,n}{X\,i} \tag{4.4}$$

де, Xi – значення показника; Xn - визначене експертами нормативне значення; Xnorm – нормований показник.

Розрахунок здійснюється послідовно від мікро рівня до макро рівня (об'єкт КІ, регіон, держава). Насамперед, визначають оцінку кожної групи індикаторів на кожному рівні (формула 4.5):

$$Ig = \Sigma Vi * Xnormi \quad (4.5)$$

де, Ig - зведений індикатор групи; Xnormi – нормований індикатор, Vi – коефіцієнт вагомості індикатора в рамках групи

Далі визначають ефективність на кожному рівні (формула 4.6):

$$IL = \Sigma Fi * Igi$$

де. IL – індекс ефективності рівня; Fi – вагомість груп індикаторів рівня; Igi – зведений індикатор групи.

Після цього розраховують інтегральний показник ефективності:

$$IIEFCI = \Sigma Fi * IL \quad (4.6)$$

де, IIEFCI – інтегральний коефіцієнт ефективності публічного управління критичною інфраструктурою.

Виділяємо такі рівні ефективності:

Рівень I. Дуже висока ефективність (IIEFCI 0,9-1,00)

Рівень II. Висока ефективність (IIEFCI 0,8-0,9)

Рівень III. Достатня ефективність (IIEFCI 0,7-0,8)

Рівень IV. Середня ефективність (IIEFCI 0,5-0,7)

Рівень V. Низька ефективність (IIEFCI 0,3-0,5)

Рівень VI. Дуже низька ефективність (IIEFCI 0,3-0,5)

При цьому, окремо можна визначити внесок кожного показника у загальний результат ефективності та прийняти управлінські рішення:

$$Part = \frac{Vi\ Fi\ Ig}{IIEFCI\ 100\%} \quad (4.7)$$

Можна також визначити невикористані резерви показників

$$Res = Vi\ Fi\ (1 - Ig) \quad (4.8)$$

Кожен з індикаторів можна проградувати, і ті індикатори, які матимуть найвищі значення Res є найбільш проблемними і такими, що потребують

негайного реагування. Їх зростання дасть змогу суттєво підвищити загальний індикатор ефективності.

Важливим елементом підвищення ефективності -є корпоратизація об'єктів КІ. Корпоратизація державних підприємств критичної інфраструктури, коли державними послугами керує державна корпорація, може призвести до різних ризиків, зокрема потенційних конфліктів інтересів, зниження прозорості та підзвітності, а також збільшення витрат. Хоча це спрямовано на підвищення ефективності та залучення приватних інвестицій, це також може призвести до зосередження уваги на прибутках, а не на державних послугах, що потенційно може завдати шкоди вразливим верствам населення та зменшити демократичний контроль [265].

З аналізу світового досвіду вважається, що корпоратизація знижує ризики політично мотивованих інвестицій, сприяє максимально ефективному використанню існуючих активів, і навіть розвитку нової інфраструктури з урахуванням комерційно обґрунтованих критеріїв. Проте насправді корпоратизація характеризується низкою «підводних камінів», що необхідно враховувати з урахуванням національної і навіть регіональної специфіки.

Уряди всього світу дедалі частіше звертаються до використання окремих державних корпорацій для надання основних послуг. Ці «корпоратизовані» структури повністю належать та управляються державою, але функціонують на незалежній основі з різним ступенем автономії. Поширеними прикладами є водо- та електропостачання, але ця практика поширюється на набагато ширший спектр товарів та послуг, включаючи аеропорти, догляд за дітьми, університети, ліси, лікарні, транспорт та виробництво [111].

З 1970-х років корпоратизація зазнала сильного впливу неоліберальної теорії та практики, що сприяло створенню комерціалізованої культури та ідеологій державного сектору, при цьому комунальні підприємства все частіше керуються на ринково-орієнтованих операційних принципах, таких як фінансово закріплені показники ефективності, ціноутворення, що рефлексує витрати, та конкурентний аутсорсинг [272].

Однак не всі корпоратизації були проведені з урахуванням цієї комерціалізації. Навіть у рамках ринкової економіки існують дуже різні мотиви. Деякі менеджери та політики розглядають корпоратизацію як перший крок до приватизації. Дехто розглядає її як можливість комерціалізувати послуги без політичних та економічних ризиків прямої участі приватного сектору. Інші віддані соціал-демократичним формам соціального забезпечення, тоді як інші все ще розглядають корпоратизацію як форму (автократичного) державного капіталізму. Загалом, як справедливо стверджує М. Макдональд [265], створення автономних державних сервісних установ не є ні історично специфічним, ні ідеологічно зумовленим, оскільки обґрунтування та функціонування таких державних підприємств разюче відрізнялися залежно від місця та часу. Їхньою єдиною спільною рисою є квазінезалежний склад професійних службовців, яким доручено керувати та виробляти окреслений набір товарів чи послуг, певною мірою захищений від прямого політичного втручання [265].

Закордонна практика показує, що корпоративне управління об’єктами громадської інфраструктури стикається також зі значними ризиками, включаючи фінансову нестабільність, збої в роботі та репутаційну шкоду. Ефективний менеджмент ризиків є надзвичайно важливим для забезпечення тривалого терміну стійкості і успіху цих проектів. Ключові зони ризику є наступними:

1. Фінансові ризики. Перевитрати бюджету, неадекватне фінансове планування та непередбачені витрати можуть призвести до фінансової нестабільності. Ризики доходів, такі як невизначені потоки доходів через коливання ринку або зміни цін, також можуть становити значні загрози.

2. Операційні ризики. Затримки та перевитрати коштів під час будівництва, низька якість виконання та перебої в роботі через непередбачені події можуть перешкоджати прогресу проекту та впливати на надання послуг.

3. Стратегічні ризики. Слабке інституційне планування, повільне затвердження проектів та нездатність адаптуватися до змін геополітичного ландшафту можуть підірвати загальні стратегічні цілі інфраструктурного проекту.

4. Ризики дотримання вимог та регулювання. Недотримання нормативних актів, екологічних стандартів та вимог безпеки може призвести до юридичних проблем, штрафів та репутаційної шкоди.

5. Репутаційні ризики. Громадське сприйняття неефективного управління, корупції або невиконання обіцянок може підірвати довіру громадськості та створити проблеми для майбутніх проектів.

6. Політичні та соціальні ризики. Зміни в урядовій політиці, соціальні заворушення та опір громади можуть вплинути на терміни та фінансування проектів.

До кінця 2000-х в Україні держкомпанії стикалися зі змінами в корпоративному управлінні, як правило, лише після того, як переставали бути державними та переходили до приватних рук. Так, стандарти корпоративного управління «Криворіжсталі» встановив новий власник підприємства - Mittal Steel. Приміром, ще під контролем держави завод «Криворіжсталь» не відрізнявся прозорістю в плані фінансової звітності. Першу звітність підприємство опублікувало вже після приватизації на початку 2008 р., що справило на інвесторів дуже сприятливе враження і дозволило компанії з легкістю пережити різке зростання цін на сировину, що відбулося на той час. У той час, як акції більшості металургійних компаній впали, акції «Криворіжсталі» продовжували зростати. Зі змінами в корпоративній галузі зіткнулися і колишні державні енергетичні підприємства, що увійшли до складу ДПЕК. За інформацією останньої, з кінця 2011 року бізнес-структура проводить організаційні зміни в системі управління. В рамках реформи було розпочато перехід від трирівневої до дворівневої моделі управління – шахтоуправління, що об'єднує кілька шахт, збагачувальні фабрики, електростанції та обленерго стали підпорядковуватися єдиному корпоративному центру ДПЕК. У той же час діяльність держкомпаній та їхнє корпоративне управління були і залишаються непрозорими, складно контрольованими та низькоефективними.

22 лютого 2024 року Верховна Рада ухвалила у другому читанні законопроєкт № 5593-д, який значно удосконалює систему корпоративного управління державних підприємств та приводить її відповідність до Керівних

принципів ОЕСР корпоративного управління державних підприємств, що підвищує суттєво ефективність системи публічного управління.

Зокрема, ключовими положеннями Закону є:

1. Встановлення виключної компетенції наглядових рад держпідприємств призначати та звільняти керівника, у тому числі і стосовно підприємств, що належать до сфери управління Кабінету Міністрів (таких як "Нафтогаз" та "Укрзалізниця"), а також затверджувати стратегічні та фінансові плани компанії.

Разом з тим, закон містить перехідні положення в цій частині. Зокрема, під час воєнного стану та протягом 12 місяців після його скасування, але не довше ніж три роки, Мінфін та Кабмін все ще будуть залучені до затвердження фінансових та стратегічних планів найважливіших держпідприємств. Так, фінансові, стратегічні та інвестиційні плани держпідприємств до 2025 року затверджуватимуться наглядовими радами, тоді як конкретні фінансові показники, включені до цих документів, а також листи очікування держпідприємств, потребуватимуть погодження з Міністерством фінансів та, в окремих випадках, з Кабінетом Міністрів.

2. Неможливість прийняття рішень суб’єктами управління з питань, що належать до виключної компетенції наглядової ради держпідприємства, у випадках відсутності призначеної наглядової ради (якщо створення наглядової ради передбачено згідно статуту) або відсутності правомочного складу наглядової ради.

3. Запровадження нового критерію незалежності членів наглядової ради для забезпечення їхньої фінансової незалежності. Такий критерій передбачає, що не може бути незалежним членом наглядової ради держпідприємства особа, якщо її винагорода за виконання функцій незалежного члена наглядової ради дежпідприємства є її єдиним або основним джерелом доходу.

4. Встановлення вичерпного переліку підстав для дострокового звільнення членів наглядової ради держпідприємства. Зокрема, це унеможливить довільне тлумачення щодо «неналежності роботи» наглядової ради з боку Кабміну та інших суб'єктів управління держпідприємствами (що є підставою для звільнення

членів наглядових рад); висновок щодо належності роботи наглядової ради буде встановлюватися з урахуванням результатів оцінки діяльності наглядової ради.

5. Встановлення процедури проведення оцінки діяльності наглядових рад держпідприємств, яка передбачає обов'язкове проведення такої оцінки не рідше одного разу на три роки. Закон також уповноважує Кабмін визначати порядок проведення таких оцінок шляхом прийняття відповідної постанови Кабміну, виходячи з вимог, встановлених законом. Зокрема, результати оцінки мають бути затверджені суб'єктами управління з урахуванням: а) висновку/звіту незалежного консультанта. Також мають бути встановлені критерії коли залучення незалежного консультанта для здійснення оцінки є обов'язковим; або б) самооцінки або пояснень наглядової ради.

Отже, нами запропоновано методичний підхід до оцінювання ефективності публічного управління критичною інфраструктурою: *Індикатори результату* (ефективність роботи об'єктів, швидкість відновлення); *Індикатори процесу* (демонструють як швидко приймаються рішень, наскільки ці рішення є злагодженими, чи забезпечується виконання плану заходів); *Індикатори інституційного розвитку* (характеризують повноту та ефективність правового забезпечення, організована діяльність інституцій публічного управління, налагодження механізмів взаємодії).

4.3. Стратегічні документи щодо відбудови об'єктів критичної інфраструктури України після війни

Україна розробила кілька стратегічних документів та рамкових програм для керівництва відновленням критичної інфраструктури після війни. Ці документи зосереджені на відновленні основних послуг, таких як енергетика, водопостачання та транспорт, а також соціальної інфраструктури, як-от школи та лікарні. До ключових стратегічних документів та ініціатив належать, зокрема, RDNA2 та RDNA3 (Швидка оцінка пошкоджень та потреб). Це комплексні документи, що окреслюють необхідність відновлення та реконструкції, особливо

критичної інфраструктури. Вони використовуються українською владою та міжнародними партнерами для координації зусиль з відновлення.

У рамках першої експрес-оцінки (RDNA1) акцент було зроблено на перші три місяці війни, з 24 лютого 2022 року по 1 червня 2022 року. За цей період загальні збитки оцінюються в 252 мільярди доларів США, а витрати на відновлення та реконструкцію протягом наступних 10 років становлять 348,5 мільярда доларів США. Найбільше постраждали сектори житлового будівництва (40% від загального обсягу завданої шкоди), транспорту (31%) та торгівлі й промисловості (10%). Найбільш ураженими регіонами з точки зору прямих збитків стали Донецька, Луганська та Харківська області, а також Київська, Чернігівська та Запорізька області.

За результатами другої експрес-оцінки (RDNA2), що охоплює період з 24 лютого 2022 року до 24 лютого 2023 року, загальні збитки сягають 289,1 мільярда доларів США. Для компенсації втрат і проведення реконструкції протягом десяти років необхідно 410,6 мільярда доларів. Згідно з оцінками RDNA2, пріоритетні заходи для відновлення та реконструкції у 2023 році потребують близько 14 мільярдів доларів, що становить приблизно 3,5 % від визначених загальних потреб. Найбільших втрат зазнали такі сектори, як житлове будівництво (38 % загальної шкоди), транспорт (26 %), енергетика (8 %), торгівля та промисловість (8 %), а також сільське господарство (6 %). Значних прямих збитків зафіксовано у Донецькій, Харківській, Луганській, Запорізькій, Київській та Херсонській областях.

Третя швидка оцінка завданої шкоди та потреб на відновлення (RDNA3) аналізує соціальні, інфраструктурні та виробничі сектори, оцінюючи вплив війни на економіку України в період з 24 лютого 2022 року по 31 грудня 2023 року. У цьому звіті враховано найактуальніші дані й висновки на основі попередніх напрацювань, щоб уникнути дублювання показників. У процесі оцінки збитків взято до уваги труднощі зі збиранням і аналізом інформації через складні умови воєнного часу, а також зроблено необхідні припущення.

Оцінка RDNA3 була розроблена спільно Світовим банком України, Кабінетом Міністрів України, службами Європейського Союзу та Організацією

Об'єднаних Націй за участю гуманітарних і міжнародних партнерів, представників наукових кіл, громадянського суспільства і приватного сектору. З боку Уряду України її проведення було організовано під керівництвом Міністерства розвитку громад, територій та інфраструктури за підтримки Офісу ProSteer цього міністерства, Офісу реформ Кабінету Міністрів та Київської школи економіки (KSE). До оцінки були залучені всі відповідні галузеві міністерства.

Незважаючи на триваючу війну, КМУ за підтримки партнерів докладає зусиль щодо якнайшвидшого відновлення та реабілітації разом із амбітною програмою реформ та модернізації відповідно до зусиль України щодо інтеграції до Європейського Союзу. У 2023 році уряд України виділив приблизно 7,2 мільярда доларів США на фінансування проектів невідкладного відновлення в енергетиці, критичній та соціальній інфраструктурі, житловому будівництві, гуманітарному розмінуванні та підтримці державного сектору. Так, у 2023 році відремонтовано 3836 житлових будинків та 19091 одноквартирних будинків; 448 шкіл, 237 дитячих садків, 390 медичних і соціальних закладів; а також завершено будівництво 9200 об’єктів критичної інфраструктури, 449 об’єктів теплопостачання, 221 об’єкт водопостачання та водовідведення. В Україні завершено аварійний ремонт більше 2 тисяч кілометрів автомобільних доріг, швидкісних та інших доріг державного значення. Відновлено 115 автомобільних мостів, близько 26 кілометрів залізничної інфраструктури та 46 залізничних мостів. Уряд впровадив ефективні інституційні механізми та розпочав реформи, спрямовані на поліпшення планування і реалізації процесів реконструкції та реабілітації. У рамках підготовки до вступу в ЄС країна розробляє масштабний пакет реформ, визначений у Плані для України, який інтегрується з Програмою підтримки України, запланованою Європейською Комісією.

RDNA3 дозволило Україні мати актуальний та глибокий аналіз втрат і потреб, що, у свою чергу, дає можливість правильного визначення пріоритетів, раціонального розподілу ресурсів та отримання очікуваних результатів. Висновки RDNA3 підтримають реалізацію програми Ukraine Facility,

затвердженої Європейським парламентом та Радою ЄС, яка передбачає виділення 50 мільярдів євро протягом наступного чотирьохрічного періоду.

Все більш важливим стає встановлення чітких пріоритетів для відновлення України, ефективна мобілізація та використання фінансування. Пріоритети відновлення та реконструкції на 2024 р., визначені галузевими міністерствами, складають 15 млрд дол. США.

Це потреби для термінових заходів з відновлення та відбудови на національному та місцевому рівнях, з особливим акцентом на підтримку і залучення приватного сектора, а також на відновлення житла, соціальної інфраструктури, послуг, енергетики та транспорту. В рамках RDNA3 було зазначено, що близько 5,5 млрд доларів США для цих потреб уже забезпечено завдяки міжнародним партнерам України та власним бюджетним коштам. Разом із тим, приблизно 9,5 млрд доларів США, що становить понад 60% від загального обсягу фінансування, наразі залишаються незабезпеченими. Найбільш значна нестача фінансування спостерігається у сферах енергетики, промисловості та послуг.

Україна визначила низку пріоритетних секторів для розвитку, серед яких оборонно-промисловий комплекс, будівництво, енергетика, цифрові технології, IT-сектор, аграрний сектор і природні ресурси. Уряд планує залучати іноземні інвестиції в ці галузі ще до завершення війни. Очікується, що кожен із секторів вироблятиме продукцію з високою доданою вартістю, що сприятиме підвищенню економічної стійкості країни. Крім того, Україна покладається на макрофінансову підтримку з боку Сполучених Штатів України.

Попри те, що війна триває, уряд України за підтримки партнерів активно веде процес відновлення, одночасно реалізуючи амбітну програму реформ та модернізації відповідно до стратегічних цілей країни.

У 2023 році уряд України виділив приблизно 7,2 мільярда доларів США для фінансування невідкладних проєктів відновлення в таких сферах, як енергетика, соціально значуща та критична інфраструктура, житловий сектор, гуманітарна допомога, розмінування, а також на підтримку державного сектору. У той же період було виконано масштабні реставраційні роботи: добудовано

3836 багатоквартирних будинків і 19091 індивідуальний будинок, зведено 448 шкіл, 237 дитячих садків і 390 медичних закладів та об’єктів соціального захисту. Крім того, відновлено 9200 об’єктів критичної інфраструктури, 449 теплопостачальних станцій, 221 об’єкт водопостачання та каналізації. Аварійно-відновлювальні роботи охопили понад 2000 км автодоріг і національних шляхів, 115 автомобільних мостів, близько 26 км залізничної інфраструктури та 46 залізничних мостів [66].

КМУ розробив інституційні механізми та впровадив реформи, спрямовані на поліпшення планування і реалізації зусиль з відновлення та реконструкції. У процесі підготовки до вступу до ЄС формується комплекс реформ у рамках Плану щодо України, що пов'язаний із Фондом для України, створеним Європейською комісією.

Четвертий звіт Швидкої оцінки збитків і потреб України (RDNA4) є найкомплекснішим. Його оновлені дані охоплюють період з лютого 2022 року до грудня 2024 року. RDNA4 було оприлюднено в лютому 2025 року. Аналіз, представлений у RDNA4, охоплює завдану шкоду в Україні за період майже трьох років – з 24 лютого 2022 року до 31 грудня 2024 року. Він вказує, що загальний обсяг прямої шкоди сягнув вже 176 мільярдів доларів США (170 мільярдів євро), що перевищує попередню оцінку RDNA3, опубліковану в лютому 2024 року. Тоді сума збитків становила 152 мільярди доларів США (138 мільярдів євро). Найбільш постраждалими секторами залишаються енергетика, житловий сектор, транспорт, торгівля, промисловість та освіта.

За поточними даними, пошкоджено або зруйновано близько 13% всього житлового фонду, що вплинуло на життя понад 2,5 мільйона домогосподарств. У енергетичному секторі зафіксовано на 70% пошкоджених або зруйнованих об’єктів порівняно з даними RDNA3 - це стосується об’єктів генерації, передачі та розподілу енергії, а також централізованого теплопостачання. Приблизно 72% усієї завданої шкоди припадає на регіони, наближені до лінії фронту, зокрема в Донецькій, Луганській, Херсонській, Харківській і Запорізькій областях, а також у Київській області.

Загальний обсяг довгострокових потреб свідчить, що найбільші витрати припадають на житловий сектор – майже 84 мільярди доларів США (81 мільярд євро). Друге місце займає транспортний сектор із майже 78 мільярдами доларів США (75 мільярдів євро), далі йдуть енергетика та видобувна галузь із приблизно 68 мільярдами доларів США (66 мільярдів євро). Торгівля й промисловість вимагають понад 64 мільярди доларів США (62 мільярди євро), а сільське господарство – більше 55 мільярдів доларів США (53 мільярди євро). Окремо варто зазначити, що витрати лише на очищення залишків руйнувань та управління ними становлять близько 13 мільярдів доларів США (12,6 мільярда євро) [67]. В RDNA4 представлено рисунок, який концептуалізує потреби у фінансуванні та показує забезпечене фінансування інвестиційних проєктів відновлення та відбудови та неінвестиційних програм (рис. 4.3).

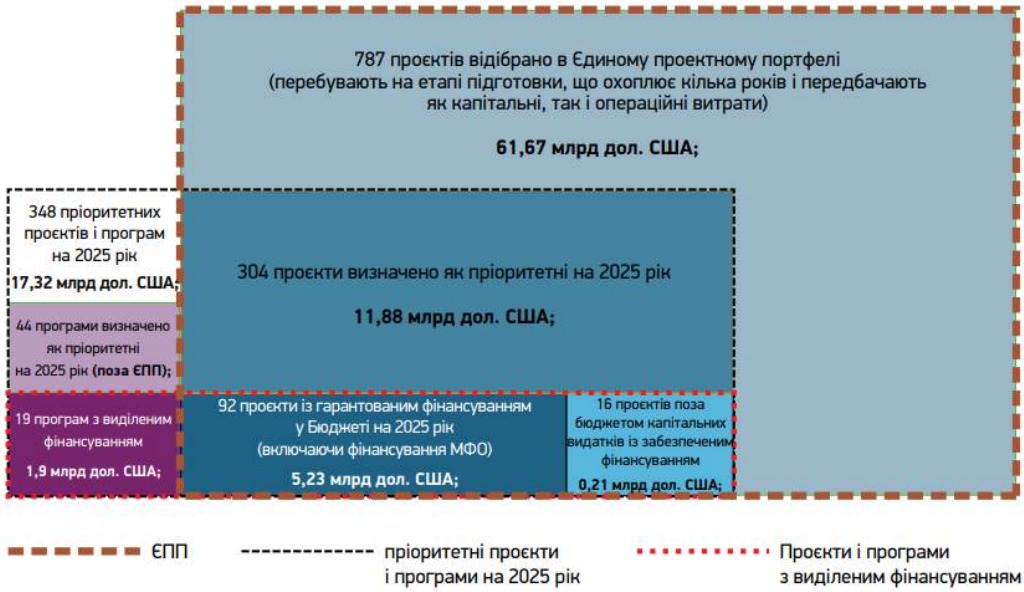


Рис. 4.3. Потреби у фінансуванні та забезпечене фінансування інвестиційних проєктів відновлення та відбудови та неінвестиційних програм*

*Джерело: розроблено автором на основі [67]

За підтримки донорів, у 2025 році за уряд України асигнував $7,37 млрд (€7,12 млрд) на подолання пріоритетних проблем у таких сферах, як соціальний захист, житло, охорона здоров’я, освіта, енергетика, транспорт, водопостачання, розмінування та цивільний захист. Водночас загальний дефіцит фінансування реабілітації та реконструкції у 2025 році становить 9,96 млрд доларів (9,62 млрд

євро). Залучення приватного сектору має вирішальне значення для успішного відновлення країни.

В результаті оцінки було встановлено та виключено потреби на суму понад 13 мільярдів доларів США (12,6 мільярдів євро) у восьми секторах, які Україна вже змогла покрити завдяки підтримці партнерів та приватного сектору. Зокрема, за інформацією уряду, у 2024 році на відновлення житлового сектору було виділено щонайменше 1,2 мільярда доларів США (1,1 мільярда євро) з державного бюджету та донорських коштів. Окрім того, здійснено аварійний ремонт понад 2000 км доріг, включаючи автомагістралі та інші шляхи державного значення [67].

Приватний сектор взяв участь у задоволенні деяких потреб з масиву існуючих нагальних потреб, що є свідченням його важливої ролі у процесах реконструкції. Доволі багато фірм почали здійснювати інвестування в ремонтні роботи та підвищення стійкості, зокрема за допомогою рішень у сфері розподіленої генерації - сонячні панелі, газові електростанції та біогаз.

Слід зазначити, зокрема, що RDNA4 рекомендує інвестувати в центри соціальних послуг та соціальне житло для забезпечення добробуту різних соціальних груп. Кожна група може мати свої специфічні потреби щодо житла, зокрема потребу в житлі, яке підходить для проживання з доглядом або отримання інших видів соціальних послуг. Проте більшість потреб, пов'язаних з житлом, можна задовольнити за допомогою соціального житла, яке відповідає принципам належного житла. Зрештою, розвиток системи соціального житла міг би допомогти задовольнити довоєнні потреби у житлі. Розробка такої системи вимагатиме змін до чинного законодавства та формулювання Національної житлової стратегії.

Тим часом, RDNA4 підкреслює суттєвий розрив між оціненими потребами у відновленні та забезпеченим фінансуванням, причому значна частина все ще не профінансована. Деякі звіти свідчать про те, що зосередження на невідкладних потребах може бути недостатнім для довгострокового відновлення та стійкості, оскільки менше уваги приділяється підтримці вразливих груп та побудові сталого майбутнього. Хоча досягнуто певного прогресу, залишаються

занепокоєння щодо прозорості та підзвітності у використанні коштів, а деякі звіти свідчать про те, що корупція та неефективне витрачання коштів можуть підірвати процес відновлення [70].

Інших стратегічних документів, що стосуються відбудови об'єктів критичної інфраструктури України після війни, поки що не сформовано. Але існує кілька ключових документів, які визначають напрямки діяльності у цій сфері:

1. Закон України «Про критичну інфраструктуру»: визначає поняття об'єктів критичної інфраструктури та їхню категорію, а також основні принципи захисту.

2. Методика категоризації об'єктів критичної інфраструктури: встановлює критерії та процедури, за якими визначається категорія об'єктів критичної інфраструктури.

3. Реєстр об'єктів критичної інфраструктури: містить перелік об'єктів, які підлягають захисту та відбудові після війни.

4. Стратегія відновлення України: загальний план відновлення країни, який має враховувати відбудову критичної інфраструктури.

19 вересня 2023 року Кабінет Міністрів України затвердив розпорядження, яким офіційно схвалено Національний план захисту, забезпечення безпеки та стійкості критичної інфраструктури. Розробкою цього документа займалася Адміністрація Держспецзв’язку. У плані визначено стратегічні цілі, ключові заходи та завдання для учасників національної системи захисту критичної інфраструктури, профільних органів, операторів критичної інфраструктури та інших державних установ. Він, зокрема, передбачає: специфікацію завдань та повноважень суб’єктів захисту критичної інфраструктури; покращення законодавства з регламентації їхньої діяльності; забезпечення проведення моніторингу; здійснення оцінки ризиків і загроз в критичній інфраструктурі; формулювання порядку взаємодії суб’єктів захисту КІ у разі кризових ситуацій; забезпечення роботи системи обміну інформацією; посилення рівня стійкості КІ; дизайн програм щодо роботи з громадами та підтримки населення у випадку виникнення кризових ситуацій; налагодження міжнародної співпраці тощо.

Передбачається, що виконання Національного плану, розрахованого на трьохрічний період, сприятиме безперебійній роботі об’єктів критичної інфраструктури різних категорій, забезпечить надійний захист від загроз та безперебійне надання життєво важливих послуг населенню.

Аналітичні центри та координаційно-експертні майданчики, які супроводжують процес відновлення України, створюються як всередині країни, так і за її межами. Українська організація громадянського суспільства ANTS за підтримки ЄС реалізує проєкт «Відновлюємо Україну разом: побудова інклюзивної платформи для відновлення України». Цей проєкт спрямований на формування експертної платформи для розробки планів повоєнного відновлення країни та забезпечення ефективної взаємодії між ключовими учасниками процесу: державними та місцевими органами влади, міжнародними донорами й партнерами, експертними та професійними об’єднаннями, а також представниками громадянського суспільства.

У рамках проєкту відбувся форум «Сильні як земля: наближаємо перемогу», на якому пройшли панельні дискусії на теми: «Бачення процесів відновлення на національному та міжнародному рівнях», «Голос громад», «Голос донорів» і «Голос бізнесу». У заході взяли участь народні депутати України, представники уряду, асоціацій місцевого самоврядування, міжнародних організацій, а також дипломати з посольств Швеції, Японії, Великобританії та США в Україні.

За кордоном було створено два аналітичні центри для підтримки відновлення України після війни. Один з них – GLOBSEC, аналітичний центр, що має штаб-квартиру в Братиславі. У вересні 2022 року він заснував Раду підтримки України, яку очолив колишній прем'єр-міністр Польщі Ян Кшиштоф Белецький. У жовтні GLOBSEC відкрив свій офіс у Києві. Основна діяльність Ради зосередиться на сприянні вступу України до Європейського Союзу, а також на процесах відновлення та інтеграції країни в Центральну Європу.Вона також планує надавати індивідуальні консультації через проведення комплексних досліджень та реалізацію пілотних проєктів.

У травні 2022 року Офіс ефективного регулювання BRDO представив дослідження під назвою "Аналіз міжнародного досвіду та найкращих практик щодо прозорої та підзвітної відбудови". У ньому зосереджено увагу на основних формах підтримки для відновлення, ключових етапах цього процесу та ризиках, а також заходах для запобігання корупції. Тоді ж «Центр прикладних досліджень» оприлюднив аналіз «Повоєнне відновлення економіки України», у якому коротко викладено стратегію економічного відновлення країни з визначенням пріоритетних галузей та результатами SWOT-аналізу.

Інститут аналітики та адвокації у межах проєкту «Re:Ukraine» здійснює дослідження досвіду країн, які пережили війни та катастрофи, з метою посилення можливостей України в ефективному економічному відновленні, проведенні реформ і змін у законодавстві після завершення військових дій. Серед публікацій проєкту – «Дослідження практик відновлення країн після руйнації: Афганістан» і «Впровадження рішень із відбудови в регіонах та громадах».

У листопаді 2022 року коаліція RISE презентувала документ «Інституційна архітектура відбудови: пропозиції RISE Ukraine», який містить рекомендації щодо загальних принципів, структури системи відновлення та її викликів.

Екологічна організація «Екодія» влітку 2022 року надала свій аналіз «Проєкту Плану післявоєнного відновлення України». У матеріалі підкреслюється підтримка ключових цілей плану, водночас акцентується увага на його недоліках із детальними рекомендаціями. Зазначається, що План, попри свої правильні напрямки, виглядає недостатньо цілісним і нагадує перелік окремих проєктів, часто несумісних і навіть конкурентних. У документі поряд із прогресивними рішеннями, такими як перехід на чисті безвуглецеві технології в металургії, заміна викопного газу на відновлювану енергію та інтеграція декарбонізації в усі сектори економіки, наявні й суперечливі або недостатньо узгоджені пункти.

Міжвідомча координаційна платформа донорів стала ключовим інструментом у процесі післявоєнного відновлення України, забезпечуючи співпрацю між українською владою та міжнародними партнерами. Серед донорів найчастіше застосовуються механізми координації у вигляді кластерів і

робочих груп: кластери здебільшого спрямовані на взаємодію з центральною владою, тоді як робочі групи забезпечують координацію між самими донорами, охоплюючи представників донорських структур та організацій громадянського суспільства. Значущим прикладом створення владою спеціалізованого органу стала робота нового Центру гуманітарного розмінування, метою якого є забезпечення ефективної взаємодії між донорами, що фінансують заходи з гуманітарного розмінування, операторами протимінної діяльності, органами місцевого самоврядування та міжнародними партнерами в сфері технічної допомоги.

«Програма з відновлення України» від ЄІБ розгортається з проєктів будівництва критично важливої інфраструктури. У 2022 році чимало гравців усередині України, включаючи представників влади, намагалися розробляти плани відновлення. Однак проведене навесні 2023 року дослідження, у якому брали участь ключові зацікавлені сторони (органи місцевого самоврядування, обласна виконавча влада, донори, організації громадянського суспільства), показало, що єдиного стратегічного плану відновлення України досі не створено. Це суттєво ускладнює роботу всіх стейкхолдерів.

На двох основних рівнях – органів центральної влади та місцевого самоврядування – спостерігаються значні проблеми у формуванні планів відновлення. Національна юридично закріплена рамка, яка була б зрозуміла для всіх учасників процесу, наразі відсутня. Хоча ситуація на рівні громад виглядає трохи кращою, це лише початок складного шляху, успіх якого залежатиме від скоординованих дій основних учасників процесу, таких як центральна влада та донори. Додатковою перепоною для громад є законодавча невизначеність: різні закони вимагають створення різних планувальних документів, які між собою не узгоджуються. Відсутність цілісного стратегічного плану на державному рівні і складнощі, які вона породжує у процесі відновлення, є центральною темою занепокоєння для більшості зацікавлених сторін: донорів, представників громад, виконавчої влади на місцях і організацій громадянського суспільства.

4.4. Механізми організації відбудови об’єктів критичної інфраструктури України в повоєнному періоді

Відновлення та реконструкція соціальної та економічної інфраструктури в постконфліктному середовищі є складними та давно обговорюваними питаннями у сфері співробітництва в галузі розвитку. Окрім того, що війна спричиняє масштабні людські страждання, породжує біженців, переміщує населення, породжує психологічний стрес, знищує інфраструктуру та трансформує економіку, у постконфліктних ситуаціях на найвищому соціальному, економічному та політичному рівнях можна спостерігати поглиблення хаосу та безладу; серйозні проблеми розвитку залишаються недостатньо вирішеними. Відновлення пошкодженої війною інфраструктури з метою реактивації місцевої економіки є викликом для всіх постконфліктних країн. Планування та реалізація проєктів реконструкції в районах, що постраждали від конфлікту, виявилися набагато складнішими, ніж очікувалося.

Відбудова об'єктів критичної інфраструктури України після війни – це складна задача, що потребує комплексного підходу. Для організації цього процесу необхідно чітке законодавче регулювання, координація зусиль різних державних органів та залучення міжнародної допомоги. Крім того, важливо врахувати особливості кожного об'єкта та його значення для стабілізації життя країни. Основні механізми організації відбудови систематизовано в таблиці 4.7.

Таблиця 4.7.

Основні механізми організації відбудови об’єктів критичної інфраструктури*

Механізм	Зміст
Законодавча база	Наявність чітких законів та нормативно-правових актів, що регламентують порядок відбудови, фінансування та управління процесом
	Закон України «Про критичну інфраструктуру» визначає перелік об'єктів, які підлягають особливій охороні та відновленню
Координація	Утворення центрального координаційного органу (наприклад, комітету або штабу), який буде відповідати за моніторинг ситуації, розробку планів відбудови та координацію дій різних органів
	Залучення до процесу секторних органів (міністерств та відомств), відповідальних за конкретні галузі

	Взаємодія з місцевими органами влади, які знають ситуацію на місцях
Фінансування	Залучення державних коштів (бюджетні асигнування, фонди)
	Залучення міжнародних партнерів та інвестицій
	Можливість залучення коштів від комерційних суб'єктів, які будуть залучені до відбудови
Збереження та відновлення	Створення реєстру об'єктів, які зазнали пошкоджень
	Оцінка обсягу пошкоджень та визначення пріоритетів відновлення
	Розробка планів відновлення, які будуть враховувати специфіку кожного об'єкта
Залучення фахівців	Залучення до процесу фахівців з різних сфер (інженерів, будівельників, енергетиків тощо)
	Надання можливості для професіоналів, які мають досвід відбудови після воєнних конфліктів, долучитися до проєкту
Контроль та моніторинг	Встановлення системи контролю за якістю робіт та дотриманням встановлених термінів
	Регулярний моніторинг процесу відновлення та внесення необхідних змін у плани
Інформаційна підтримка	Надання інформації населенню про процес відбудови
	Пояснення пріоритетів та обґрунтування прийнятих рішень

*Джерело: власна розробка автора

Відбудова об'єктів критичної інфраструктури - це не лише технічний процес, а й важка політична та економічна задача. Необхідно чітко визначити механізми координації та фінансування, залучити фахівців та забезпечити контроль за процесом.

Earnest (2015) стверджує, що після закінчення війни стало очевидно, що було завдано значної шкоди життю, майну та бізнесу; значною мірою ключова інфраструктура, така як дороги, мости, системи водопостачання, медичні центри, школи та телекомунікації, була серйозно пошкоджена або зруйнована, що призвело до термінової необхідності вирішення проблем гуманітарної кризи, що торкається великої кількості внутрішньо переміщених осіб і біженців. Стагнація економічного зростання в Косово та десятиліття неефективного управління знищили державний сектор, особливо в сфері охорони здоров'я та освіти в країні. Сільськогосподарський сектор, який відігравав життєво важливу роль у підтримці сільської економіки, був сильно порушений, а безробіття було поширеним. Підприємництво було недостатнім, і спостерігалися суттєві перебої в комунальних послугах, що призвело до перебоїв у постачанні води та електроенергії. Тим часом, міжнародні агенції працювали паралельно над тими

самими проблемами і водночас працювали в різних сферах, не залучаючи місцеві громади. Також Ернест [200] справедливо зазначає, що члени постконфліктного громадянського суспільства рідко включаються до процесів прийняття рішень, хоча їх частіше розглядають як партнерів у реалізації проєктів розвитку. Для досягнення сталого зростання та розвитку бенефіціари повинні систематично залучатися до процесів планування та прийняття рішень протягом усього життєвого циклу проєкту.

Проєкти є ключовими складовими у розробці та впровадженні політики та стратегій у сфері трансформації та реконструкції інфраструктури. Фактично, життєвий цикл проєкту – це не лише дати початку та завершення; це радше визначений та логічний підхід до планування та управління розвитком протягом усього життєвого циклу процесу. Згідно з PMI, процеси керуються п'ятьма групами процесів: ініціювання, планування, виконання, моніторинг та контроль, а також закриття [297]. Наголошується, що, хоча процеси управління проєктами загалом визнаються та застосовуються, це не означає, що ці практики повинні широко застосовуватися до всіх проєктів. У постконфліктному середовищі команда управління проєктом, у співпраці та партнерстві з ширшим керівним комітетом проєкту та спільнотою-учасником, повинна відповідати за визначення того, які знання, навички, інструменти та методи є доречними в даній ситуації. Проєктний цикл складається з низки поступових фаз, які, загалом кажучи, ведуть від визначення потреб та цілей до планування та впровадження заходів для задоволення заздалегідь визначених потреб та цілей, а також до оцінки результатів; він слугує для забезпечення структури та напрямку діяльності з розвитку, водночас дозволяючи залишатися в центрі уваги на ключових цілях та питаннях. Хоча точна кількість етапів дещо відрізняється залежно від кожної організації та кожного проєкту, як і назви що дані кожному етапу, можна визначити певні загальні фази, які присутні майже у всіх проєктних циклах. Планування та розробка проєктів повинні ґрунтуватися на точному аналізі постконфліктного середовища, зумовленого місцевими умовами. Належна підготовка, виконання та моніторинг є життєво важливими для ефективного та результативного використання донорських коштів, щоб забезпечити

використання ресурсів за призначенням та, що ще важливіше, для досягнення довгострокових цілей. Однак все ще існує великий розрив між теоретичними та практичними знаннями.

Варто зазначити, що Рада бізнес-омбудсмена в Україні систематизувала проблеми, з якими стикається бізнес у сфері відновлення критичної інфраструктури. Вона представила результати дослідження та свої рекомендації під вражаючим слоганом «Стратегія замість імпровізації».

У звіті Ради бізнес-омбудсмена висвітлено основні проблеми, які перешкоджають або повністю блокують зусилля щодо відновлення критичної інфраструктури. Серед цих проблем слід зазначити нестабільність фінансування, затримки у виплатах підрядникам, адміністративні бар'єри, труднощі з земельними питаннями, корупційні ризики в процесах державних закупівель, кадровий дефіцит, а також недосконале нормативне регулювання. Загалом, організація акцентує на проблемах, які є відомими та зрозумілими всім, зокрема й тим, хто має їх вирішувати.

Автори вищезазначеного звіту особливо наголошують на наявності проблеми слабкої комунікації між державою й бізнесом. Через відсутність ефективних механізмів залучення приватного сектору компанії нерідко опиняються в умовах правової та фінансової невизначеності. Це не лише демотивує їх брати участь у процесі відновлення, але й ускладнює довгострокове стратегічне планування.

Існує також проблема, яка залишається нерозв'язаною ще з часів СРСР, – неефективне використання виділених ресурсів. Територіальні громади часто не спроможні належним чином реалізувати проєкти відновлення, що призводить до невикористання наданих їм коштів. Крім того, інколи виникають затримки у прийнятті урядових рішень щодо використання міжнародного донорського фінансування, що значно ускладнює процес відновлення, зазначає РБО.

Крім того, слід звернути увагу на відсутність чітких критеріїв для відбору постачальників. Дискримінаційні вимоги замовників нерідко сприяють просуванню «зручних» компаній, що негативно позначається на якості виконаних робіт і їх ціні. Особливості проведення публічних закупівель під час

воєнного стану регулюються постановою Кабінету Міністрів України, котра дозволяє укладати договори без проведення відкритих торгів або використання електронного каталогу для придбання товарів. З одного боку, таке спрощення має на метіпришвидшитивідновлення критичної інфраструктури. З іншого боку, воно створює ризики зловживань і можливість тиску на бізнес з боку правоохоронних органів, залишаючи приватні компанії в потенційно вразливій правовій ситуації. Це ускладнює для замовників досягнення оптимального співвідношення ціни та якості, а також обмежує доступ нових учасників до ринку [43]. На сьогодні більшість закупівель відбувається за участю лише одного підрядника. Зокрема, за перші шість місяців 2024 року 85% тендерів, що проводилися через електронну систему закупівель, та 97% тендерів без її використання, були реалізовані з одним учасником [43].

Відсутність належного регулювання системи прямих закупівель та потенційні юридичні ризики стають серйозними стримуючими факторами для бізнесу, який міг би долучитися до процесу відновлення, зазначає РНБО. Окрім цього, вказується на те, що окремі експериментальні проєкти демонструють недостатній рівень прозорості у використанні державних коштів.

РНБО також акцентує увагу на ще одній надзвичайно важливій проблемі - примушенні бізнесу до співпраці. Формально участь компаній у відновленні визначається як добровільна й відбувається через тендерні процедури. Проте на практиці значний тиск з боку держави нерідко перетворює цю співпрацю на «добровільно-примусову». Державні органи та місцева влада часто звертаються до компаній із пропозицією залучитися до робіт із відновлення, але реальної можливості відмовитися від цих запитів практично немає. Як наслідок, бізнес змушений брати на себе фінансові та операційні ризики без жодних гарантій. У підсумку компанії залишаються наодинці з проблемами, що виникають після виконання робіт, включаючи затримки виплат, труднощі з оформленням необхідної документації тощо. Держава поки що не розробила ефективних механізмів захисту бізнесу від подібних ситуацій.

Тим часом, відновлення пошкодженої інфраструктури є життєво важливим для розбудови миру та соціальної стійкості, оскільки ефективна інфраструктура

є основою процесу відновлення та стійкості міст, у поєднанні з екологічною та соціальною стійкістю [314] та сталим розвитком [371]. Виходячи з наявної літератури, відновлення країни, що постраждала від війни, після конфлікту та воєнних дій [262] та досягнення її макроекономічної стабільності вимагає пріоритетного відновлення фізичної інфраструктури з акцентом на транспорт, енергетику, сільське господарство та розвиток міст. Окрім відновлення фізичної інфраструктури та об'єктів, економічний вимір постконфліктної реконструкції також включає надання гуманітарної допомоги та відновлення соціальних та інших послуг [200]. Така підтримка має забезпечити належні умови для розвитку приватного сектору, впровадження необхідних структурних реформ для зростання [325] та більш сталої інфраструктури [363] для узгодження з Цілями сталого розвитку Організації Об'єднаних Націй та зменшення вразливості міст. Звісно, допомога у відбудові може формуватися зовнішніми організаціями, застосовуючи концептуальні рамки для нових забудов, проте ці рамки можуть бути невідповідними для країн, в яких відбуваються військові дії [191], що стосується, звісно, й України.

Відновлення інфраструктури країни, зруйнованої війною, – це величезна операція, у здійсненні якої можукть бути корисними останні досягнення у моделюванні катастроф та стійкості, а також використання відкритих доступних даних для кращого інформування цих моделей [160]. Однак, існують також виклики, які необхідно подолати для успішної реалізації таких фреймворків [235]. По-перше, надзвичайно важливо мати практичну рамкову систему стійкості для відбудови та відновлення життєво важливої інфраструктури, наприклад, транспорту, енергетики, водопостачання та зв'язку. Рамкова система повинна забезпечити відновлення, яке є сталим та добре обґрунтованим, ґрунтуючись на (i) потребах людей, регіону та/або країни, (ii) змінах у використанні, важливості та перепрофілюванні критичної інфраструктури, (iii) пріоритетах у відбудові на основі наявних коштів та ресурсів, та (iv) ризиках тривалих бойових дій [231]. Останнє може продовжити період відновлення, оскільки після воєнного конфлікту все ще існують проблеми безпеки, і тому руйнування інфраструктури може повторитися, впливаючи на соціальні

(наприклад, домогосподарства, економіка, фірми та підприємства), а також фізичну інфраструктуру (наприклад, мости, дороги, залізничні станції, лікарні та школи) [222]. По-друге, фреймворк повинен адаптувати наявну теорію, структури та інструменти стійкості до потреб та особливостей країни, що пережила конфлікт, та її держави [113]. По-третє, фреймворк стійкості повинен повністю використовувати найсучасніші технології для пришвидшення виявлення пошкоджених активів та мереж, а отже, сприяння цілеспрямованому та обґрунтованому прийняттю рішень під час операцій з реконструкції [211].

Пошкоджені активи можна систематично ідентифікувати під час війни для отримання змістовних даних та документації про стан інфраструктури, наприклад, шляхом моніторингу пошкоджень за допомогою методів дистанційного спостереження (наприклад, супутникових знімків) [167; 367] та інших технологій [250; 365], а також використання доступних карт та геопросторового аналізу для кращого планування відновлення постраждалих міст [166]. Використання супутникових знімків та краудсорсингу соціальних мереж для оцінки порушень інфраструктури було широко досліджено в минулому в контексті стихійних лих [240] та впливу на навколишнє середовище [220] або місця розташування та ступеня пошкодження будівель в результаті конфліктів [155]. Ці дослідження продемонстрували додаткову цінність аерофотозйомки, яка, головним чином, сприяє ідентифікації або тяжкості пошкоджень [175] та забезпечує адаптивне відновлення та визначення пріоритетів [248]. У таких випадках основна увага, як правило, зосереджена на енергетичних мережах, може бути застосовним динамічне перепланування на основі оновлень інформації про пошкодження та коригування дій з відновлення. Однак, основна увага цих робіт зосереджена на будівлях або енергетичних мережах і не інтегрує інформацію з різних джерел (наприклад, краудсорсинг).

Однак, ці дані можуть бути корисними для визначення цілей, оцінки та визначення пріоритетів, що потім може бути використано під час та після конфлікту для пришвидшення прийняття рішень щодо реконструкції та стимулювання фінансування стійкості. Наприклад, це може сприяти відновленню виробничого потенціалу, ремонту та реконструкції

інфраструктури, зміцненню управління та інституцій, використанню можливостей для виходу на нові ринки шляхом зменшення невизначеності та чіткого донесення аргументів на підтримку реконструкції. Однак передача цієї конфіденційної інформації часто є складною, оскільки вона не повинна бути доступною у відкритому доступі.

Тим не менш, на сьогодні бракує відповідних структур стійкості для поствоєнного будівництва критичної інфраструктури. Наявні структури постконфліктної реконструкції в основному стосуються соціальних імплікацій та пом'якшення їх наслідків [263] та не надають належної інформації про матеріальні активи та інфраструктуру. Структури реконструкції зосереджені, наприклад, на впливі конфліктів на засоби до існування та переміщення населення, ролі соціальних мереж та діях щодо забезпечення соціального благополуччя та інклюзивності, а також відновлення внутрішньої безпеки [239]. Існує низка різних суб'єктів, які надають фінансову підтримку різними способами, включаючи уряди, міжнародні організації, установи з фінансування розвитку та неурядові організації. Ці організації допомагатимуть у реконструкції через офіційну допомогу розвитку, пільгове та непільгове кредитування та інші інструменти та заходи фінансування, такі як скасування боргу та бюджетна підтримка.

Мітуліс та ін. (2023) [269] пропонують структуру стійкості пошкодженої критичної інфраструктури, яка має на меті стимулювати відновлення та розбудову миру в країнах, що постраждали від війни, шляхом сприяння покращенню управління та прийняття рішень. Головною новизною цієї структури є те, що вона вперше запроваджує стійкість шляхом оцінки (RBA) у країнах, що постраждали від війни, тобто оцінку постраждалої критичної інфраструктури під час конфлікту, у поєднанні зі стійкістю шляхом втручання (RBI), тобто після конфлікту [237; 257] для пришвидшення прийняття рішень та реконструкції. Визнано, що RBA широко використовується у випадках стихійних лих, які виникають протягом тривалих періодів часу, що призводить до пошкодження інфраструктури, тим самим підвищуючи стійкість [166].

Тим не менш, нова структура RBA передбачає оцінку параметрів безпеки та збір даних для підвищення постконфліктної стійкості. Фреймворк використовує дані щодо топології та типології критичних активів, тоді як RBI використовує постконфліктні польові дані та експертизу для оцінки надійності, пропускної здатності, працездатності та змінних потреб інфраструктури. Проактивна стійкість шляхом проєктування (RBD) [257] для цивільної інфраструктури тут не розглядається, оскільки вона є нереалістичною у разі конфліктів. Mitoulis та ін. [268] застосовують цей фреймворк у кейсі транспортної мережі в районі Києва, щоб продемонструвати, як стійкість шляхом оцінки може підтримувати прийняття рішень та постконфліктну політику та практику у сфері відновлення інфраструктури. Автори вважають, що таке дослідження призведе до подальшого розвитку шляхом розширення його застосовності на інші активи, включаючи взаємозалежності інфраструктурних систем, у поєднанні з доказами та даними, що стануть доступними, коли буде можливий безпечний доступ до інфраструктури.

Цей кейс демонструє, як оцінка пошкоджень критично важливих об'єктів та ліній життєзабезпечення, у поєднанні з аналізом стійкості, заснованим на спостереженнях за станом подій під час конфлікту, може пришвидшити відновлення. Застосування фреймворку базується на кейсі руйнувань транспортної інфраструктури у західній частині Київської області - під час бойових дій було значно пошкоджено кілька мостів вздовж річки Ірпінь. Розташування та розмір досліджуваної території були обрані з урахуванням просторового розподілу пошкоджених об'єктів, стратегічного значення району, близькості до столиці та залежності від її надзвичайних ситуацій (наприклад, лікарень) та інших служб (наприклад, фінансових, освітніх), а також наявності даних для потреб цього кейсу. Це застосування фреймворку передбачає відновлення до повної операційної спроможності (FOC), однак, цю структуру можна застосовувати, прагнучи до вищих або нижчих рівнів операційної спроможності (наприклад, мінімальної сталої або мінімальної операційної спроможності) залежно від потреб після конфлікту. Mitoulis та ін. [268] справедливо стверджує, що хоча захист критично важливої інфраструктури

нещодавно був запроваджений у політиці національної безпеки України (2023 року Уряд України ухвалив розпорядження, яке затверджує Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури), це було переважно на концептуальному рівні та для мирних умов.

На національному рівні (крок 1) очікується, що певні кошти будуть виділені для кожного регіону/області та витрачені на максимізацію стійкості країни. Крок 2 показує регіон на захід від Києва, включаючи міста Ірпінь, Гостомель, Буча та Стоянка. На карті на кроці 2 рис. 4.4 зображено основні автомобільні та залізничні колії, мости, залізничні станції та лікарні. Можна стверджувати, що їх відновлення є більш ефективним, коли проводиться пріоритезація, гіпотетично показана тут як випадок «після конфлікту з рамковою структурою», на відміну від випадку «після конфлікту без рамкової структури», де було відновлено менше активів та з'єднань. Ця пріоритезація вимагає визначення сценарію, який забезпечує максимальну стійкість мережі, як на кроці 3, та активу, як на кроці 4.

На кроці 3 стійкість регіону показано як функцію часу, включаючи початок і кінець конфлікту, період відсутності реконструкції (час простою), після якого настає період тривалих бойових дій, протягом яких очікується коливання функціональності регіону. Відновлення може досягти різних рівнів ефективності, які описуються трьома цільовими можливостями (згідно з [231]), тобто мінімальна операційна здатність (MOC), яка, найімовірніше, відповідає плануванню на випадок надзвичайних ситуацій, мінімальна стійка здатність (MSC), яка відповідає ефективності, яку можна підтримувати за допомогою наявних ресурсів у країні після конфлікту, та повна операційна здатність (FOC), аналогічна або вища (в результаті адаптаційних заходів та втручань) до початкової (тобто, по суті, тут закладена можливість імплеменації концепції «Build Back Better»). Крок 4 стосується стійкості окремого об'єкта, яка залежить від оцінки та рішення, прийнятого на рівні мережі. Відновлення об'єкта після пошкодження залежатиме від ступеня пошкодження, тривалості конфлікту, ресурсів, виділених на відновлення після конфлікту та/або протягом тривалого періоду конфлікту, а також рівня цільових можливостей (див. крок 3).

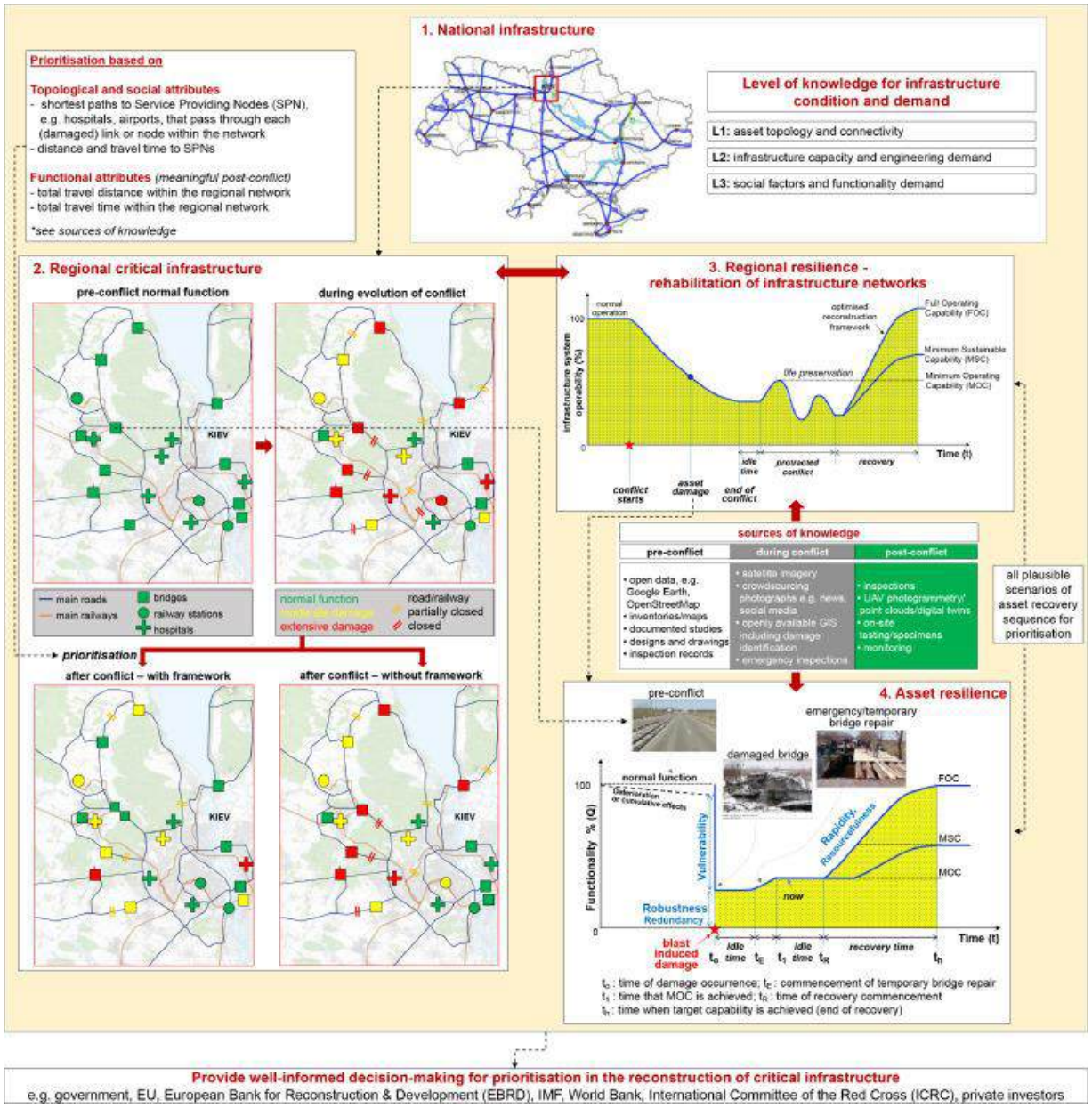


Рис. 4.4. Структура стійкості для відновлення критично важливої інфраструктури*

*Джерело сформовано автором на основі: [268]

На кроку 4 згадуються наступні терміни, які додатково обговорюються Mitoulis та ін. [268]: (1) Вразливість та стійкість, які залежать від типу мосту, наприклад, безперервне або просто опорне покриття, матеріалу та компонента(ів), пошкодженого(их) вибухом. (2) Надмірність, яка залежить від альтернативних структурних компонентів для передачі навантажень на ґрунт (тобто статично невизначеної конструкції), тоді як для мережі залежить від альтернативних маршрутів. (3) Ресурсозабезпеченість залежить від наявності

необхідних ресурсів і послуг, а також від здатності мобілізувати їх для відновлення після стихійного лиха. (4) Час простою залежить від тривалості конфлікту, доступності об’єкту, швидкості реагування та визначення пріоритетів. (5) Швидкість та час відновлення залежать, серед іншого, від важливості мосту, наявних ресурсів і політики, ступеня пошкодження та завдань з відновлення.

З моменту появи концепції стійкості в цивільному будівництві, представленої в [158], було розроблено кілька фреймворків для різноманітних систем та послуг (236; 247). Ці фреймворки зосереджені на стійкості громад та міст, критичній інфраструктурі, що зазнала впливу повеней або землетрусів, включаючи наслідки погіршення. Інші рамки стосуються множинних небезпек [269], включаючи залежності, та пропонують репрезентативні показники стійкості на основі задокументованих минулих подій. Спираючись на вищезазначені дослідження, можна створити нову та вкрай необхідний фреймворк постконфліктної стійкості для критичної інфраструктури в повоєнній Україні. Цей фреймворк має значні труднощі та відмінності від усталених фреймворків, а також запроваджує інновації, як обговорюється нижче:

1. Стійкість за оцінкою (resilience by assessment, RBA). Це суттєва прогалина в знаннях для досягнення обґрунтованої та швидкої постконфліктної реконструкції критичної інфраструктури. Існуючі рамки стійкості критичної інфраструктури застосовуються переважно до стихійних лих, таких як землетруси та кліматичні стресори, наприклад, повені. Таким чином, практичність та вплив RBA є низькими в рамках стійкості до стихійних лих порівняно з RBD та RBI, оскільки тривалість цих подій відносно коротка і, таким чином, забезпечує мінімальні можливості для RBA. Однак в енергетичних мережах адаптивні стратегії можуть бути застосовні шляхом коригування рішень під час відновлення на основі оновленої інформації та доказів стану мережі, заснованих на спостереженнях та даних про стан мережі. Проте це не є типовим або поширеним у транспортній інфраструктурі, наприклад, стосовно доріг, мостів або тунелей, які мають низьку резервованість, а розробка відновлювальних заходів передує їх застосуванню та дуже рідко коригується або

адаптується під час фази відновлення. Це пов'язано з відсутністю адаптивності типових тендерів, контрактів та процесів закупівель у будівельній галузі.

Існуючі заходи постконфліктного будівництва наголошують на реактивних заходах протягом періоду реконструкції [231]. Однак ефективне впровадження постконфліктних операцій вимагає інтенсивного моніторингу протягом усього конфлікту. Наприклад, Світовий банк наголошує на необхідності виділення достатніх ресурсів для моніторингу та оцінки, щоб кошти на будівництво виділялися під час мирних переговорів. Крім того, моніторинг та спостереження за станом безпеки можуть скоротити час затримки, пов'язаний з очікуванням оцінки стану інфраструктури до моменту вирішення конфлікту, оскільки доступ до землі під час конфлікту є складним та пов'язаний з високим ризиком. Час затримки також може бути результатом того, що органи влади мають різні пріоритети, або стан пошкоджень не залишатиметься остаточним, а руйнування, спричинені війною, часто тривають, і немає чітких перспектив щодо того, що станеться з активом, яким буде його стан, коли вручання буде нарешті безпечним.

Однак, цю перешкоду можна подолати, використовуючи відкрито доступні дані, які можна зібрати за допомогою дистанційних спостережень, у поєднанні з криміналістикою та краудсорсингом. Такі дані можна отримати з різних джерел, доступних до конфлікту, наприклад, дані про дорожній рух, супутникові знімки, інвентаризація, карти, записи інспекцій, попередні дослідження, а також під час конфлікту та тривалих бойових дій, наприклад, супутникові знімки, аерофотозйомка, доповнені метаданими телефонних дзвінків та новинами або краудсорсингом соціальних мереж. Ці дані можуть пришвидшити оцінку критичної інфраструктури та сприяти швидшому прийняттю рішень та відновленню після конфлікту, а отже, і більш ефективному фінансуванню стійкого та сталого будівництва міст, зосередженого на безпеці суспільства, включаючи політичні процеси, основні державні функції та верховенство права.

2. Оцінка типу та розподіл пошкоджень інфраструктури, наприклад, внаслідок обстрілів та антагоністичних атак, які суттєво відрізняються за наслідками та масштабами від пошкоджень, завданих іншими стресорами.

Інтенсивність конфлікту та спричинених ним руйнувань може бути загальнонаціональною, із змінною інтенсивністю, яка не підпорядковується певним законам згасання, що має місце у разі стихійних лих. У рамках постконфліктної стійкості пошкодження переважно стосуються видимих надземних компонентів та активів інфраструктури, наприклад, прогонових конструкцій мостів, фасадів та дахів будівель, резервуарів для води, тоді як вплив на фундаменти або підземні споруди, наприклад, трубопроводи, значно менший. З точки зору топології мережі, ця інформація менш доступна для багатьох інфраструктурних систем, частково або повністю закопаних під землею, і тому оцінка їх структурної та експлуатаційної спроможності під час конфлікту є дуже складною, якщо не неможливою. Ще однією особливістю є те, що превентивні заходи не є релевантними для рамок стійкості до конфліктів, наприклад, зміцнення транспортної інфраструктури від атак, подібно до зміцнення від стихійних лих [177]. Тим не менш, концепції теорії ігор можуть бути використані для захисту, наприклад, електромереж від атак. Це суттєво відрізняється від інших підходів, наприклад, адаптації до клімату до виникнення стихійних лих. Щодо розсіювання пошкоджень інфраструктури під час конфлікту, вони можуть бути розподілені по великих територіях, регіонах та/або по всій країні. Збитки можуть бути значними, включаючи численні критичні об'єкти, наприклад, мости, лікарні, транспортні вузли, такі як порти, аеропорти та залізничні станції, а також вежі зв'язку. Така інфраструктура може бути мішенню в рамках запланованих нападів або оборонних дій та навмисного виведення з ладу, які важко передбачити, наприклад, підрив критично важливих мостів та скидання води з дамб для блокування військового просування. Таким чином, антропогенні атаки призводять до пошкоджень з боку інтелектуальних супротивників, мають різну пам'ять і є менш випадковими порівняно, наприклад, з кліматичними небезпеками. Крім того, конфлікти призводять до широкомасштабних, а в деяких випадках і до загальнонаціональних збитків, тоді як збитки, спричинені стихійними лихами, більш локалізовані в певних районах та регіонах.

3. Розмежування планування дій у надзвичайних ситуаціях під час та після конфлікту. Планування потребує адаптації та варіації залежно від тривалості

конфлікту, затяжних бойових дій, суспільних потреб та військових операцій. Ці відмінності не потрібні для планування дій у надзвичайних ситуаціях після стихійних лих, які відбуваються протягом коротших періодів часу та зазвичай супроводжуються втручаннями, що підкріплюються загальнонаціональними механізмами цивільного захисту, і, ймовірно, будуть повністю функціональними для підтримки процесу відновлення.

4. Заходи післявоєнного відновлення зумовлені метою «перш за все збереження життя» та змінами у функціональному призначенні певних активів і мереж. Це означає збільшення резервування мережі та надання йому пріоритету над її ефективністю [174], таким чином захищаючи функціональність суспільства в періоди тривалих військових дій, на відміну від проєктування підвищення ефективності кількох активів. Наприклад, в енергетичних системах звичайною практикою проти малоймовірних подій з високим впливом є збільшення мережі шляхом додавання резервних маршрутів передачі та розподілу електроенергії для захисту інфраструктури від зовнішніх потрясінь (235; 248). Щодо перепрофілювання інфраструктури, заходи післявоєнного відновлення можуть суттєво відрізнятися від заходів після стихійних лих, оскільки люди втекли та/або змінили звички, тому структура враховує невідкладне використання та функціональне призначення критичної інфраструктури. Це може включати зниження потреб у потужностях, змінні моделі мобільності та різні потреби в певних районах.

5. Постконфліктна структура повинна враховувати нові політичні умови та обмеження. Існуючі структури передбачають наявність національного потенціалу для реконструкції та відновлення, достатніх фінансових ресурсів та технічної допомоги, досвіду у сфері реконструкції, а також людських ресурсів і матеріалів для відновлення пошкоджених активів. Однак у постконфліктних країнах політичні рішення, прийняття народом миротворчої діяльності або відмова від іноземної допомоги (наприклад, заборона на в'їзд до країни) та підтримки з боку міжнародних організацій визначатимуть політику та післявоєнну стійкість. Ці фактори визначатимуть час затримки у відновленні, який може бути значно довшим, ніж період відновлення після стихійних лих.

Підхід до реконструкції, створений після Другої світової війни, успішно дозволив відновити повоєнну Німеччину та Японію, як це було задумано. Цей підхід, відомий як план Маршалла, поєднував допомогу, реконструкцію та розвиток, щоб повернути країни до фінансової нормальності. Цей шаблонний підхід, який деякі вчені називають «парадигмою реконструкції», встановив модель для відновлення наступних зон воєнного конфлікту, але його застосування з того часу було менш успішним. Порівняння умов і, як наслідок, основних припущень є повчальним. У повоєнній Німеччині та Японії соціальні та професійні/торговельні інституції залишалися здебільшого неушкодженими, а населення загалом повернулося до своїх довоєнних професій. Ці інституції забезпечили необхідну основу, яка дозволила реінтеграцію колишніх комбатантів, примирення громади та реконструкцію навколо спільної мети та вигоди. Однак у більшості сучасних конфліктів фахівці та інші особи з ліквідними активами, як правило, знаходять способи покинути зону конфлікту. Чим довше триває конфлікт, тим менша ймовірність їхнього повернення, швидкого або взагалі. Аналогічно, чим довше триває конфлікт, тим менше працездатне населення пам'ятає, що таке нормальне життя. Це призводить до руйнування соціальних та економічних інститутів, необхідних для реконструкції, зокрема соціального капіталу. Соціальний капітал – це система «мереж та ресурсів, доступних людям через їхні зв'язки з іншими», і це набагато більше, ніж просто згуртованість громади та спільна ідентичність, хоча вони й впливають на неї. Було показано, що він особливо важливий для відновлення громад після стихійного лиха [231].

Наслідки конфлікту найбільше відчуваються на місцевому рівні, проте ця точка зору рідко представлена. Дійсно, точки зору часто принципово відрізняються у кожної зацікавленої сторони. Те, як кожна зацікавлена сторона сприймає потребу в інфраструктурі та пріоритети реконструкції, природно, буде базуватися на її відповідному баченні бажаного результату, а не на точному розумінні того, що існує. Здається очевидним, що якби можна було встановити спільне розуміння поточної ситуації на місцях, було б набагато легше також дійти згоди щодо того, якими є додаткові потреби.

Процеси трансформації та відновлення інфраструктури, особливо на локальному рівні, доцільно організовувати у вигляді своєрідної циклічної моделі (рис. 4.5).

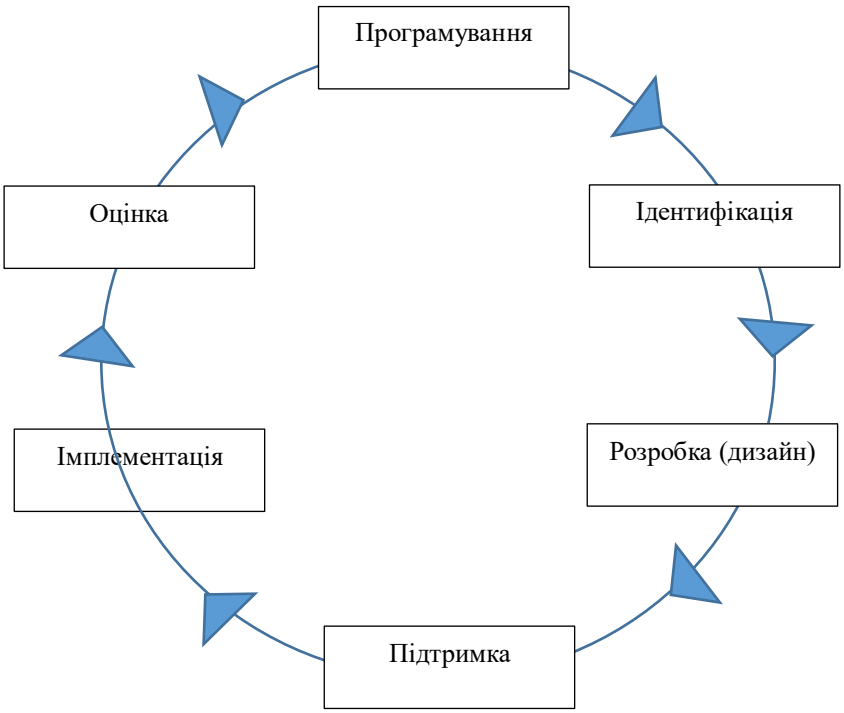


Рис. 4.5. Циклічний процес трансформації та відновлення інфраструктури*

* Джерело: власна розробка автора

Більше того, структура PMBOK пропонує комплексний підхід, що охоплює різні аспекти реконструкції інфраструктури, від початкового планування до остаточної передачі. Це дає можливість врахувати всі існуючі обмеження та збалансувати інтереси стейкхолдерів. Структура PMBOK передбачає чіткі етапи проєкту, чіткі зони відповідальності, прозорий бюджет та добре структуровані етапи. Управління проєктом повоєнної реконструкції для трансформації/реконструкції об'єктів критичної інфраструктури схематично можна зобразити, як показано на рис. 4.6. Здійснені зусилля з модернізації повинні пріоритезувати безпеку та стійкість, задовольняючи нагальні потреби людей та готуючись до майбутніх викликів.

Більше того, зростає інтерес до літератури щодо впровадження гнучкого управління проєктами в кількох промислових сферах, пов'язаних із середовищами, що характеризуються швидкими змінами [214]. Цей досвід також

є доцільним для використання в проєктаї повоєнної відбудови/трансформації критичної інфраструктури, завдяки гнучкості та можливості внесення миттєвих змін до проєктного процесу у відповідь на зміни у складових проєкту (наприклад, ресурсах), або у зовнішньому середовищі.

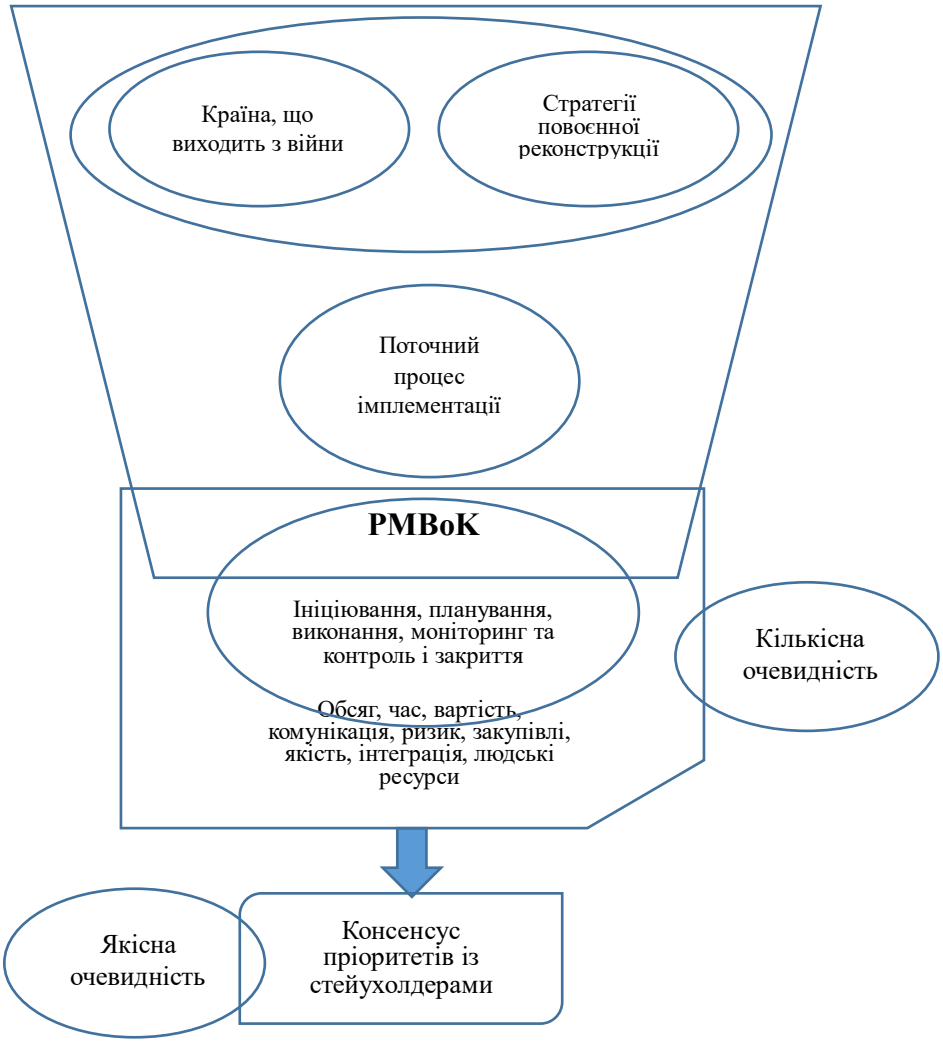


Рис. 4.6. Управління проєктами повоєнної реконструкції*

* Джерело: власна розробка автора

Гнучка методологія може дуже добре працювати для складної інфраструктури та складних інфраструктурних проєктів.

Практика показує високу застосовність поєднання Agile та Waterfall: у гібридному підході Agile використовується для планування, проєктування та технологічної інтеграції на ранніх стадіях. Як тільки проєкт досягає фази будівництва, вступають у дію перевірені методології Waterfall або #PRINCE2,

забезпечуючи стабільність та передбачуваність. Наприклад, під час планування лондонської залізниці Crossrail методи Agile використовувалися для вирішення складних змін у проєкті, тоді як будівництво спиралося на традиційні підходи до управління [284].

Більше того, інфраструктурні проєкти можуть використовувати зосередженість Agile на взаємодії з людьми, регулярних перевірках та коротких зустрічах. Регулярні зустрічі із зацікавленими сторонами проводяться у формі спринт-оглядів, що робить комунікацію дуже гнучкою, не ставлячи під загрозу стратегічне планування, необхідне для цих проєктів. Це особливо важливо, якщо проєкт реалізується в рамках моделі державно-приватного партнерства (ДПП).

Старіння інфраструктури, нові перешкоди, а також регуляторні, фінансові та демографічні зміни ускладнюють зусилля з адаптації та стійкості. Купріянов [253] визначають стійку інфраструктурну систему як таку, що добре функціонує сьогодні, «відновлюється» після збоїв, якщо вони трапляються, та «рухається вперед» або «краще відбудовується», щоб відповідати майбутнім викликам та запобігати майбутнім збоям. Це визначення узгоджується зі стандартом Міжнародної організації зі стандартизації (ISO), який визначає організаційну стійкість у більш широкому сенсі як «здатність організації абсорбувати та адаптуватися до змінного середовища, щоб мати змогу досягати своїх цілей, виживати та процвітати». Адаптації, які можуть бути реактивними, проактивними або трансформаційними – це конкретні зміни, які можуть підвищити стійкість системи, особливо для відновлення та/або руху вперед. Трансформаційні адаптації, тобто фундаментальні зміни в системі, все частіше визнаються необхідними для стійкості.

Існує багато підходів до постконфліктного відновлення, які визначають потреби в інфраструктурі на основі потреб громади. Дійсно, кожна країна, яка займається такою роботою, має свої власні тонкі варіації підходу відповідно до впливу своєї внутрішньої та зовнішньої політики. Існують інші підходи, що застосовуються міжнародними та комерційними організаціями. Потреби громади у відновленні є абсолютно правильним рушієм для визначення потреб в інфраструктурі, але менш зрозуміло, як це враховується. Якщо хтось має

розвивати інфраструктуру для певної мети, загальновизнано, що потрібно розуміти, що існує на даний момент, у контексті, а також будь-які обмеження та заборони щодо її розвитку. Це не завжди так – проєкти реконструкції інфраструктури, які призводять до заблокованих активів і мало сприяють відновленню чи взагалі сприяють, є надто поширеними. Необхідно використовувати різні підходи до відновлення.

Розвиток інфраструктури безпосередньо корелює з економічним зростанням, оскільки він пропонує можливість брати участь у виробництві державних послуг. Виконання договірних зобов'язань за допомогою ДПП у державних установах забезпечує ефективність інфраструктурних проєктів. Очікуваний результат економічного зростання, як у контексті Сирії, слід оцінювати шляхом виявлення проблем якості на початкових етапах. Для уряду, який прагне державно-приватних партнерств для великих інфраструктурних проєктів, використання можливостей приватного сектору в управлінні ризиками може бути більш ефективним та результативним підходом. Андрес та ін. [114] стверджують, що значний імпульс для державно-приватних партнерств полягає в досягненні підвищення ефективності надання інфраструктурних послуг та активів. Аналогічно, Fablre та Straub [210] підкреслюють, що розвиток інфраструктури на основі ДПП забезпечує підвищення ефективності надання послуг. Зазвичай підвищення ефективності визначається співвідношенням витрат до результату. Його можна покращити, забезпечуючи однаковий результат за зниженою вартістю (вхідні дані) або більший результат, використовуючи точне співвідношення вхідних ресурсів/витрат [114]. Згідно з [210], ДПП часто забезпечують підвищення ефективності приватного сектору та заздалегідь визначені або бажані показники ефективності державного сектора, такі як охоплення та якість. Це означає, що ДПП дозволяють державам або урядам укладати контракти на конкретні результати, прив'язуючи штрафи та платежі до результатів, тим самим стимулюючи залучену приватну організацію до зниження своїх витрат враховуючи результати [210]. Можна стверджувати, що це вимагає від приватного сектору більше зусиль для мінімізації повторюваних збоїв, таких як перевитрата коштів та затримки в

інфраструктурних проєктах. Зменшення таких очікуваних ризиків гарантує виконання проєктних результатів у рамках партнерства. Державний та приватний сектори визначають спільні підстави для скорочення витрат під час перевірки показників ефективності.

Однак, занадто часто ці ініціативи не в змозі знайти оптимальний рівень участі приватного сектору та, як наслідок, стикаються з тими ж проблемами, що й традиційні державні проєкти фінансування закупівель, – перевитратами коштів, затримками та підвищеною складністю. Головною проблемою є те, що уряди можуть не повною мірою скористатися справжньою перевагою залучення зацікавлених сторін приватного сектору: їхньою здатністю оцінювати, визначати ціну та управляти певними видами ризиків. ДПП, які не передають ризики та не отримують вигод від можливостей приватного сектору в управлінні ризиками, ймовірно, не виправдають очікувань.

Важливо наголосити, що ДПП не є варіантом вирішення проблеми інфраструктурних послуг, але це життєздатний механізм реалізації проєкту для бажаного варіанту рішення. Часто брак державного фінансування був основною причиною розгляду варіанту ДПП для проєкту. Однак брак державного фінансування може не бути основною причиною вибору варіанту ДПП для реалізації проєкту. Проєкти ДПП мають додаткові витрати – зазвичай вартість позики коштів вища для приватного сектору, ніж для державного сектору, а також існують адміністративні витрати на управління договірними режимами ДПП. Транзакційні витрати проєктів ДПП також можуть бути значними. Проєкти ДПП також можуть накладати багато явних та неявних зобов'язань на уряд. Проєкт не може розглядатися для реалізації як проєкт ДПП, якщо підвищення ефективності від покращення реалізації, експлуатації та управління проєктом, а також доступ до передових технологій не можуть компенсувати вищезгадані додаткові витрати. Фактично, багато країн встановили співвідношення ціни та якості як основний критерій оцінки переваг варіанту ДПП для проєкту [108].

Щоб покращити свої досягнення, державні розробники політики можуть узгодити свою діяльність з приватним сектором для кращого управління

ризиками, пов'язаними з реалізацією великого проєкту. Передача конкретних ризиків та відповідальності за проєкт протягом усього його життєвого циклу, включаючи розробку, будівництво та експлуатацію, приватним інвесторам (та кредиторам) використовує можливості управління ризиками приватного сектору та відповідних ринків, тоді як державний сектор часто залишається законним власником проєкту. Такий підхід часто передбачає премію за ризик, яка у великих приватних проєктах є центральною частиною рівняння витрат і, як така, повинна бути включена до розрахунку ДПП.

Тим часом існує багато важливих економічних, соціальних, політичних, правових та адміністративних аспектів, які необхідно ретельно оцінити, перш ніж уряд розглядатиме питання про схвалення ДПП. ДПП мають різні обмеження, які також слід враховувати під час їх розгляду. Основні обмеження включають:

– не всі проєкти є доцільними (з різних причин: політичної, правової, комерційної життєздатності тощо);

– приватний сектор може не зацікавитися проєктом через уявні високі ризики або може не мати технічних, фінансових чи управлінських можливостей для реалізації проєкту;

– проєкт ДПП може виявитися дорожчим, якщо додаткові витрати (через вищі транзакційні та фінансові витрати) не можуть бути компенсовані за рахунок підвищення ефективності;

– зміна в експлуатації та управлінському контролі над інфраструктурним активом через ДПП може бути недостатньою для покращення його економічних показників, якщо не будуть виконані інші необхідні умови. Ці умови можуть включати відповідні реформи сектору та ринку, а також зміну операційної та управлінської практики експлуатації інфраструктури.

Часто успіх ДПП залежить від ефективності регулювання, і саме цей фактор є вирішальним для України, враховуючи підводні камені, невдачі та затримки в інфраструктурних проєктах ДПП до війни 2022 року. Також зараз чіткі механізми ДПП не викладені в стратегічних документах щодо післявоєнної реконструкції інфраструктури. Кожна з цих п'яти категорій має багато варіантів.

Хоча спектр моделей можливий як окремі варіанти, можливі також комбінації, такі як договір оренди або (часткової) приватизації існуючих об'єктів, який включає положення про розширення через лагцюжок «Будівництво-Експлуатація-Передача». Фактично, багато проєктів ДПП останнього часу є комбінованими.

Моделі ДПП можна класифікувати на п'ять широких категорій у порядку загального (але не завжди) збільшення участі та прийняття ризиків приватним сектором. Ці п'ять широких категорій: договори на постачання та управління; договори «під ключ»; афермаж/оренда; концесії; приватна фінансова ініціатива (ПФІ) та приватна власність.

Забезпечення передбачуваних ризиків передбачає використання ефективних стратегічних заходів під час реалізації. Зусилля, що докладаються в рамках ДПП, спрямовані на сприяння зростанню охоплення та якості інфраструктурних проєктів. Постійні перешкоди у виконанні завдань уряду та бізнесу дозволяють успішним партнерствам будувати інфраструктуру. З іншого боку, Хюн, Парк та Тянь [238] стверджують, що два різні мотиви стимулюють розвиток інфраструктури через ДПП. По-перше, уряд або держава прагне досягти як розвитку інфраструктури, так і економічної ефективності завдяки участі приватного сектору. По-друге, приватний сектор прагне отримувати прибуток, пропонуючи послуги та інфраструктуру [110]. Оскільки приватний сектор бере участь у ДПП, він отримує прибуток від контрактів, одночасно постачаючи матеріали для використання. Це включає взаємодію з їхніми підприємствами для підтримки виконання угод про ДПП. Для досягнення ефективних та успішних партнерств як приватний, так і державний сектори мають схожі цілі щодо ефективності, якості та підзвітності у наданні послуг та будівництві інфраструктури [238]. Фінансування приватного сектору підвищує кредитну цінність суспільства, а уряд створює значні інвестиційні проєкти для громадського використання. Збіг цілей та завдань державного та приватного секторів впливає на економічний зсув у бік зростання. Зростання реального кредитування приватного сектору уповільнило приватні інвестиції, а державні інвестиції є основними факторами, що впливають на участь приватного сектору

в розвитку інфраструктури та наданні послуг. ДПП сприяють економічному зростанню шляхом будівництва інфраструктури [114; 210]. У світовій практиці ДПП в основному реалізуються в транспортній інфраструктурі, такій як дороги, мости, залізниці, автомагістралі та тунелі [114]. Іншими ключовими сферами ДПП є об'єкти громадського обслуговування, такі як в'язниці, гуртожитки, шкільні будівлі, лікарні та спортивно-розважальні заклади. Ці сектори слід ретельно вивчити, щоб отримати фінансові вигоди, пов'язані з інфраструктурними проєктами.

Роль ДПП спрямована на забезпечення стабільності в діяльності уряду та приватних підприємств, що є критично важливим як в умовах війни, так і в процесі повоєннох відбудови. Оскільки організації співпрацюють з урядом, посилена увага до покращення якості життя громадян залишається пріоритетом. Завдяки ДПП місцеві органи влади, включаючи уряд, забезпечують досягнення економічного зростання в рамках цієї співпраці. Економічне зростання досягається завдяки збільшенню інвестицій та вищим економічним результатам у цих проєктах.

Висновки до розділу 4

1. Проведений аналіз демонструє суттєве погіршення стану критичної інфраструктури в Україні внаслідок бойових дій на території країни. Російські атаки завдали значної шкоди численним об’єктам енергетичної інфраструктури в сфері сфери енергетики, телекомунікації, комунального господарства транспорту, охорони здоров'я. При цьому об’єкти енергетичної інфраструктури, як мишені прицільних атак російських військ, зазнали найбільш руйнівного впливу. Повністю знищено Каховську ГЕС та деякі ТЕС. Постраждав як сектор виробництва, так і передачі електроенергії. Найбільш суттєві руйнування зафіксовані у прифронтових областях, але енергетичний сектор став об’єктом атак ворога і в тилових регіонах. Суттєвих пошкоджень зазнала також транспортна інфраструктура, автономобільні дороги і мости, портова

інфраструктура. Загальний стан об'єктів критичної інфраструктури в Україні вказує на потребу в терміновому відновленні та модернізації, навіть в умовах ще не закінченої війни.

2. Незважаючи на нагальну потребу відбудови критичної інфраструктури, в Україні не сформовано пул стратегічних документів щодо відбудови об’єктів критичної інфраструктури, що безсумнівно є негативним фактором. Відповідно, не сформовано і чітких механізмів та дорожніх карт відбудови, не проводиться систематизоване вивчення зарубіжного досвіду відбудови критичної інфраструктури. Між тим, було складено звіти RDNA - швидка оцінка завданої шкоди та потреб у відновленні. Вього таких документів чотири, останній з яких (RDNA4) було орубліковано в лютому поточного року. Цей документ концептуалізує потреби у фінансуванні та показує забезпечене фінансування інвестиційних проєктів відновлення та відбудови та неінвестиційних програм. Попри те, що отримані оцінки характеризуються доволі високою точністю та достовірністю, детальних механізмів відбудови не запропоновано.

3. В роботі розглянуто поняття структура стійкості для відновлення критично важливої інфраструктури та запропоновано здійсннювати управління проєктами повоєнної реконструкції на основі проєктної методології PMBoK з урахуванням інтересів стейкхолдерів. Структура PMBOK передбачає чіткі етапи проєкту, чіткі зони відповідальності, прозорий бюджет та добре структуровані етапи. Розроблено відповідну концептуальну схему. Пропонується також інтегрувати елементи проєктного управління Agile, що дозволить вносити швидкі зміни в документацію та реалізацію проєктів у разі різких змін умов середовища – наприклад, зміни безпекової стьуації. Також доведено доцільність застосування моделей ДПП для планування та реалізації проєктів відбудови критичної інфраструктури. В той же час підкреслюється, що критично важливою задачею є знаходження оптимального рівня і моделі участі приватного сектору в ДПП-проєктах.

РОЗДІЛ 5
УДОСКОНАЛЕННЯ КОНЦЕПТУАЛЬНИХ ЗАСАД ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ТРАНСФОРМАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

5.1. Концепція публічного управління у сфері трансформації об'єктів критичної інфраструктури

Необхідність оновлення концепції публічного управління у сфері трансформації об'єктів критичної інфраструктури зумовлена глибокими змінами суспільно-політичного, безпекового та економічного середовища України. Повномасштабна агресія росії проти України спричинила безпрецедентні руйнування енергетичних, транспортних, водопостачальних, комунікаційних та соціальних систем, оголивши системну вразливість існуючих моделей управління. Традиційна бюрократична парадигма, орієнтована на централізоване прийняття рішень, виявила свою неефективність у кризових ситуаціях, де необхідна швидкість реакції, гнучкість і координація між секторами. Водночас процес децентралізації, цифрової трансформації та зростання ролі місцевих громад вимагає принципово нових підходів до публічного управління - таких, що забезпечують не лише відновлення зруйнованої інфраструктури, а й її перетворення у стійкі, адаптивні й безпечні системи [103].

Сучасне публічне управління має виходити з інтеграції стратегічного, ризик-орієнтованого та інноваційного мислення, де ключовим ресурсом виступають не лише фінанси чи технології, а дані, довіра та взаємодія. В умовах постійних загроз, кіберризиків і гібридних атак ефективне управління неможливе без побудови системи моніторингу, прогнозування та швидкої реакції на основі цифрових платформ. Таким чином, оновлення концепції управління критичною інфраструктурою не є лише адміністративним завданням,

а стратегічною умовою збереження державності, безпеки громад і сталого розвитку (табл. 5.1).

Таблиця 5.1

Порівняння традиційної та оновленої концепції публічного управління у сфері трансформації критичної інфраструктури*

Ознака порівняння	Традиційна модель управління	Оновлена концепція управління
Основна парадигма	Централізоване реагування на події	Адаптивне, проактивне та децентралізоване управління
Ключовий принцип	Підпорядкування вертикалі влади	Партнерство, поліцентричність, взаємодія секторів
Джерело управлінських рішень	Нормативно-адміністративні процедури	Аналітика даних, оцінка ризиків, стратегічне планування
Характер рішень	Реактивний, орієнтований на наслідки	Превентивний, орієнтований на запобігання та розвиток
Інформаційна основа	Фрагментарна звітність	Інтегровані цифрові системи моніторингу та аналізу
Участь заінтересованих сторін	Обмежена, формальна	Широка, з урахуванням позицій громад, бізнесу, міжнародних партнерів
Цільова орієнтація	Відновлення функціональності	Забезпечення стійкості, інноваційності та безпеки

*Джерело: сформовано автором на основі [38; 49; 60; 103]

Концептуальне ядро оновленого публічного управління у сфері трансформації об'єктів критичної інфраструктури становить триконтурна управлінська архітектура, у якій стратегічно-планувальний, ресурсний та інституційний контури функціонують не як ізольовані підсистеми, а як взаємозалежні площини єдиного управлінського циклу. Стратегічно-планувальний контур задає цілі, пріоритети й сценарії розвитку інфраструктури на національному, регіональному та локальному рівнях; ресурсний контур забезпечує мобілізацію, розподіл і перерозподіл фінансових, матеріально-технічних, людських та інформаційних ресурсів відповідно до визначених пріоритетів; інституційний контур формує норми, процедури, організаційні структури та механізми підзвітності, що уможливлюють реалізацію стратегічних рішень. Саме поєднання цих трьох контурів дозволяє подолати розрив між стратегічним баченням і практикою його впровадження – розрив, який у традиційній моделі управління залишався системною вадою (рис. 5.1.).

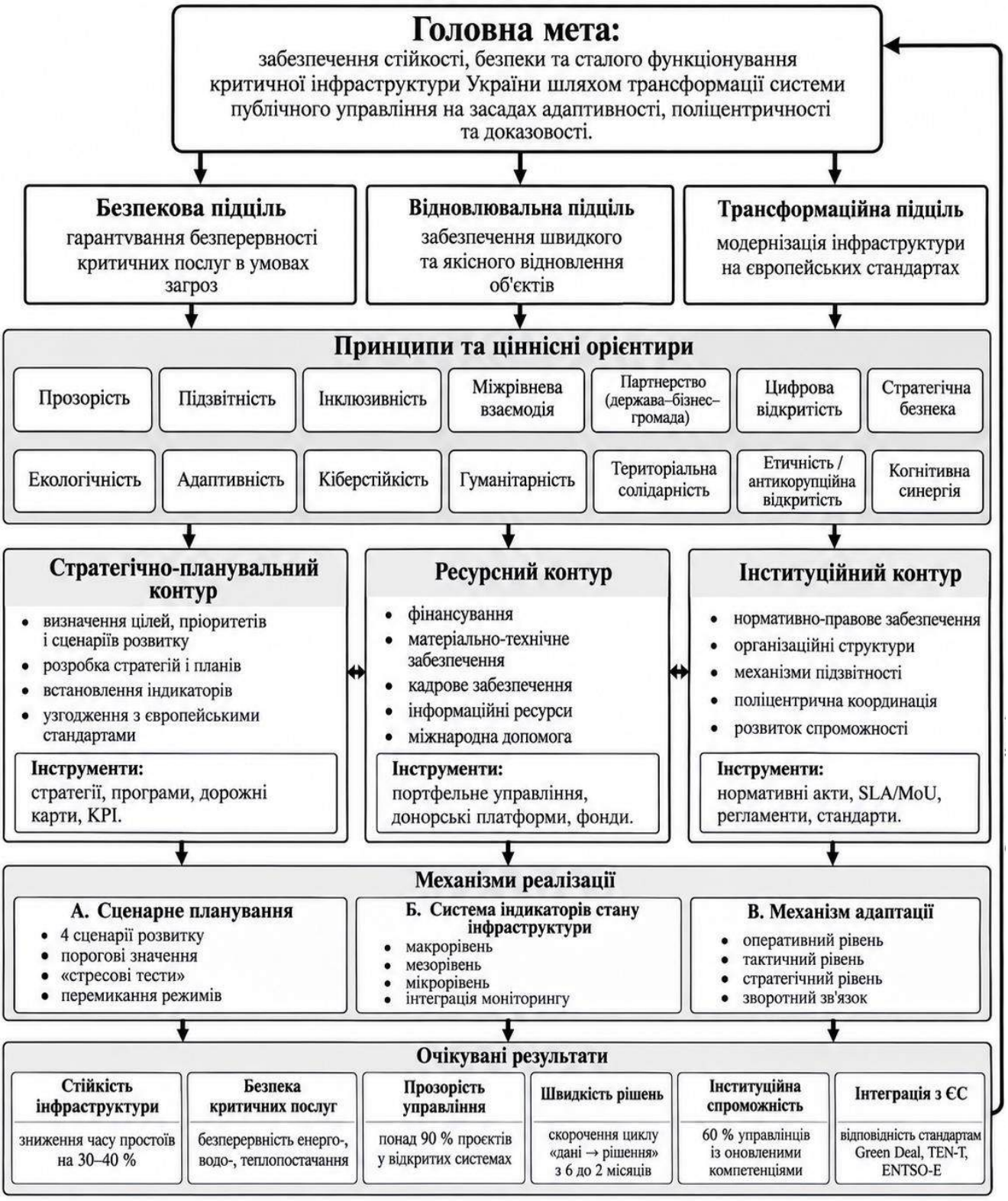


Рис. 5.1. Концепція публічного управління змінами об’єктів критичної інфраструктури

*Джерело: власна розробка автора

На відміну від лінійних моделей «рішення – виконання – звітність», триконтурна архітектура передбачає постійну синхронізацію: стратегічні цілі

коригуються з урахуванням ресурсних обмежень, ресурсні рішення легітимізуються через інституційні процедури, а інституційні зміни ініціюються у відповідь на стратегічні виклики та ресурсні диспропорції. Така конфігурація забезпечує не лише керованість, а й адаптивність системи – здатність перебудовувати власні функції та процедури відповідно до динаміки загроз і потреб відновлення.

Головна мета Концепції: забезпечення стійкості, безпеки та сталого функціонування критичної інфраструктури України шляхом трансформації системи публічного управління на засадах адаптивності, поліцентричності та доказовості. *Підцілі:*

– безпекова підціль: гарантування безперервності критичних послуг в умовах загроз;

– відновлювальна підціль: забезпечення швидкого та якісного відновлення об'єктів;

– трансформаційна підціль: модернізація інфраструктури на європейських стандартах.

Контури:

1. *Стратегічно-планувальний контур:* визначення цілей, пріоритетів і сценаріїв розвитку; розробка стратегій і планів; встановлення індикаторів; узгодження з європейськими стандартами. Інструменти: стратегії, програми, дорожні карти, KPI.

2. *Ресурсний контур:* фінансування; матеріально-технічне забезпечення; кадрове забезпечення; інформаційні ресурси; міжнародна допомога. Інструменти: портфельне управління, донорські платформи, фонди.

3. *Інституційний контур:* нормативно-правове забезпечення; організаційні структури; механізми підзвітності; поліцентрична координація; розвиток спроможності. Інструменти: нормативні акти, SLA/MoU, регламенти, стандарти.

У сучасних умовах повоєнного відновлення механізми інтеграції процесів реконструкції у державну політику набувають системного характеру, формуючи цілісну управлінську архітектоніку, у якій взаємодіють п’ять взаємопов’язаних

рівнів - стратегічний, координаційний, операційний, аналітичний і соціальний. Ця структура функціонує не як лінійна адміністративна модель, а як динамічна система взаємного підсилення, що забезпечує зворотний зв'язок між плануванням, реалізацією, моніторингом та громадською участю. Вона є інституційним ядром переходу від короткотермінових проєктів до довготривалої політики стійкого розвитку, у якій відбудова трактується як безперервний процес управлінського навчання та адаптації. Логіку взаємодії цих рівнів можна подати у вигляді блок-схеми (рис. 5.2).



Рис. 5.2. Управлінська архітектоніка інтеграції відбудови у систему державної політики*

*Джерело: власна розробка автора

На рис. 5.2 відображено послідовну, але взаємопов'язану логіку функціонування управлінських рівнів. На стратегічному рівні відбувається інституалізація відбудови - перетворення разових рішень на політику, синхронізовану з національними стратегіями розвитку та бюджетним циклом. Координаційний рівень забезпечує горизонтальну взаємодію між секторами, урядом, громадами та міжнародними партнерами, перетворюючи політичні рішення на керовані програми. На операційному рівні реалізується програмно-

цільовий підхід - формуються пакети проєктів із єдиними процедурами моніторингу, контролю та звітності.

Аналітичний рівень забезпечує зворотний зв’язок: за допомогою систем оцінки ефективності, цифрового моніторингу та big data формується база для коригування державних рішень. Соціальний рівень замикає управлінське коло, залучаючи громадян до процесів контролю та формування політики. Саме тут відбувається легітимація рішень через публічність, відкритість і спільну відповідальність.

У сукупності ці рівні створюють інтегровану систему управління відбудовою, яка здатна працювати в умовах невизначеності та забезпечувати адаптивність державної політики. Її ефективність вимірюється не лише кількістю реалізованих проєктів, а здатністю територій до самовідновлення, економічного відтворення й довгострокової стабільності, що визначає перехід України до політики відновлювальної резильєнтності.

Проблеми реалізації процесів відновлення на деокупованих територіях України мають цивілізаційний, а не лише технічний характер, оскільки стосуються глибинних соціальних, просторових і ціннісних трансформацій. Вони формують специфічне управлінське середовище, де традиційні інструменти державної політики стикаються з викликами, що виходять за межі інфраструктурного відновлення.

Становлення оновленої концепції публічного управління у сфері трансформації критичної інфраструктури зумовлене переходом від процедурно-бюрократичної логіки до ціннісно орієнтованого, аналітично обґрунтованого й цифрово інтегрованого управління. У такій рамці базові засади - прозорість, підзвітність, інклюзивність, міжрівнева взаємодія, партнерство держави, бізнесу та громади, цифрова відкритість і стратегічна орієнтація на відновлення та безпеку - виконують роль не декларацій, а операційних вимог до даних, процесів і відповідальності. Повномасштабна війна Росії проти України розширила цю систему принципів: практичні виклики 2022–2025 рр. інституціоналізували екологічність, адаптивність, кіберстійкість, гуманітарність, територіальну

солідарність, етичність/антикорупційну відкритість і когнітивну синергію як обов'язкові критерії якості рішень і архітектури відновлення (табл. 5.2).

Таблиця 5.2

Принципи та ціннісні орієнтири оновленої Концепції публічного управління трансформацією критичної інфраструктури*

Принцип / орієнтир	Зміст і прояв у сучасному управлінні	Аналітичне значення / очікуваний ефект
Прозорість	Відкритість даних про планування, фінансування та реалізацію проєктів; публічні масиви та машинна валідація звітності.	Зростання довіри, зниження корупційних ризиків, відтворюваність обліку.
Підзвітність	Зовнішній аудит, незалежна верифікація результатів, персоніфікована відповідальність виконавців.	Перехід від формального контролю до оцінки результатів і впливу.
Інклюзивність	Участь громад, бізнесу, академії та донорів у плануванні й моніторингу.	Легітимність політики, пристосованість рішень до локальних потреб.
Міжрівнева взаємодія	Узгодження дій уряду, регіонів і громад на спільній даній та методичній основі.	Усунення дублювання, зменшення транзакційних витрат.
Партнерство (держава–бізнес–громада)	Спільні портфелі, співфінансування, співуправління активами.	Синергія ресурсів, розподіл ризиків і вигод.
Цифрова відкритість	Інтероперабельність реєстрів, стандарти даних, захищені канали обміну.	Прискорення циклу «дані → рішення», менші інформаційні асиметрії.
Стратегічна безпека та відновлення	Сценарне планування, резервування потужностей, безперервність послуг.	Підвищення готовності, скорочення часу простоїв.
Екологічність	«Зелене» проєктування, енергоефективність, циркулярність матеріалів.	Узгодженість із Green Deal, менший вуглецевий слід і витратність життєвого циклу.
Адаптивність	Регулярна ревізія планів під фактичні ризики/ресурси; гнучкі цикли рішень.	Оперативність реагування, стабільність сервісів у кризі.
Кіберстійкість	Неперервність цифрових сервісів, захист критичних даних, реагування на інциденти.	Збереження цілісності керування, зниження системних ризиків.
Гуманітарність	Пріоритет безпеки, здоров'я, доступності та рівності у реконструкції.	Соціальна згуртованість, справедливий доступ до послуг.
Територіальна солідарність	Баланс ресурсів між регіонами, підтримка вразливих територій.	Зменшення просторової асиметрії відновлення.
Етичність та антикорупційна відкритість	Етичні стандарти рішень, відкритий нагляд, запобігання конфлікту інтересів.	Нульова толерантність до зловживань, легітимність політики.
Когнітивна синергія	Використання наукових знань і big data для моделювання політик.	Кращі прогнози, інноваційність управлінських рішень.

*Джерело: сформовано автором на основі [44; 48; 312]

Система індикаторів стану інфраструктури, передбачена концепцією, має будуватися за принципом багаторівневості та взаємодоповнюваності. На

макрорівні (національному) доцільно використовувати агреговані показники: індекс фізичної доступності критичних послуг, коефіцієнт резервування потужностей, середній час відновлення після інцидентів (MTTR), частку об'єктів, що відповідають стандартам кіберстійкості. На мезорівні (регіональному та галузевому) – показники функціональної стійкості: рівень дублювання критичних вузлів, частку децентралізованої генерації, щільність сенсорних мереж моніторингу, індекс готовності громад до надзвичайних ситуацій. На мікрорівні (об'єктовому) – технічні параметри: знос обладнання, залишковий ресурс, відповідність проєктним вимогам, наявність автоматизованих систем управління. Інтеграція цих індикаторів у єдину систему моніторингу дозволяє не лише фіксувати поточний стан, а й прогнозувати ризики, визначати пріоритети інвестування та оцінювати ефективність управлінських рішень у динаміці. Запровадження такої системи відповідає принципам evidence-based policy та data-driven public management і створює основу для переходу від реактивного управління до управління на основі випереджального передбачення.

Оновлена Концепція публічного управління у сфері трансформації об’єктів критичної інфраструктури сьогодні формується під впливом безпрецедентних викликів, спричинених воєнною агресією росії проти України. За оцінкою Київської школи економіки, сукупні прямі збитки інфраструктури України станом на 1 вересня 2023 р. сягнули 151,2 млрд дол. США, зокрема у транспортній, енергетичній, житловій та комунальній сферах [32]. Оновлена оцінка Світового банку, ЄС та ООН у 2025 р. фіксує загальні потреби у відбудові та модернізації на рівні 524 млрд дол. США, з яких понад 20 % припадає на критичну інфраструктуру [355]. Це свідчить про масштабність завдання, що виходить за межі звичайного відновлення - йдеться про глибинну трансформацію управлінської системи, здатної забезпечити адаптивність, безпеку й енергетичну незалежність держави.

Під час активної фази бойових дій у 2022–2024 рр. зафіксовано понад 967 випадків пошкодження критичних об’єктів, включно з енергетичними, телекомунікаційними та транспортними вузлами [121]. У сфері енергетики, за

даними Міжнародного енергетичного агентства, понад 800 котелень і десятки теплоелектростанцій було пошкоджено або зруйновано, що призвело до тимчасової втрати ≈21 ГВт потужностей [34]. У 2024 р. рівень пошкоджень енергомереж оцінювався ще у 9 ГВт, тобто близько 30 % довоєнної генерації [34]. За інформацією ООН, лише в опалювальний сезон 2023–2024 рр. зафіксовано 223 масовані атаки на енергетичну інфраструктуру у 23 областях, у середньому понад сім на тиждень [196].

У таких умовах централізована модель управління, побудована на вертикалі підпорядкування, виявилась неефективною: вона не забезпечує швидкого реагування, гнучкої координації та аналітичної підтримки рішень. Тому відбувається поступовий перехід до мережевої, поліцентричної моделі, у якій держава, громади, приватний сектор і міжнародні партнери взаємодіють у реальному часі через цифрові платформи. Яскравим прикладом стала діяльність Державного агентства відновлення та розвитку інфраструктури України, створеного у 2023 р., яке інтегрувало дорожню й інфраструктурну політику, запровадило антикорупційні механізми й систему публічного моніторингу [209]. Агентство координує понад 800 локальних проєктів та використовує цифрову платформу для відстеження стану об’єктів, що відповідає принципам evidence-based governance.

Водночас формується нова архітектура міжрівневої співпраці між урядом, громадами та міжнародними фінансовими інституціями. Європейський інвестиційний банк уже профінансував близько 200 проєктів у 18 регіонах України на суму понад €99,6 млн, спрямованих не лише на відновлення, а на створення стійких систем із підвищеними стандартами безпеки [361]. У концепції ОЕСР «Architecture of Infrastructure Recovery» [201] підкреслено необхідність переходу від адміністративного управління до інтегрованого стратегічного планування з акцентом на ефективність, прозорість і довіру до управлінських рішень.

Сутність трансформації полягає у переході від управління «після події» до управління на основі прогнозу, коли рішення приймаються на базі цифрової аналітики, даних з сенсорних мереж і супутникового моніторингу. У 2024 р. у

Харківській області реалізовано пілотну систему «Резильєнтна громада», що об'єднує дані з безпілотних обстежень, SCADA-комплексів і супутникових знімків для прогнозування ризиків руйнування споруд. Завдяки цьому середній час реагування на аварійні події скоротився з 36 до 6 годин [327]. Таким чином, нова концепція публічного управління демонструє перехід від контрольного адміністрування до аналітичної координації, де інформація та взаємодія стають головним ресурсом.

Процес формування цієї моделі має етапний характер, у якому поступово відбувається ускладнення управлінських зв'язків і зміна самої управлінської парадигми – від реактивного реагування до аналітично-резильєнтного управління. Послідовність такої еволюції відображено на рис. 5.3, яка систематизує основні етапи розвитку публічного управління трансформацією критичної інфраструктури України.



Рис. 5.3. Етапи еволюції публічного управління трансформацією критичної інфраструктури України

Джерело: сформовано автором на основі [13; 16; 73]

Трансформація системи публічного управління у сфері критичної інфраструктури має еволюційний характер, що відображає поступову зміну

управлінського мислення - від реакції на кризу до управління ризиками та передбаченням сценаріїв розвитку. Зміни відбуваються не лише в інституційній структурі, а й у культурі прийняття рішень, що підтверджується конкретними прикладами реалізації нових управлінських практик.

Так, у межах реалізації проєкту Ukraine Rapid Damage and Needs Assessment (RDNA), розробленого спільно Світовим банком, ЄС та урядом України, запроваджено єдину методологію оцінювання руйнувань і відновлення, що охоплює понад 20 секторів інфраструктури - від енергетики до освіти та охорони здоров'я [345]. Цей підхід відповідає третьому етапу еволюції, коли відбувається інтеграція баз даних і створення спільної аналітичної рамки для ухвалення рішень.

На регіональному рівні ефективним прикладом реалізації аналітично-резильєнтного управління стала діяльність координаційного центру відновлення у Чернігівській області, який об'єднує представників державних структур, громад і донорів через цифрову платформу «RebuildChernihiv» [159]. Платформа дозволяє відстежувати хід реконструкції об'єктів у режимі онлайн, публікувати фінансові звіти й пріоритезувати відновлення відповідно до соціальної важливості об'єктів.

В енергетичному секторі, що є ключовим елементом критичної інфраструктури, Міністерство енергетики спільно з USAID та НЕК «Укренерго» у 2024 р. запровадили платформу Energy Resilience Dashboard, яка агрегує дані з понад 250 підстанцій і генераційних об'єктів [90]. Це дало змогу створити динамічну карту вразливості енергомереж, автоматично оновлювати інформацію після атак і оперативно визначати пріоритети для ремонтів. Такий підхід відображає перехід до четвертого етапу - аналітично-резильєнтного управління, заснованого на цифрових потоках даних і машинній аналітиці.

Ще одним прикладом поліцентричної взаємодії є спільна ініціатива «Safe Water for Ukraine», у межах якої понад 300 громад Дніпропетровської, Миколаївської та Херсонської областей отримали доступ до модульних систем очищення води, профінансованих у партнерстві ПРООН, уряду Японії та місцевих органів самоврядування [355]. Тут бачимо реалізацію принципу

спільного управління (co-governance), коли рішення ухвалюються не централізовано, а через взаємодію між державними й місцевими акторами.

Водночас аналітична спроможність поступово зміцнюється через освітні програми та розвиток управлінських кадрів. Зокрема, у 2024 р. Національне агентство з питань державної служби запустило навчальну програму «Crisis and Resilient Governance», у якій вже пройшли підготовку понад 600 державних службовців і керівників громад [207]. Це означає, що реформа має не лише технологічний, а й інституційно-культурний вимір - формування нової управлінської культури, здатної діяти в умовах ризику й невизначеності. Так, приклади сучасної практики підтверджують, що етапність, зображена на схемі 5.1, не є теоретичною конструкцією, а відображає реальні процеси трансформації управлінської системи України. Від реактивного реагування після 2014 р. до впровадження аналітичних платформ і партнерських мереж у 2023–2025 рр. - кожен етап поглиблює взаємодію, підвищує прозорість і забезпечує стійкість критичної інфраструктури як основи національної безпеки.

Формування теоретико-методологічних засад нової концепції публічного управління у сфері трансформації критичної інфраструктури зумовлене переходом від традиційної адміністративно-командної моделі до гнучкої, аналітичної та поліцентричної системи управління, що відповідає сучасним викликам безпеки, цифровізації й відбудови. Сучасні теоретичні підходи визначають, що публічне управління в умовах воєнних і поствоєнних ризиків має спиратися не лише на нормативну ієрархію, а на принципи мережевої взаємодії, довіри, системності та стійкості. Основою нової концепції є інтеграція таких напрямів, як resilience governance, adaptive governance, polycentric governance та data-driven public management, які забезпечують спроможність системи реагувати на непередбачувані події, адаптуватися до динаміки загроз і приймати рішення на основі достовірних даних. Науково-методологічна база нового управління також охоплює принципи доказового аналізу (evidence-based policy), соціальної координації (collaborative governance) і управління ризиками, що дозволяють переорієнтувати державне управління з контролю на аналітичне передбачення та запобігання кризам (табл.5.3).

Таблиця 5.3

Теоретико-методологічні підходи, що формують основу нової концепції публічного управління трансформацією критичної інфраструктури

Підхід	Ключові методологічні положення	Узагальнені приклади застосування
Resilience governance	Орієнтація на життєстійкість систем і безперервність послуг під час ударів	Запуск урядових механізмів Національної системи стійкості; розбудова центрів життєстійкості в громадах
Adaptive governance	Безперервні цикли «спостереження-аналіз-корекція», децентралізація повноважень	Корекція планів відновлення енергетики та мереж на підставі оперативних оцінок ушкоджень
Polycentric governance	Кілька центрів прийняття рішень, координація замість підпорядкування	Мультиагентна Донорська платформа: спільне планування потреб і портфельне фінансування
Data-driven public management	Рішення на основі даних, цифрові реєстри та платформи ПІМ	Екосистема DREAM як «єдине вікно» для управління публічними інвестиціями
Collaborative governance	Спільне управління за участі уряду, громад, бізнесу, IFI/донорів	Портфелі раннього відновлення інфраструктури за підтримки ООН та партнерів
Evidence-based policy	Стандартизовані методики оцінювання та KPI, зовнішній аудит	RDNA4: уніфікована методологія для 20+ секторів із кошторисами потреб [4]

Джерело: сформовано автором на основі [104; 134; 372]

Методологічною основою триконтурної Концепції виступає сценарне планування, яке дозволяє враховувати невизначеність середовища функціонування критичної інфраструктури та формувати управлінські рішення не на основі єдиного «оптимального» прогнозу, а через сукупність альтернативних сценаріїв розвитку подій. У межах запропонованого підходу доцільно розрізняти щонайменше чотири базові сценарії:

1) стабілізаційний – помірний рівень загроз, поступове відновлення та модернізація;

2) кризовий – періодичні атаки та локальні руйнування, що вимагають оперативного реагування та резервування;

3) надзвичайний – масовані удари по критичних об'єктах, що потребують негайної мобілізації ресурсів і тимчасового переходу до централізованого управління;

4) трансформаційний – постконфліктне відновлення з акцентом на інноваційну модернізацію та інтеграцію до європейських стандартів. Кожному сценарію відповідає власний набір управлінських інструментів, критеріїв пріоритизації та порогових значень індикаторів, що дозволяє системі публічного управління перемикатися між режимами функціонування без втрати керованості. Такий підхід відповідає принципам adaptive governance та resilience governance, закріпленим у міжнародній практиці управління критичною інфраструктурою, і дозволяє уникнути як надмірної централізації, так і неконтрольованої децентралізації в умовах кризи.

Resilience-підхід закріплений на рівні державної політики через затверджений План заходів із реалізації Концепції забезпечення Національної системи стійкості (розпорядження КМУ № 1025-р від 10.11.2023), що формує індикаторний підхід до готовності, запроваджує міжвідомчу координацію та навчання публічних службовців щодо дій у разі загроз і порушення вертикалі рішень [376]. Практичний сенс: стійкість із декларації перетворюється на операційний стандарт – з вимогами до підготовки персоналу, сценарного планування та підтримання критичних функцій громад (енергія, вода, зв’язок, укриття).

Adaptive governance реалізується як безперервна петля коригування планів відновлення відповідно до змін ризиків. Енергетичні оператори та органи влади у 2024–2025 рр. переходили від «ремонту після атаки» до превентивного посилення вузлів мереж і балансування імпортом/експортом електроенергії: за оцінкою IEA (жовтень 2025 р.), у 2024 році імпорт електроенергії досяг рекордних 4 436 ГВт·год, що відображає втрати внутрішньої генерації та потребу в оперативних регулюваннях попиту/пропозиції [35]. Додатково практики «адаптивного планування» закріплено через фінансово-технічні документи системного оператора (оновлення інтеграції з ENTSO-E, пріоритети модернізації мереж і ризик-менеджмент) [117]. Узагальнення: адаптивність проявляється не одноразовими «переплануваннями», а регулярною ревізією планів під фактичні ушкодження, сезонні ризики та можливості імпортної підтримки.

Polycentric governance працює через Українську донорську платформу (колишня Multi-agency Donor Coordination Platform), що з 26.01.2023 координує бюджетну підтримку, інвестпроєкти та техдопомогу між ЄС, G7, МФО й урядом – із прозорими мандатами та спільними пріоритетами в коротко- і середньостроковому горизонті [184; 273]. Це зменшує транзакційні витрати й ризики дублювання програм, переводячи допомогу в режим портфельного управління («одна країнова стратегія - багато виконавців»). Узагальнення: поліцентричність - це узгодженість стратегій і бюджетів без жорсткої ієрархії, але з чіткою підзвітністю.

Data-driven public management задає операційну тканину рішень. Екосистема DREAM документує повний життєвий цикл публічних інвестицій (ідентифікація – підготовка – фінансування – закупівлі – реалізація – моніторинг) і, за оцінкою Open Contracting Partnership (липень 2025 р.), перебуває на етапі масштабування як національна платформа ПІМ; уже проведено навчання 1500+ представників восьми регіонів перед розширенням на всю країну [335]. На енергетичному плечі data-driven-підхід підсилено міжурядовою Угодою про співпрацю зі стійкості енергосистеми (грудень 2024 р.), де зафіксовано пріоритети відновлення інфраструктури, кіберстійкість і координацію партнерів [199].

Collaborative governance проявляється у портфелях раннього відновлення, де уряд і громади співпрацюють із ПРООН та партнерами над критичною соціальною інфраструктурою. У 2024 році за підтримки ПРООН завершено 21 інфраструктурний об’єкт (медичні центри, освітні заклади, системи водопостачання, житло), з безпосередньою вигодою для 25 000+ осіб; паралельно в дев’яти областях створювалися бізнес-хаби та центри навчання для відновлення зайнятості [267]. Окремі портфелі підготовлені громадами (Сумська, Чернігівська, Харківська, Чернівецька області) у партнерстві з ПРООН і за підтримки уряду Японії - як локальні кейси співуправління з відкритими матеріалами [322].

Evidence-based policy забезпечує верифікаційну основу для рішень. Документ RDNA4 (лютий 2025 р.) систематизує методологію оцінювання

пошкоджень і потреб у 20+ секторах за період лютий 2022 - грудень 2024 рр., задаючи фінансові «вилки» й пріоритети для уряду та донорів у середньостроковій перспективі [241]. Ця ж логіка лягає в рамку донорської платформи, яка публічно підтвердила мандат на безперервну координацію фінансування відновлення та реконструкції у 2025 р. і далі [273]. Узагальнення: доказовість - це єдині правила рахунку + спільні базові дані, що уможливлюють вимірюваність ефективності та корекцію політик.

Інтеграція зазначених теоретико-методологічних підходів формує нову управлінську архітектуру, у якій публічне управління у сфері трансформації критичної інфраструктури функціонує як єдина екосистема взаємопов'язаних елементів. Кожен підхід виконує специфічну функцію: resilience – задає стійкі орієнтири й нормативну рамку; adaptive – забезпечує гнучкість і здатність системи реагувати; polycentric – узгоджує взаємодію багатьох центрів рішень; data-driven – наповнює управління об'єктивною інформацією; collaborative – залучає партнерів і громади; evidence-based – гарантує відтворюваність і підзвітність політики. Така взаємодія формує динамічний контур «дані -рішення – стійкість», який лежить в основі сучасної концепції публічного управління у післявоєнний період.

Як показано на рис. 5.4, нова управлінська екосистема функціонує як динамічна петля зворотних зв'язків, де кожен рівень підсилює інший. Resilience формує «каркас стійкості» через нормативну політику, стандарти готовності та індикатори критичних функцій. Adaptive governance наповнює цю структуру гнучкістю, забезпечуючи корекцію рішень у реальному часі під впливом даних і ризиків. Polycentric governance розгортає управління у вигляді мережі, де різні центри – уряд, громади, міжнародні партнери - синхронізують ресурси, уникаючи дублювання.

Data-driven public management створює основу цифрової аналітики, що зменшує інформаційні розриви між центрами прийняття рішень і дозволяє прогнозувати втрати, оптимізувати ресурси та контролювати фінансування. Collaborative governance забезпечує горизонтальну взаємодію, коли громади, донори й бізнес виступають не лише виконавцями, а й співвиробниками рішень,

що особливо важливо у відновленні регіональної соціальної інфраструктури. Нарешті, evidence-based policy гарантує перевірюваність усіх процесів, інтегруючи результати моніторингу у наступні цикли стратегічного планування. Таким чином, ця блок-модель демонструє перехід від ієрархічного управління до поліцентричної системи із взаємопідсилюваними елементами, у якій дані, довіра та адаптивність є ключовими драйверами трансформації критичної інфраструктури.

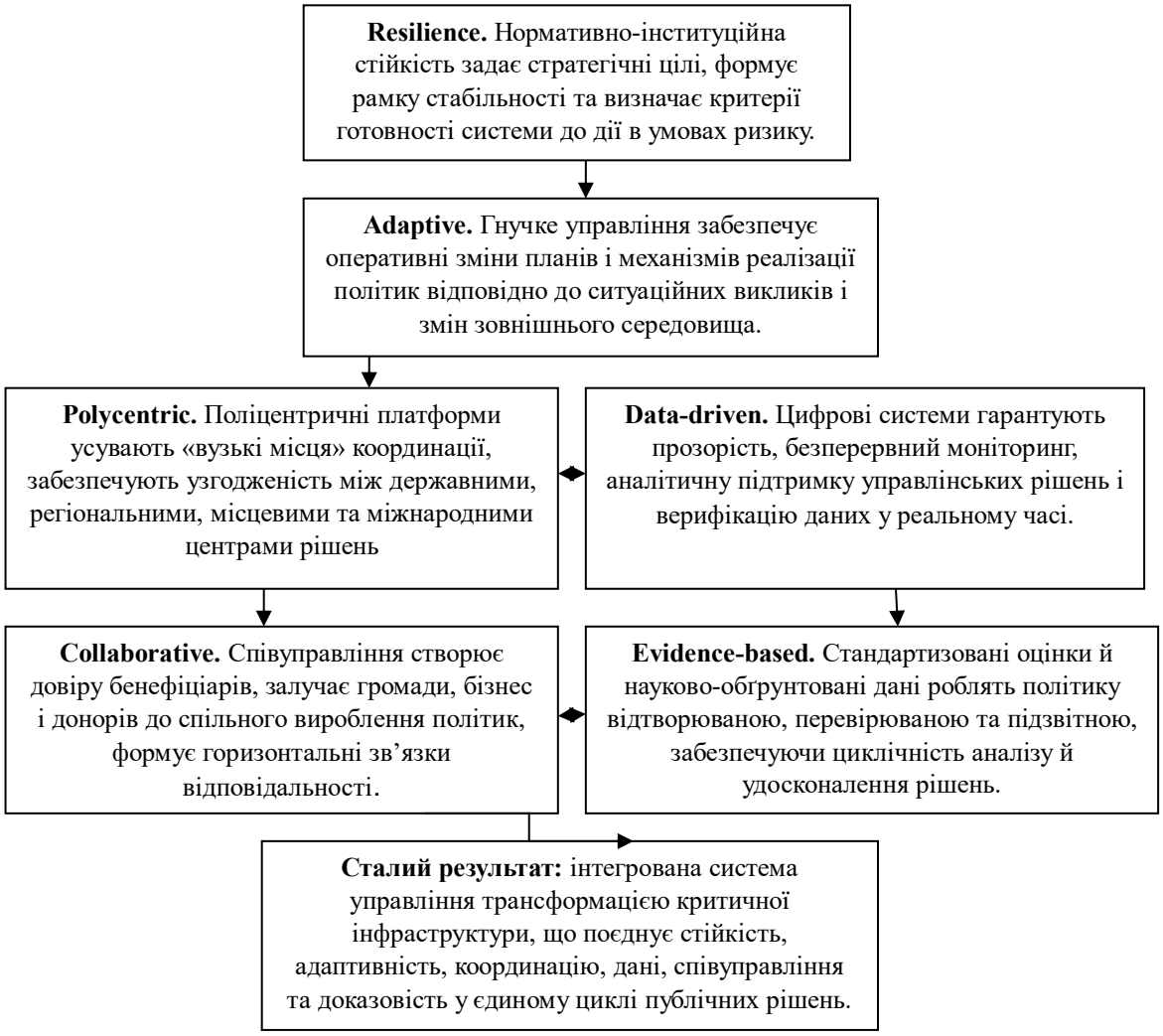


Рис. 5.4. Єдина екосистема публічного управління трансформацією критичної інфраструктури*

*Джерело: сформовано автором на основі [89; 96; 128]

Така концептуальна рамка відповідає міжнародним принципам resilience governance і забезпечує можливість масштабування рішень як на національному, так і на регіональному рівнях.

Воєнна реальність надала цим засадам конкретного змісту. По-перше, стратегічна безпека та екологічність стали взаємопов'язаними умовами проєктування: за оцінкою RDNA-4, потреби відновлення та модернізації становлять $524 млрд на десятиріччя, причому цільові напрями включають енергоефективність і зниження вуглецевої інтенсивності, що вбудовує «зелені» критерії у відбір проєктів на всіх рівнях [341]. По-друге, адаптивність закріпилася в енергетичному управлінні: за аналітикою IEA, у 2025 р. операційний баланс підтримується через динамічне коригування генерації та режимів імпорту/експорту, з постійним оновленням пріоритетів ремонту під впливом атак і дефіцитів [67; 360]. По-третє, партнерство й міжрівнева взаємодія набули інституційної форми завдяки Україні Донорській платформі ЄС–G7, що синхронізує бюджетну підтримку, інвестиції та техдопомогу з підтвердженими зовнішніми потребами на 2025 р. і високою часткою покриття за рахунок ЄС - це зменшує транзакційні витрати й запобігає дублюванню програм [170].

Практичний вимір гуманітарності та територіальної солідарності проявляється у зимовій підтримці громад і забезпеченні безперервності критичних функцій. ЄС у червні 2024 р. мобілізував понад 1000 генераторів із резервів rescEU для стабілізації лікарень, систем водопостачання й об'єктів теплопостачання — приклад поєднання стратегічної безпеки, партнерства і міжрівневої взаємодії в «пакеті» рішень [342]. Загальна гуманітарна картина 2025 р. засвідчує масштаб адресних потреб: за даними OCHA, допомоги потребують мільйони людей, що вимагає інклюзивного налаштування портфелів відбудови та пріоритезації вразливих груп [123]. У секторі освіти UNICEF фіксує тривалу напругу: одночасно із розширенням доступу до безпечного навчання триває відновлення освітньої інфраструктури та укриттів, що відображає гуманітарний і безпековий фокус реконструкції [100].

Кіберстійкість перетворилася на «несучу балку» управлінської архітектури. CERT-UA у 2024 р. опрацювала 4315 кіберінцидентів, а державна аналітика фіксує еволюцію технік атак і необхідність постійного моніторингу та координації реагування з європейськими командами; це безпосередньо накладається на енергетику, транспорт і телеком, змушуючи інтегрувати SLA

кібербезпеки в контракти, резервування даних і відмовостійкі сервіси [185; 299]. У свою чергу, когнітивна синергія матеріалізується в спільних дослідницько-управлінських ініціативах: рамки відновлення, які підтримує ПРООН, включають методичні блоки з ризик-менеджменту, розмінування, цифрового моніторингу та участі громад - це переводить знання, дані й локальний досвід у прикладні механізми політики [348].

Фактичні тренди 2024–2025 рр. демонструють, що адаптивність і екологічність змикаються з енергетичною безпекою: за офіційною довідкою ЄС з цивільного захисту, до початку 2025 р. через логістичні хаби доставлено понад 155 тис. тонн допомоги, включно з енергетичним обладнанням, тоді як оператори маневрують між імпортом, відновленням генерації та децентралізацією потужностей [280; 328; 353]. На ринку газу спостерігається «плаваючий» імпорт для досягнення сезонних цілей заповнення сховищ; системні удари по видобутку та інфраструктурі періодично підвищують потребу в додаткових закупівлях, що підсилює важливість партнерських фінансових інструментів і планів запасів [182; 333]. Усе це підтверджує: нові принципи не є «надбудовою», а частиною механіки управління - вони визначають, як саме проєктуються, фінансуються, відстежуються та коригуються рішення в реальному часі.

Так, базова сімка (прозорість, підзвітність, інклюзивність, міжрівнева взаємодія, партнерство, цифрова відкритість, стратегічна безпека) формує каркас керованості; додані війною засади (екологічність, адаптивність, кіберстійкість, гуманітарність, територіальна солідарність, етичність/антикорупційна відкритість) забезпечують життєстійкість і легітимність; когнітивна синергія «зшиває» їх через моделювання та доказовий аналіз. У підсумку формується еволюційна, поліцентрична і водночас керована екосистема публічного управління, що поєднує випереджальне передбачення ризиків з прозорою реалізацією та перевірюваною віддачею для громад.

У сучасній логіці публічного управління трансформацією критичної інфраструктури відбувається перехід від фрагментарних рішень до інтегрованого циклу, де дані, координація, цифрові процеси, адаптаційні

механізми та оцінювання замикаються у відтворювану управлінську петлю. Цей перехід не зводиться до технічної «оцифровки» - він означає зміну архітектури відповідальності: об’єктивна діагностика визначає пріоритети, координація синхронізує ресурси між рівнями влади та донорами, цифровізація забезпечує прозорість і швидкість, адаптація підтримує керованість в умовах невизначеності, а оцінювання результативності перетворює політику на доказовий процес із постійним зворотним зв’язком. У такій системі кожен етап має власні інструменти, джерела даних і стандарти верифікації, що дозволяє переходити від реактивних дій до випереджального «roadmap»-управління (табл. 5.4).

Таблиця 5.4

Концептуальна логіка становлення інтегрованої системи публічного управління трансформацією критичної інфраструктури*

Етап	Зміст і ключові механізми	Очікуваний результат / ефект
Діагностика	Мультиджерельний збір і просторовий аналіз (супутникові зйомки, швидке картографування наслідків, галузеві реєстри, аудит пошкоджень та ризиків)	Об’єктивна картина втрат і вразливостей; пріоритизація портфелів відновлення
Координація	Узгодження планів і фінансування між урядом, громадами, донорами; єдині протоколи та дорожні карти інвестицій	Усунення дублювання, синхронізація ресурсів і термінів
Цифровізація	Інтероперабельні платформи для «планування–закупівель–виконання–звітності», аналітичні модулі та відкриті дані	Прозорість, прискорення рішень, контроль якості виконання
Адаптація	Сценарне управління й гнучка корекція планів на основі поточних даних (енергетика, логістика, гуманітарні потреби, кіберризики)	Стійкість сервісів, оптимізація витрат і часів простою
Оцінювання результативності	KPI, зовнішній моніторинг, ризик-індикатори закупівель, аудит впливу та суспільної віддачі	Відтворюваність політики, підзвітність, корекція «roadmap»

Джерело: сформовано автором на основі [11;164; 271; 303]

На етапі діагностики вирішальну роль відіграє оперативна дистанційна зйомка і швидке картографування: активування сервісів Copernicus EMS для надзвичайних ситуацій забезпечує офіційні карти розливів і пошкоджень

упродовж 24–48 годин, що безпосередньо підживлює відбір першочергових об’єктів і маршрути логістики [236]. Паралельно, нові дослідження зі світовою вибіркою розмічених зруйнувань будівель покращують алгоритмічну точність оцінок на місцевому рівні, дозволяючи калібрувати планування відновлення на основі зіставних метрик пошкоджень і знищення [340].

Координація переноситься з площини «узгоджувальних нарад» у площину правил і спільних фінансових рамок. Протягом 2024–2025 рр. під парасолькою Ukraine Facility ЄС схвалено «Ukraine Plan» як чотирирічну реформаторсько-інвестиційну стратегію; механізм передбачає поетапне фінансування залежно від виконання індикаторів, що дисциплінує розклад пріоритетних проєктів і синхронізує донорські інструменти з державними пріоритетами [339]. Окремі звіти Єврокомісії фіксують виконані кроки плану та відповідні транші, що надає координації вимірюваної «шкали поступу» і спрощує перерозподіл ресурсів між секторами [366].

На рівні цифровізації критичним є замикання всього циклу публічних фінансів у прозорі дані. Екосистема Prozorro/DOZORRO поєднує електронні закупівлі з громадським моніторингом: у 2025 р. DOZORRO випустила методичні настанови, як проводити предметний нагляд за тендерами так, щоб впливати на бюджетну ефективність (від аналізу тендерної документації до подання обґрунтованих скарг) [331]. Додатково, аналітика ЄБРР показує, що ризик-індикатори (ex ante) та ризик-моніторинг у Prozorro з 2018/2021 рр. знижують імовірність зловживань і підвищують відповідність стандартам відкритих контрактних даних - це перетворює цифрову прозорість на інструмент управління до, а не після факту [178].

Адаптація наочно проявляється в енергетиці: ENTSO-E спочатку підвищила комерційні ліміти експорту до України/Молдови до 2 100 МВт на зиму 2024/25, а 18 червня 2025 р. запустила нову процедуру обрахунку пропускної здатності на кордоні UA–MD із щомісячним переглядом TSO - це дає змогу оперативно коригувати обміни залежно від інцидентів та ремонтів, зберігаючи системну безпеку [206; 334]. На практиці це означає, що регіональні графіки ремонтів і плани генерації можуть підлаштовуватися під динаміку атак

без «ручного» перегляду всієї політики - механізм працює як вбудований регулятор адаптивності.

Аспект кіберстійкості формує «несучу балку» цифрових сервісів: у жовтні 2025 р. ЄС та Україна на четвертому Кібердіалозі підтвердили поглиблення операційної співпраці (включно з обміном практиками реагування та нарощенням спроможностей), що підвищує здатність утримувати безперервність державних платформ і критичних сервісів у періоди пікових загроз [205]. Ширший контекст задає ENISA Threat Landscape 2025, який документує ескалацію DDoS, зловмисної активності та міждержавних впливів у 2024/25 рр., тим самим обґрунтовуючи політику резервування даних і SLA кіберзахисту в контрактах реконструкції [169].

Нарешті, оцінювання результативності виходить за межі «виконання плану» і переходить до перевірки суспільної віддачі. Професійні посібники DOZORRO 2025 навчають, як вибудовувати доказову ескалацію виявлених ризиків (від ідентифікації аномалій у даних до звернень у контролюючі органи), а галузеві аналітики демонструють, що ризик-орієнтований підхід у закупівлях зменшує транзакційні витрати і підвищує якість виконання договорів [178; 331]. В енергетиці метрика результативності доповнюється показниками системної стійкості - доступні потужності для перетоків, час відновлення після інцидентів, частота коригувань на підставі нової TSO-процедури [301]. У гуманітарній площині координаційні сторінки ЄК щодо цивільного захисту консолідують «паспорт країни» з потоками допомоги та сезонними пріоритетами, що дозволяє уряду і донорам спільно тестувати, чи дійсно інвестиції закривають найбільш критичні «вузькі місця» [169].

Узагальнення практичних і аналітичних спостережень дозволяє візуалізувати нову архітектоніку управління трансформацією критичної інфраструктури не як послідовність окремих процедур, а як замкнену операційну систему “дані – координація – цифра – адаптація – результат”, де кожен елемент живить наступний і водночас отримує зворотний зв’язок. Така система функціонує як динамічна «рамка рамок» - вона не замінює наявні моделі, а інтегрує їх у єдиний управлінський контур, де інформаційні, нормативні,

фінансові та соціальні потоки узгоджуються в реальному часі (рис. 5.5.). Інституційний контур запропонованої концепції потребує окремого посилення через створення спеціалізованих координаційних структур, наділених мандатом на міжвідомчу взаємодію та оперативне прийняття рішень. Йдеться про формування національного офісу управління трансформацією критичної інфраструктури, який би виконував функції стратегічного планування, координації ресурсів, моніторингу виконання та оцінювання результатів.



Рис. 5.5. Інтегрована логіка публічного управління трансформацією критичної інфраструктури (операційна "петля управління")*

*Джерело: власна розробка автора

Такий офіс має поєднувати представників ключових міністерств, регуляторів, місцевих громад, приватного сектору та міжнародних партнерів, діючи на принципах поліцентричності та спільного управління. Його завданнями мають стати: розробка та оновлення сценаріїв розвитку інфраструктури; координація портфелів проєктів відновлення та модернізації; забезпечення інтероперабельності даних між відомствами; організація публічних консультацій і залучення стейкґолдерів; проведення регулярних «performance reviews» із

залученням незалежних аудиторів. Досвід функціонування Державного агентства відновлення та розвитку інфраструктури України, а також координаційних центрів у Чернігівській та Харківській областях засвідчує ефективність такої моделі, однак її масштабування на національний рівень потребує чіткого нормативного закріплення повноважень, ресурсного забезпечення та механізмів підзвітності.

У цій системній конфігурації діагностика забезпечує вхідні дані (verifiable data), координація - нормативно-організаційне узгодження ресурсів, цифровізація створює технологічний каркас, адаптація перетворює управління на реактивно-прогностичне, а оцінювання результативності гарантує публічну відтворюваність рішень. На відміну від традиційних вертикалей, така модель функціонує як відкрита петля даних і довіри, де ключовим ресурсом стає не обсяг фінансування, а швидкість циркуляції достовірної інформації. Вона поєднує аналітичну глибину діагностики з етичними принципами прозорості й відповідальності, створюючи передумови для стратегічної дорожньої карти (“roadmap”) реконструкції, у якій управління виступає не як контроль, а як постійне

Реалізація нової концепції державного управління в Україні зіштовхується з комплексом взаємопов’язаних проблем, які мають системний, глибинно-інституційний характер і суттєво обмежують ефективність реформування. Їхній зміст виявляється не лише у технічних чи процедурних вадах, а у самій логіці взаємодії нормативних, кадрових, організаційних і комунікаційних механізмів, що формують основу державної політики.

Однією з фундаментальних проблем є нормативна неузгодженість. Незважаючи на значний масив ухвалених стратегічних документів, між ними зберігаються численні суперечності [44]. Норми законів, підзаконних актів та урядових постанов часто формувалися у різні періоди під впливом різних політичних і економічних контекстів, тому вони не узгоджені між собою за термінологією, структурою цілей та механізмами реалізації. Відсутність єдиної методології оцінювання політик призводить до того, що навіть реформи з подібними завданнями мають різні критерії результативності. Це створює

правову невизначеність для виконавців на місцях, посилює ризик вибіркового тлумачення норм і породжує ситуацію, коли одна й та сама дія може бути оцінена як ефективна в одному відомстві і як нецільова - в іншому. Такий стан підриває принципи узгодженості політик (*policy coherence*) і зменшує керованість державного розвитку [340].

Не менш критичною є проблема дублювання функцій між органами виконавчої влади, місцевого самоврядування та спеціалізованими агентствами [73]. Внаслідок невизначеності меж відповідальності часто спостерігається накладання повноважень — наприклад, у сферах соціального захисту, екологічного контролю, управління об’єктами критичної інфраструктури чи публічних закупівель [331]. Відсутність механізмів “розв’язування функціональних вузлів” призводить до конкуренції відомств за ресурси та до втрати ефективності через паралельні управлінські процеси. Коли одна функція виконується кількома структурами, виникає ефект «розмитої відповідальності», що унеможливлює притягнення до персональної або інституційної відповідальності у разі неефективності. З точки зору управлінської теорії, це є проявом ентропійної фрагментації державного апарату, яка руйнує принцип субсидіарності та підриває вертикаль виконавчої дисципліни [376].

Вагомим обмеженням залишається недостатня кадрова спроможність державного сектору. Сучасна концепція передбачає використання аналітичних, цифрових, комунікативних і проєктних компетентностей, однак система підготовки та добору кадрів не відповідає цим вимогам [35]. Державна служба переважно зберігає адміністративно-бюрократичну модель, у якій превалює формальне дотримання процедур замість досягнення результатів. Плинність кадрів, політичні призначення без належної професійної оцінки, відсутність системи безперервного навчання та інституційної пам’яті знижують стабільність реалізації політик.

Недостатня координація між рівнями влади - ще одна структурна вада. Формально реалізована децентралізація не супроводжується адекватним розподілом функцій і ресурсів між центральними, регіональними та місцевими органами [49]. Центральні відомства часто зберігають контроль над ресурсними

потоками, водночас перекладаючи відповідальність за результати на громади. Координаційні ради, міжвідомчі платформи та обласні адміністрації не мають дієвих інструментів інтеграції даних і планів розвитку [90; 199]. Це створює дисбаланс у політико-адміністративній вертикалі: державна політика набуває директивного характеру, а місцеві ініціативи - декларативного.

Окремо слід підкреслити слабкість комунікації з громадами, що має як технічні, так і соціально-психологічні виміри [322]. Відсутність сталої практики публічного діалогу, електронних консультацій, відкритих панелей моніторингу та платформ спільного планування формує відчуження громадян від процесу прийняття рішень [366]. У багатьох громадах стратегічні документи розробляються без залучення стейкґолдерів — бізнесу, громадських організацій, професійних асоціацій. Це позбавляє реформи легітимності на рівні місцевих соціальних систем і породжує інерцію «пасивного сприйняття», коли громадяни не ідентифікують державну політику як власний інтерес.

Не менш значущою є проблема відсутності інтегрованої системи моніторингу та оцінювання ефективності. Збір, оброблення та використання даних залишається розрізненим: статистичні служби, міністерства та регіональні структури застосовують різні методики, а інформаційні системи не інтероперабельні [96]. У результаті аналітичні висновки формуються на основі застарілих або неповних даних. Без системного *data-driven* підходу управлінські рішення залишаються реактивними, а не прогнозними, що позбавляє державну політику адаптивності до динаміки соціально-економічних процесів.

Крім того, реалізація концепції ускладнюється інституційною інерцією [48]. Навіть за наявності сучасних стратегій, старі управлінські практики, засновані на вертикальному контролі та процедурному формалізмі, відтворюють себе у нових формах [44]. Це проявляється у тому, що інноваційні елементи реформ - цифровізація, оцінювання за результатами, міжсекторальна взаємодія - впроваджуються фрагментарно, як пілотні проєкти, а не як системні механізми. Відсутність мотивації до інституційного навчання й внутрішнього самовдосконалення створює парадокс: нова концепція реалізується старими засобами, що нівелює її потенціал.

Узагальнюючи, можна стверджувати, що ключові проблеми реалізації нової концепції не є ізольованими - вони формують єдиний контур інституційної слабкості, у якому нормативна фрагментарність породжує функціональне дублювання, кадрова нестача - управлінську інерцію, а слабка комунікація - соціальну недовіру [44; 128]. Подолання цих бар'єрів потребує не лише оновлення нормативно-правової бази, а й формування інтегрованої системи управлінських компетентностей, стандартизованих процедур координації між рівнями влади та механізмів відкритої участі громад у стратегічному плануванні [49]. Лише за умови інституційного узгодження, професійного кадрового забезпечення та цифрової інтеграції можливо перетворити нову концепцію з декларативного документа на дієвий інструмент управління сталим розвитком держави.

Узагальнюючи, можна стверджувати, що ключові проблеми реалізації нової концепції не є ізольованими - вони формують єдиний контур інституційної слабкості, у якому нормативна фрагментарність породжує функціональне дублювання, кадрова нестача - управлінську інерцію, а слабка комунікація - соціальну недовіру. Подолання цих бар'єрів потребує не лише оновлення нормативно-правової бази, а й формування інтегрованої системи управлінських компетентностей, стандартизованих процедур координації між рівнями влади та механізмів відкритої участі громад у стратегічному плануванні. Лише за умови інституційного узгодження, професійного кадрового забезпечення та цифрової інтеграції можливо перетворити нову концепцію з декларативного документа на дієвий інструмент управління сталим розвитком держави.

Запровадження нової концепції публічного управління доцільно здійснювати через узгоджений пакет правових, інституційних і технологічних рішень, який зменшує нормативну фрагментацію, підсилює аналітичну спроможність, професіоналізує державну службу, забезпечує цифрову інтероперабельність та переводить моніторинг результатів у режим доказовості й публічної підзвітності. На законодавчому рівні слід кодифікувати принципи узгодженості політик і субсидіарності, гармонізувати терміни та дефініції між законами й підзаконними актами, закріпити обов'язковість попередньої та

післядії оцінки впливу (ex-ante/ex-post), «сонсет-клаузи» для нормативів, що потребують регулярного перегляду, і єдину процедуру публічних консультацій з мінімальними стандартами залучення стейкґолдерів. Необхідно чітко розмежувати повноваження центральних і місцевих органів, ліквідувавши дублювання функцій через типовий класифікатор адміністративних послуг і регламентовані міжвідомчі угоди (SLA/MoU), а також юридично зобов'язати всі органи влади дотримуватися стандартів інтероперабельності та «once-only principle», призначивши формальних кураторів даних (data stewards) і відповідальних за управління якістю даних у кожній установі.

Розвиток аналітичної інфраструктури має спиратися на побудову державної «data fabric»: реєстрово-орієнтовані довірені джерела, уніфіковані моделі даних і метаданих, керування головними даними (MDM), каталогізацію та контроль якості, а також безпечні дослідницькі середовища для міжвідомчого аналізу з чіткими режимами доступу. Варто інституціоналізувати процес «дані - інсайт - рішення»: створити урядовий аналітичний хаб із функціями економетричного моделювання, прогнозування, просторової аналітики та швидких політичних експериментів; запровадити стандарти відтворюваності (version control, audit trails), управління модельним ризиком і незалежну валідацію алгоритмів. Фінансова архітектура має підтримувати аналітику: програмно-цільовий метод з результатними індикаторами, портфельне управління проєктами з «stage-gate» і резервами на швидкі пілоти, умовні трансферти громадам, прив'язані до досягнутих результатів.

Система управлінської освіти потребує переходу від формальної підвищувальної кваліфікації до компетентнісної моделі. Доцільно запровадити обов'язкові мікрокваліфікації для державних службовців з даних і доказових політик (data literacy, policy evaluation, product management, цифрові закупівлі), створити національну школу публічного лідерства з модульною програмою (стратегія, фінанси, регуляторна політика, етика та відкрите врядування), механізми міжсекторальних стажувань і внутрішні «communities of practice». Кадрові процедури варто пов'язати з результатами: прозорі кар'єрні траєкторії,

оплата за компетентності й внесок у показники відомства, інституційна пам’ять через наставництво та «knowledge transfer» під час ротацій.

Цифрова взаємодія має будуватися за принципами «API-first», «mobile-by-default» і «service-as-a-product». Потрібні реєстрова шина даних і шлюзи для безпечного обміну, єдині дизайн-стандарти державних послуг, обов’язкова доступність (WCAG), багатоканальний зворотний зв’язок та інструменти співучасті громадян: електронні консультації, краудсорсинг рішень, партисипативне бюджетування, кабінети отримувачів послуг із трекінгом статусів. Кібербезпека і приватність - «by design»: класифікація інформаційних активів, моделі загроз, багаторівнева автентифікація, регулярні пентести, прозорі політики використання даних, незалежні комітети з етики даних для алгоритмічних рішень. Державні закупівлі слід адаптувати під GovTech-цикли: рамкові угоди, пісочниці для інновацій, поетапні контракти за результатами з чіткими метриками сервісної якості.

Моніторинг та оцінювання результатів мають перейти від формальної звітності до управління за цілями та доказами. Доцільно затвердити єдину логіку «теорії змін» для програм, стандартизувати систему індикаторів результату й впливу з базовими та цільовими значеннями, розгорнути публічні панелі моніторингу в реальному часі та щоквартальні «performance reviews» із залученням незалежних аудиторів. Для ключових реформ слід використовувати контрфактичні підходи там, де можливо (квазіексперименти, RCT-елементи), швидкі цикли оцінювання («rapid-cycle evaluation») і механізми корекції політик на основі даних. Зовнішній контур підзвітності забезпечується регулярними публічними звітами з відкритими наборами даних, «citizen scorecards» і процедурою реагування на запити громад.

Щоб перетворити ці напрями на керовану програму, потрібні операційні механізми: урядовий офіс впровадження з мандатом на міжвідомчу координацію, дорожня карта з пріоритизацією і залежностями, портфельне управління та ризик-реєстр, зміни в регламенті КМУ для швидших погоджень цифрових інтеграцій, а також комунікаційна стратегія, що пояснює «цінність для громадянина» кожного етапу. Така конфігурація синхронізує законодавство з

технологіями, підсилює аналітичні й кадрові спроможності, підвищує якість цифрових сервісів і робить результати політик вимірюваними та публічно верифікованими.

З огляду на складність переходу до нової моделі публічного управління, важливо не лише визначити стратегічні напрями, а й сформувати операційну послідовність дій, яка дозволить перетворити рекомендації на керований процес реформування. Покрокова схема впровадження виступає своєрідним «механізмом розгортання концепції», що поєднує стратегічну логіку з інституційними та технологічними інструментами. Такий підхід дає змогу уникнути хаотичності дій, забезпечити етапність і зворотний зв'язок, а також закріпити досягнуті результати у нормативному й організаційному полі (рис. 5.6.).



Рис. 5.6. Схема поетапного впровадження нової концепції публічного управління*

*Джерело: власна розробка автора

На етапі діагностики здійснюється системне оцінювання стану критичної, транспортної, соціальної та енергетичної інфраструктури з урахуванням просторових ризиків і ступеня руйнування. Це включає аудит технічного

ресурсу, логістичних зв'язків, нормативного забезпечення та фінансових потоків. Очікувано, формування інтегрованої карти стану об'єктів дозволить підвищити точність планування відбудови на 70–80 %, скоротивши дублювання проєктів і помилки у визначенні пріоритетів.

Етап проєктування спрямований на створення цільової архітектури управління інфраструктурою, у межах якої визначаються пріоритетні кластери - транспортно-логістичний, енергетичний, водний, цифровий та соціальний. У кожному кластері формуються цільові програми з єдиними критеріями ефективності, зокрема індексом відновлення (Recovery Index) та показником соціально-економічної віддачі. Очікується, що впровадження стандартизованої архітектури скоротить терміни узгодження проєктів щонайменше на третину та зменшить розрив між етапами планування і реалізації.

Під час нормативної узгодженості головним завданням є синхронізація галузевих норм (ДБН, технічних регламентів, стандартів енергоефективності) з європейськими вимогами та принципами «відбудови з підвищенням якості» (build back better). Йдеться про встановлення єдиних критеріїв оцінки безпеки, довговічності й екологічності об'єктів, а також механізмів контролю використання ресурсів. Очікувано, це зменшить кількість нормативних колізій у сфері будівництва на 40–50 % і забезпечить правову визначеність для інвесторів.

Етап цифровізації передбачає створення інтегрованої інформаційної платформи управління інфраструктурою - національного «цифрового двійника» територій, що поєднує ГІС, будівельні реєстри, супутниковий моніторинг і модулі прогнозування ризиків. Такий інструмент забезпечує прозорість усіх етапів - від проєктування до експлуатації, зменшує корупційні ризики та оптимізує розподіл ресурсів. Очікується, що використання цифрових моделей дозволить скоротити тривалість планування об'єктів на 25 % і підвищити точність розрахунків витрат на 15–20 %.

Кадрове підсилення має ключове значення, адже ефективність інфраструктурної політики залежить від наявності фахівців нової генерації - інженерів, урбаністів, економістів, аналітиків, здатних працювати у цифровому середовищі. Розгортання системи мікрокваліфікацій у сфері управління

проєктами відбудови, BIM-технологій, енергоаудиту та ризик-менеджменту дозволить створити кадровий резерв, який забезпечить автономність регіонів у прийнятті технічно виважених рішень. Очікувано, до кінця другого року впровадження частка управлінців із оновленими компетенціями має зрости до 60 %, а рівень технічних помилок у проєктній документації - зменшитися вдвічі.

Етап пілотування забезпечує апробацію моделі в окремих областях або секторах - наприклад, у відновленні мостів, водопостачання чи мережевої енергетики. Важливим є використання комбінованого фінансування (державного, муніципального, донорського) та моніторинг ефектів у реальному часі. Очікується, що понад 50 % пілотних рішень будуть масштабовані, а ефективність інвестиційних витрат на цих ділянках підвищиться на 20–25 % порівняно з традиційними підходами.

Під час масштабування апробовані практики переходять у національний рівень, інтегруються в державні програми розвитку регіонів і підкріплюються довгостроковим фінансуванням через механізми цільових фондів. На цьому етапі формується єдиний портфель інфраструктурних проєктів, де відбір ґрунтується на прозорих критеріях - соціальному ефекті, екологічній відповідності, мультиплікаторі зайнятості. Очікувано, рівень ефективності витрачання державних коштів під час масштабування зросте щонайменше на 30 %, а залучення приватного капіталу - на 15 %.

Завершальний етап - моніторинг і зворотний зв’язок - передбачає створення системи безперервного аналізу технічного стану об’єктів, виконання робіт і досягнення цілей відновлення. Національна аналітична платформа дозволяє об’єктивно вимірювати прогрес і прогнозувати потреби у фінансуванні чи модернізації. Очікувано, за перші три роки реалізації системи тривалість циклу прийняття коригувальних рішень скоротиться з шести до двох місяців, а рівень прозорості звітності за інфраструктурними проєктами перевищить 90 %.

Реалізація цієї схеми формує циклічну модель управління інфраструктурою, де кожен етап підкріплює попередній, створюючи механізм самонавчання системи. У результаті держава отримує не просто відновлену матеріальну базу, а керовану, цифрово інтегровану та кадрово підсилену

інфраструктуру, здатну підтримувати економічну стійкість і соціальну згуртованість. Очікуваним підсумком упровадження концепції є підвищення індексу якості інфраструктури (Global Competitiveness Index) України не менш ніж на 0,4 пункту протягом п’яти років, а також зменшення регіональних диспропорцій у доступі до транспортних, енергетичних і цифрових ресурсів щонайменше на 25 %.

Очікувана ефективність запропонованої Концепції визначається не лише кількісними показниками відновлення, а й якісними змінами в самій логіці публічного управління. Перехід від ієрархічної вертикалі до поліцентричної мережі, від фрагментарної звітності до інтегрованих цифрових платформ, від реактивного реагування до сценарного планування та адаптивного управління – усе це формує нову управлінську культуру, здатну діяти в умовах постійної невизначеності. Водночас реалізація концепції вимагає не лише технологічних і нормативних змін, а й глибокої інституційної трансформації: подолання відомчого егоїзму, формування культури співпраці та довіри, розвитку аналітичних компетентностей державних службовців, забезпечення прозорості та підзвітності на всіх рівнях.

На відміну від існуючих підходів, які зосереджуються переважно на окремих аспектах управління критичною інфраструктурою (нормативно-правове регулювання, фінансування, цифровізація або кадрове забезпечення), запропонована концепція інтегрує ці аспекти в єдину триконтурну модель, де стратегічно-планувальний, ресурсний та інституційний контури взаємодіють через механізми сценарного планування, систему індикаторів стану інфраструктури та багаторівневу адаптацію до змін середовища. Це дозволяє не лише підвищити ефективність окремих управлінських рішень, а й забезпечити системну стійкість і керованість трансформаційних процесів у цілому, що є принципово новим внеском у теорію публічного управління в умовах кризових і посткризових викликів.

5.2. Інноваційні інструменти публічного управління у сфері трансформації об’єктів критичної інфраструктури

Методологічні засади інноваційності у сфері публічного управління трансформацією критичної інфраструктури базуються на поєднанні системного, аналітичного та адаптивного підходів. Інноваційність у цьому контексті розглядається як ключовий атрибут сучасної управлінської парадигми, що дозволяє переходити від реактивних дій до проактивного прогнозування, від фрагментованого адміністрування до цілісного поліцентричного управління. Її сутність полягає не лише у впровадженні нових технологій чи цифрових рішень, а у зміні самої логіки прийняття рішень - з орієнтацією на дані, прозорість, відкритість та залучення багатьох акторів до спільного процесу управління [61]. У такий спосіб інноваційність стає не інструментом, а методологічним принципом, який формує нову якість державного управління в умовах воєнної та післявоєнної реконструкції.

Практична реалізація цього методологічного принципу потребує відповідного інструментального забезпечення, яке б поєднувало технологічну спроможність із управлінською логікою. Таким інструментальним ядром виступає запропонований інноваційний інструментарій публічного управління трансформацією об'єктів критичної інфраструктури, що функціонує як трикомпонентна система:

1) цифрові платформи моніторингу, які забезпечують безперервний збір і первинну обробку інформації про стан об'єктів;

2) аналітичні модулі оцінювання стану об'єктів, що перетворюють різнорідні дані на структуровані аналітичні сигнали;

3) алгоритми підтримки управлінських рішень, які на основі прогнозних моделей визначають сценарії розвитку ситуації та формують рекомендації щодо оптимальних управлінських дій.

Така архітектура забезпечує наскрізний цикл «дані – сигнал – рішення», усуваючи розрив між інформаційним і управлінським контурами, який залишався системною вадою традиційних моделей. Ключовою властивістю

інструментарію є не окреме застосування кожного компонента, а їхня взаємодія: моніторингові платформи постачають верифіковані дані, аналітичні модулі виявляють відхилення та ризики, а алгоритми підтримки рішень перетворюють ці сигнали на керовані дії з урахуванням сценарних прогнозів.

Інноваційна модель публічного управління трансформацією критичної інфраструктури функціонує як динамічна система взаємодії управлінських, технологічних і соціальних компонентів. В її основі лежить аналітична інноваційність, яка забезпечує інтелектуальне ядро прийняття рішень. Від неї розгалужуються організаційні, партнерські та фінансові інновації, що формують гнучку архітектуру координації. Синтез цих елементів породжує адаптивну модель, здатну підтримувати сталість функціонування критичної інфраструктури навіть у режимі невизначеності. Узагальнену логіку цієї взаємодії відображено на рис. 5.7.

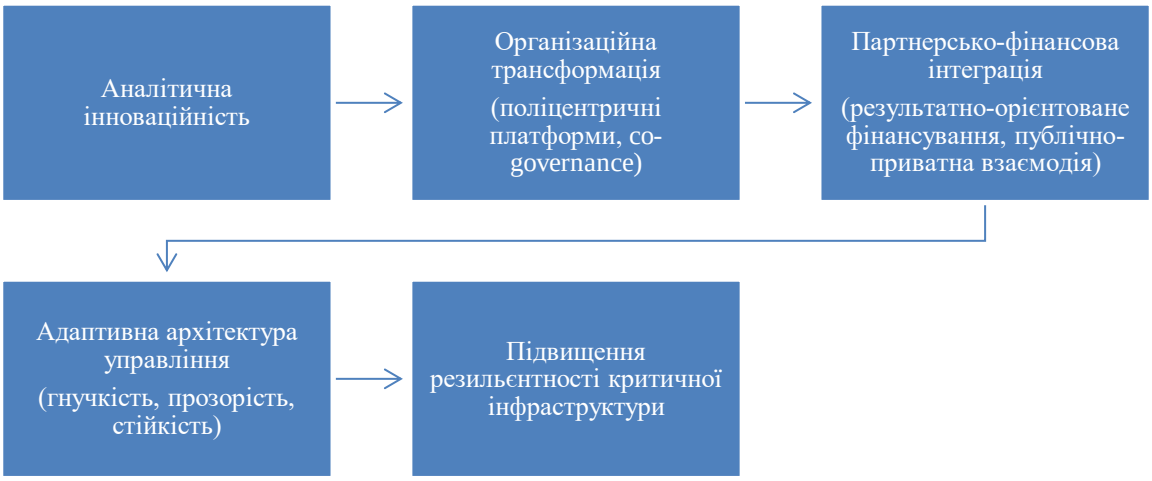


Рис. 5.7. Інноваційна архітектура публічного управління трансформацією критичної інфраструктури*

*Джерело: власна розробка автора

Представлена схема демонструє системну логіку становлення інноваційної моделі управління, у якій аналітична інноваційність виступає вихідною умовою, що визначає якість і глибину всіх подальших управлінських процесів. На цьому рівні відбувається формування механізмів evidence-based та data-driven

governance, що перетворюють інформацію на стратегічний ресурс. Наступним рівнем є організаційна трансформація - створення поліцентричних платформ та форматів co-governance, які дозволяють державі діяти як координатору, а не контролеру, забезпечуючи горизонтальну взаємодію між урядом, громадами та донорами. Третій рівень - партнерсько-фінансова інтеграція - забезпечує мобілізацію ресурсів через результатно-орієнтоване фінансування, публічно-приватне партнерство та донорські платформи, що мінімізують дублювання проєктів і підвищують ефективність витрат. Кінцевим рівнем є адаптивна архітектура управління, що поєднує гнучкість, прозорість та стійкість системи у єдиному циклі управління. Її результатом стає підвищення резильєнтності критичної інфраструктури - здатності не лише витримувати зовнішні удари, а й швидко відновлюватися на основі накопиченого управлінського досвіду. Таким чином, інноваційність у публічному управлінні постає як багаторівневий механізм: від аналітичної діагностики до інституційної гнучкості та стратегічної стійкості. Ця логіка безпосередньо визначає структуру інструментів управління, узагальнену у таблиці 5.5.

Запропонований інструментарій доцільно розглядати як цілісну систему, у якій кожен із трьох компонентів виконує чітко визначену функцію в загальному управлінському циклі. Цифрові платформи моніторингу формують «сенсорний шар» системи: вони забезпечують збір даних із технічних сенсорів, SCADA-комплексів, супутникових джерел, реєстрів і звітності підрядників, а також первинну валідацію та уніфікацію інформації. Аналітичні модулі оцінювання стану об'єктів утворюють «когнітивний шар»: вони обчислюють інтегральні індекси стану, виявляють аномалії, оцінюють ризики та формують аналітичні сигнали, які передаються суб'єктам управління. Алгоритми підтримки управлінських рішень створюють «рішеннєвий шар»: на основі прогнозних моделей вони визначають сценарії розвитку ситуації, оцінюють наслідки альтернативних дій та формують рекомендації щодо вибору оптимального управлінського впливу. Така тришарова архітектура дозволяє перейти від практики «управління за звітами» до практики «управління за сигналами», де кожне рішення має доказову основу, а його наслідки можуть бути заздалегідь

змодельовані. У сукупності це знижує ризики прийняття неузгоджених рішень, які виникають у традиційній моделі через інформаційну асиметрію між рівнями влади та відсутність єдиної аналітичної картини.

Таблиця 5.5

Типологія інновацій у публічному управлінні трансформацією об'єктів критичної інфраструктури*

Тип інновації	Приклад	Короткий опис
Організаційна	Поліцентрична модель, міжвідомча координація	Зміна моделі управління від централізації до мережі
Цифрова	Платформи моніторингу, цифрові двійники	Використання даних і цифрових систем для керування процесами
Фінансова	Результатно-орієнтоване фінансування, портфельні моделі	Зміна фінансового підходу від витрат до результату
Кадрово-компетентна	Програми підготовки з data literacy	Підвищення спроможності управлінців працювати з даними
Партнерська (collaborative)	Співуправління громадою, бізнес-донори	Залучення нетрадиційних акторів до управління
Регуляторна	Адаптивні стандарти, ex-ante/ex-post оцінки політик	Зменшення нормативної інерції, підвищення адаптивності

*Джерело: сформовано автором на основі [39; 48; 255]

У сучасних умовах методологічна інноваційність у публічному управлінні виявляється через побудову інтегрованої управлінської екосистеми, у якій поєднуються цифрові інструменти, фінансові моделі, поліцентричні форми координації та нова культура державного мислення. Після 2022 року акцент державної політики змістився від реагування на кризу до системного управління даними, ризиками й результатами. Це означає перехід до аналітичного передбачення, де цифровізація стає засобом стратегічного планування, а не лише обліку [374].

Аналітична інноваційність реалізується через розвиток національних дата-платформ, які акумулюють багаторівневі дані про стан критичної інфраструктури та забезпечують їхню інтероперабельність. Відмінно від попередніх етапів цифровізації, нове покоління платформ перетворює інформаційні потоки на управлінські сигнали: наприклад, системи типу DREAM 2.0 застосовують принцип «цифрового двійника», коли цифрова копія об'єкта

використовується для моделювання наслідків рішень та оптимізації ресурсів [352].

Організаційна інноваційність полягає у зміні архітектури управління - від ієрархічної вертикалі до поліцентричної взаємодії. Формати співуправління, як-от Ukraine Donor Platform, дозволяють координувати проекти на національному, регіональному та муніципальному рівнях, формуючи єдину екосистему координації [337]. Кадрова інноваційність підтримує цю архітектуру через розвиток компетентностей державних службовців у сфері data literacy, аналітики політик і risk management - це створює управлінський потенціал, здатний працювати з даними, а не з формальними звітами [194].

Фінансова інноваційність проявляється у впровадженні performance-based budgeting та портфельного управління проектами, що дає змогу підвищити ефективність використання коштів і створює основу для формування партнерської фінансової культури. Публічно-приватні механізми у сфері відновлення мостів, енергетики чи водопостачання, які поєднують державні гарантії та технології приватного сектору, поступово трансформують фінансову логіку публічного управління [219].

Регуляторна інноваційність спрямована на впровадження адаптивних норм, які періодично переглядаються залежно від фактичної ефективності. Принцип *sunset clauses* у законодавстві про критичну інфраструктуру дозволяє зменшити нормативну інерцію, узгодити українські стандарти з європейськими та підвищити динамічність правового середовища.

Так, інноваційність у публічному управлінні формує багаторівневу систему - від аналітичної діагностики до інституційної довіри, від цифрових інструментів до гнучких нормативних моделей. Вона створює нову методологічну якість державного управління, засновану на даних, результативності та партнерстві, забезпечуючи реальну стійкість критичної інфраструктури навіть в умовах воєнних ризиків.

Цифровізація публічного управління трансформацією критичної інфраструктури України поступово перетворюється на системоутворювальний чинник стійкості. Її сутність полягає не лише у переході на електронні форми

звітності чи моніторингу, а у створенні нової аналітичної екосистеми управління, у якій взаємодіють державні платформи, локальні цифрові сервіси, геоінформаційні системи (GIS), SCADA-комплекси, енергетичні панелі та «цифрові двійники» територій. Такі системи інтегруються через відкриті API-інтерфейси, забезпечуючи принцип interoperability - взаємної сумісності даних, сервісів та форматів. Цей підхід відображає концепцію data-driven decision making, коли управлінські рішення формуються на основі актуальної інформації, а не адміністративних припущень. У результаті цифрові інструменти створюють «нервову систему» публічного управління, що дозволяє відстежувати стан об'єктів, автоматично реагувати на загрози та забезпечувати прозору координацію дій між державою, громадами й міжнародними партнерами (табл. 5.6).

Таблиця 5.6

Типологія цифрових інструментів публічного управління у сфері трансформації критичної інфраструктури України*

Тип інструменту	Характеристика	Управлінське призначення
Інтеграційно-управлінські платформи	Єдині середовища збору, перевірки та візуалізації даних про відновлення (державні портали, міжвідомчі бази)	Координація державної політики, фінансовий моніторинг, підзвітність перед донорами
Аналітико-контрольні системи	Інструменти відкритих закупівель, аудитів, управління контрактами	Забезпечення прозорості, антикорупційного моніторингу, верифікації витрат
Операційно-технічні комплекси	Системи моніторингу стану інженерних мереж, технічних вузлів, енергетичних об'єктів	Контроль у реальному часі, раннє попередження, підвищення кіберстійкості
Просторово-аналітичні сервіси	Геоінформаційні системи, супутникові карти, інтегровані дашборди	Візуалізація руйнувань, пріоритизація проєктів, планування відновлення
Прогнозно-моделювальні системи	Цифрові двійники об'єктів, міські цифрові моделі, енергетичні панелі стійкості	Сценарне планування, оцінка ризиків, стратегічне управління

*Джерело: сформовано автором на основі [203; 261; 285; 304]

Центральною інтеграційною платформою є DREAM (Digital Restoration Ecosystem for Accountable Management), створена у партнерстві

Мінінфраструктури, USAID та Open Contracting Partnership [90]. Станом на 2025 рік вона об’єднує понад 35 тисяч проєктів реконструкції та слугує єдиним аналітичним «ядром» системи відбудови. DREAM інтегрує дані з Prozorro, Є-Data, кадастрових реєстрів та місцевих GIS-систем, забезпечуючи контроль над фінансуванням і технічними показниками. Її унікальність полягає у тому, що кожен проєкт має геопросторову прив’язку, фінансову історію й цифрову «паспортну картку» від ідеї до реалізації. Це дозволяє урядовим інституціям здійснювати предиктивне управління - своєчасно виявляти ризики затримок і перевитрат.

Екосистема DREAM є практичним втіленням першого компонента запропонованого інструментарію – цифрових платформ моніторингу. Її функціональність виходить за межі облікової системи: платформа забезпечує безперервний збір даних про стан об'єктів на всіх етапах життєвого циклу – від ідентифікації потреби до введення в експлуатацію, а також формує уніфіковане інформаційне поле для всіх суб'єктів управління. Завдяки інтеграції з Prozorro, Є-Data, кадастровими реєстрами та місцевими ГІС-системами DREAM створює передумови для переходу від фрагментованого збору даних до цілісного моніторингу, коли кожен об'єкт має геопросторову прив'язку, фінансову історію та цифрову «паспортну картку». Це дозволяє суб'єктам управління отримувати не розрізнені звіти, а інтегровану картину стану інфраструктури, що є необхідною умовою для функціонування наступних компонентів інструментарію – аналітичних модулів та алгоритмів підтримки рішень. Саме тому цифрові платформи моніторингу доцільно розглядати не як самостійний технологічний продукт, а як базовий шар інноваційного інструментарію, що уможливлює аналітичну надбудову та алгоритмічну підтримку рішень.

Важливою аналітичною складовою є система Prozorro, що функціонує як головний інструмент фінансової доброчесності. За даними ЄБРР, Prozorro щороку забезпечує економію близько 78 млрд грн за рахунок конкурентних закупівель [331]. Система інтегрує аналітичний модуль DOZORRO, який здійснює моніторинг понад 40 тис. тендерів на рік, виявляючи аномалії через алгоритми машинного навчання. Prozorro підтримує відкриті API, що дозволяє

створювати незалежні модулі аудиту, підвищуючи довіру до державних процесів закупівель. У 2025 році ЄБРР визнав Prozorro прикладом найуспішнішої моделі публічної цифрової відкритості в Східній Європі.

У контексті регіональної цифровізації діє платформа RebuildChernihiv, розроблена за участю міжнародної інженерної групи *Egis* [192]. Система поєднує супутникові знімки, кадастрові шари, звіти підрядників і дані донорських програм, створюючи інтерактивну «карту відбудови». Її інтерфейс дозволяє громадам у режимі реального часу відстежувати відновлення житла, транспортних вузлів і соціальних об'єктів. Важливо, що RebuildChernihiv інтегрована з DREAM, забезпечуючи наскрізну видимість фінансування від центрального до місцевого рівня. Таким чином формується модель *spatial accountability* - просторової підзвітності у процесі реконструкції.

Технічну основу цифрової екосистеми становлять SCADA-комплекси (Supervisory Control and Data Acquisition), які забезпечують оперативний контроль за роботою інженерних мереж і критичних вузлів енергосистеми. Сучасні SCADA-рішення побудовані на протоколі OPC UA та Wi-Fi mesh-мережах, що дозволяє отримувати дані в реальному часі навіть у разі порушення централізованих каналів зв'язку. Як доведено у дослідженні Carballo, застосування сучасних SCADA-комплексів у критичній інфраструктурі підвищує енергоефективність на 8–10 % і знижує ризик аварійних відключень на до 20 % [165]. В українських умовах подібні системи інтегруються з аналітичними панелями DREAM та енергетичними модулями для оперативного реагування на пошкодження мереж після ракетних атак.

Просторово-аналітичну основу управління формує Copernicus Emergency Management Service, який у партнерстві з UN-SPIDER здійснює супутникове картографування руйнувань [182]. Дані Copernicus використовуються для створення геоінформаційних моделей реконструкції: у 2024–2025 рр. було зафіксовано понад 4 200 зруйнованих об'єктів критичної інфраструктури, для яких автоматично побудовані карти пошкоджень. GIS-платформи місцевих органів влади інтегрують ці дані для визначення пріоритетів фінансування та технічного проєктування.

В енергетичній сфері функціонує Energy Resilience Dashboard - аналітичний модуль, створений у межах *USAID Energy Security Project* [316]. Його система об’єднує дані з понад 300 енергетичних вузлів і застосовує алгоритми машинного навчання для прогнозування дефіциту потужностей. Це дозволило знизити середню тривалість аварійних відключень на 18 % та підвищити точність балансування мереж. У Dashboard інтегровано функції оцінювання впливу атак на енергетичну інфраструктуру, що робить її інструментом для оперативного реагування та стратегічного планування.

Energy Resilience Dashboard є прикладом другого компонента інструментарію – аналітичного модуля оцінювання стану об'єктів. Його функція полягає не лише у візуалізації даних, а у формуванні аналітичних сигналів, які передаються суб'єктам управління для прийняття рішень. Модуль обчислює інтегральні показники стану енергетичних вузлів, виявляє аномалії споживання та генерації, оцінює ймовірність дефіциту потужностей і формує сигнали раннього попередження. Застосування алгоритмів машинного навчання дозволяє не лише фіксувати поточний стан, а й прогнозувати його динаміку під впливом зовнішніх чинників – атак, сезонних навантажень, ремонтних кампаній. У такий спосіб аналітичний модуль перетворює моніторингові дані на управлінську інформацію, придатну для безпосереднього використання в процесі прийняття рішень. Це принципово відрізняє його від традиційних систем звітності, які фіксують факти post factum, але не генерують сигналів для випереджального реагування. Саме на цьому рівні відбувається перехід від реактивного управління до проактивного, коли суб'єкт управління отримує не констатацію проблеми, а її завчасне передбачення.

Наступний етап цифрової еволюції - впровадження цифрових двійників інфраструктурних об’єктів і територій. За даними досліджень, пілотна система моніторингу «Укренерго» на основі цифрового двійника скоротила час реагування на інциденти на 27 % і підвищила точність прогнозування навантаження на 15 % [115]. Такі технології дозволяють тестувати сценарії пошкоджень без реального втручання, оптимізувати розподіл енергії та підвищувати кіберстійкість. У містобудуванні цифрові двійники

використовуються для моделювання реконструкції мостів, транспортних вузлів і укриттів - створюючи основу для *resilience-based design*, орієнтованого на довготривалу стійкість.

Цифрові двійники інфраструктурних об'єктів і територій виступають технологічною основою третього компонента інструментарію – алгоритмів підтримки управлінських рішень. Їхня принципова відмінність від аналітичних модулів полягає у функціональному призначенні: якщо аналітичні модулі відповідають на запитання «що відбувається з об'єктом», то алгоритми підтримки рішень – на запитання «що слід зробити». На основі прогнозних моделей цифровий двійник дозволяє моделювати наслідки альтернативних управлінських дій: перерозподілу навантажень, зміни пріоритетів ремонтів, резервування потужностей, тимчасової децентралізації генерації. Сценарний аналіз дає змогу оцінити не лише технічну, а й економічну та соціальну ефективність кожного варіанта рішення, а також виявити потенційні конфлікти між цілями різних суб'єктів управління. У результаті суб'єкт управління отримує не єдину «правильну» відповідь, а набір обґрунтованих альтернатив із прогнозованими наслідками, що дозволяє ухвалювати узгоджені рішення з урахуванням багаторівневої природи управління критичною інфраструктурою. Такий підхід безпосередньо знижує ризики прийняття неузгоджених рішень, які виникають через відсутність спільної аналітичної картини у різних суб'єктів управління.

Отже, цифрові інструменти управління критичною інфраструктурою формують когнітивну екосистему, у якій дані перетворюються на центральний ресурс державної стійкості. Вони об’єднують аналітичні, технічні й управлінські рівні, створюючи середовище, де прозорість, швидкість і точність дій стають стандартом публічного управління. У перспективі саме ці системи визначатимуть якість повоєнного відновлення та ефективність інтеграції України в європейський простір управлінських інновацій.

Інноваційні фінансові та партнерські інструменти публічного управління формують нову парадигму відновлення критичної інфраструктури України, орієнтовану не на обсяги залучених коштів, а на якість їхнього управління,

результативність і довгострокову стійкість. У сучасних умовах, коли інвестиційні потоки стають багаторівневими - від донорських до муніципальних, - ключовою метою державної політики є створення інтегрованої фінансово-управлінської архітектури, здатної забезпечити прозоре узгодження пріоритетів, синхронізацію міжурядових та міжнародних програм і стимулювання ефективного використання ресурсів на місцевому рівні.

На відміну від традиційної бюджетної логіки, що фокусується на процесі витрачання, інноваційна модель фінансування орієнтується на результат - measurable outcomes. Це виражається у використанні програм performance-based budgeting, у рамках яких платежі здійснюються після досягнення верифікованих індикаторів результативності. Згідно з аналітичним оглядом Організації економічного співробітництва та розвитку (OECD), такий підхід у 2025 році закріплюється як центральний елемент підвищення стійкості державних фінансів та зменшення політичних ризиків у програмах відбудови [226]. Світовий банк у новій серії документів наголошує, що для України релевантною є модель Results-Based Financing (RBF), яка поєднує елементи фінансової умовності, незалежного аудиту та цифрового відстеження показників [159].

Ця модель забезпечує ефективну інтеграцію донорських ресурсів із внутрішніми бюджетами, дозволяючи уникнути дублювання програм і підвищити довіру партнерів (табл. 5.7). Впровадження таких інструментів поступово формує в Україні нову архітектуру фінансового управління, орієнтовану не на обсяги освоєних коштів, а на реальні результати відбудови. У межах програм RBF та Stage-Gate, реалізованих спільно з міжнародними партнерами, верифікація результатів здійснюється незалежними аудиторськими групами, що значно підвищує довіру до державних систем. За даними World Bank (2025), застосування RBF у пілотних регіонах дозволило скоротити середній час реалізації інфраструктурних проєктів на 18–22 %, а рівень недофінансування через неефективність - на 25 %.

Таблиця 5.7

Інноваційні фінансові та партнерські інструменти публічного управління у сфері трансформації критичної інфраструктури*

Тип інструменту	Зміст та механізм дії	Очікуваний управлінський ефект
Бюджетування, орієнтоване на результат (Performance-Based Budgeting / Results-Based Financing – RBF)	Виплати здійснюються після досягнення підтверджених результатів; акцент на ефективності та незалежному моніторингу	Прозорість, зменшення ризику нецільового використання коштів, підвищення підзвітності
Багатостороння донорська координаційна платформа (Multi-Agency Donor Coordination Frameworks)	Єдина система узгодження пріоритетів між ЄС, Світовим банком, ЄІБ, МВФ та Урядом України	Узгодженість програм, синергія ресурсів, скорочення бюрократичних бар'єрів
Фіскальні трансферти на основі результативності (Performance-Based Fiscal Transfers)	Умовні субвенції та гранти для громад за досягнення стандартів управління, фінансової дисципліни та зрілості проєктів	Підвищення спроможності місцевого самоврядування, стимул до розвитку системного планування
Портфельне управління за моделлю Stage-Gate (Stage-Gate Portfolio Management)	Програмне управління інвестиційними портфелями через послідовність етапів (stage) і контрольних «воріт» (gate)	Керованість ризиками, виявлення неефективних ініціатив, оптимізація життєвого циклу
Рамки ESG та «Зеленої відбудови» (ESG and Green Recovery Frameworks)	Інтеграція екологічних, соціальних та управлінських критеріїв у відбір і фінансування проєктів	Зниження вартості капіталу, довгострокова економічна й кліматична стійкість
Глобальні рамки інновацій для інфраструктури (Global Infrastructure Hub Innovation Frameworks)	Глобальні рекомендації G20 щодо інновацій у фінансуванні кліматостійкої інфраструктури	Гармонізація українських підходів із міжнародними стандартами інвестиційного управління

*Джерело: сформовано автором на основі [120; 193; 245; 266; 273; 290; 87; 323; 343; 346]

Паралельно Європейська комісія у межах Ukraine Donor Platform впровадила портфельну систему управління (Portfolio Governance), у якій донори звітують не лише про обсяги фінансування, а й про частку досягнутих індикаторів відновлення (наприклад, кількість відновлених об'єктів критичної інфраструктури, рівень енергоефективності або цифрової інтеграції) [120]. Це створює новий рівень координації та взаємної підзвітності між міжнародними фінансовими інституціями та українськими виконавцями.

На місцевому рівні, за оцінками UNDP Ukraine (2025), громади, які беруть участь у пілотних програмах performance-based fiscal transfers, демонструють у середньому на 30 % вищу якість реалізації інфраструктурних проєктів і скорочення термінів будівництва на 15–20 % [347]. Це доводить, що навіть за обмежених ресурсів, результатно-орієнтовані механізми стимулюють інституційний розвиток громад і підвищують зрілість їхніх управлінських процесів.

Окрему роль відіграє впровадження ESG-та Green Recovery Frameworks, що дозволяють залучати дешевший капітал. За даними Eurosif (2025), проєкти, сертифіковані за ESG-стандартами, отримують фінансування у середньому на 1,5–2 п.п. дешевше, ніж традиційні кредитні лінії [245]. Водночас European Investment Bank уже реалізує програму Green Recovery Investment Framework, яка забезпечує спільне фінансування інфраструктурних і кліматичних проєктів з орієнтацією на повний життєвий цикл об’єкта [323]. Глобальний вимір цих процесів відображено у звіті Global Infrastructure Hub (2025), що пропонує модель, у якій держава фокусується не на володінні активами, а на керуванні ризиками й інституційній стійкості системи фінансування [193; 290].

У підсумку, інноваційні фінансові та партнерські інструменти не лише змінюють механізми бюджетної політики, а й перетворюють систему публічного управління на адаптивну фінансову екосистему, що поєднує глобальні фонди, державні програми, муніципальні бюджети та приватні інвестиції в єдину логіку результативного відновлення.

Інституційно-організаційні інновації сучасного державного управління формують нову парадигму поліцентричного врядування, у межах якої роль держави поступово трансформується від контролюючої до координуючої. Це зумовлено потребою реагувати на зростаючу складність середовища, багаторівневість ухвалення рішень і участь великої кількості стейкхолдерів у відбудові країни. У сучасних умовах Україна послідовно переходить від вертикальної моделі управління до policy-centered ecosystems, де держава стає ядром багаторівневої взаємодії з громадянами, приватним сектором, науковими установами та міжнародними партнерами. Така зміна логіки управління

заснована на принципах відкритості, довіри й технологічної інтеграції - тобто поєднанні цифрових інструментів, партисипативних практик і гнучких міжвідомчих структур.

Центральним елементом інституційних інновацій виступає поліцентрична координація, коли прийняття рішень відбувається не в межах однієї ієрархії, а через мережу взаємопов'язаних акторів, що мають власні компетенції та ресурси. В українських реаліях це виражається у створенні міжвідомчих офісів впровадження (Delivery Units), спільних проектних офісів при Міністерстві інфраструктури, Мінекономіки та Уряді, платформ координації між громадами й бізнесом. Такі структури не дублюють функції міністерств, а навпаки - забезпечують горизонтальну взаємодію й прискорюють реалізацію стратегічних програм (табл.5.8).

Таблиця 5.8

Інституційно-організаційні інструменти поліцентричного врядування у сфері публічного управління*

Інструмент	Зміст і механізм дії	Очікуваний ефект
Поліцентричні координаційні моделі (Polycentric Coordination Models)	Децентралізована структура управління, у межах якої рішення приймаються через мережу незалежних, але узгоджених центрів - міністерств, регіональних агенцій, громадських рад	Узгодженість політик, зменшення дублювання функцій, адаптивність у кризових ситуаціях
Спільне управління (Co-Governance Platforms)	Механізми залучення громадян, експертних спільнот і бізнесу до планування, моніторингу та оцінки державних програм через відкриті консультаційні панелі та цифрові сервіси	Зростання легітимності рішень, формування довіри, підвищення соціальної відповідальності
GovTech-екосистема (GovTech Ecosystem)	Інтеграція стартапів і технологічних компаній у вирішення публічних завдань через відкриті конкурси, інкубатори, API-платформи (Diia, Prozorro, DREAM)	Ефективність і прозорість процесів, інноваційність рішень, підвищення якості цифрових послуг
Краудсорсинг та партисипативне планування (Crowdsourcing & Participatory Planning)	Використання онлайн-платформ для збору пропозицій громадян щодо пріоритетів розвитку, бюджету, реконструкції; інтеграція цих даних у рішення місцевих рад	Оптимізація управлінських рішень, підвищення залученості населення, скорочення конфліктності

Публічні панелі моніторингу (Public Monitoring Panels)	Інструменти громадського контролю, що базуються на відкритих даних та аналітичних панелях (Public Dashboard, Spending.gov.ua, e-Recovery)	Підзвітність, швидкий зворотний зв'язок, антикорупційний ефект

*Джерело: сформовано автором на основі [169; 202; 259; 336; 344; 349]

Сучасна архітектура публічного управління в Україні поступово набуває рис адаптивної поліцентричної системи, де державні структури взаємодіють із технологічними стартапами, громадами, академічними центрами та громадськими інституціями. Це забезпечує швидкість рішень і скорочення транзакційних витрат - ключовий чинник для країни, що відновлюється після масштабних руйнувань. Такі інституційно-організаційні інновації не є декларативними: вони функціонують як реальні механізми управління змінами у сфері критичної інфраструктури, енергетики, цифровізації, прозорих закупівель і місцевого врядування.

У 2025 році платформа Digital State UA, створена за підтримки Мінцифри, EU4DigitalUA і Програми розвитку ООН, об'єднала понад 140 GovTech-стартапів, які розробляють рішення для державного сектору - від інтелектуальних систем аналітики енергоспоживання до алгоритмів прогнозування відновлення мостів та мереж [326]. Це перший в Україні приклад co-creation-підходу, коли уряд надає API-інтерфейси та тестові дані для стартапів, а ті створюють прототипи, які інтегруються у платформи типу Diia, DREAM, e-Recovery. Зокрема, рішення «CivicLink» дозволяє відстежувати виконання місцевих програм у режимі реального часу, а проєкт «SmartTender-AI» оптимізує перевірку закупівель у Prozorro через машинне навчання.

Система краудсорсингу та партисипативного планування, яку наразі тестують понад 40 громад у межах ініціативи UNDP «Participation 2.0», забезпечує інтеграцію громадських пропозицій у локальні стратегії розвитку. За оцінками Центру розвитку інновацій CID, громади, що використовують цифрові платформи для участі мешканців, мають на 35 % вищий рівень реалізації затверджених проєктів, а прозорість прийняття рішень зросла на 42 % порівняно

з контрольними громадами [349]. Це свідчить, що цифрова демократія поступово переходить від символічної до практичної площини.

Водночас Delivery Units, які діють при Міністерстві інфраструктури та в регіональних адміністраціях, стали «операційним ядром» міжвідомчої координації. Вони поєднують дані систем Prozorro, DREAM, та E-Plan і використовують дашборди для моніторингу виконання проєктів. Наприклад, у рамках пілоту у Чернігівській області час між затвердженням і фактичним початком відновлювальних робіт скоротився з 83 до 56 днів, а рівень верифікованого виконання зріс із 61 % до 89 % [202]. Цей ефект став можливим завдяки автоматизації документообігу та «цифровим сигнатурам» результатів, що мінімізують людський чинник.

GovTech-екосистема активно розвивається через лабораторії спільного управління. Зокрема, GovTech Lab Ukraine, запущена у 2025 році спільно з EBA та USAID, проводить щорічні конкурси «Digital Bridge», у яких переможці отримують гранти для створення публічних технологічних рішень [259]. Відбір здійснюється за моделлю Stage-Gate - після кожного етапу оцінюється практична цінність рішення, що забезпечує відбір лише життєздатних ідей.

Не менш значущою є тенденція до інтеграції публічних моніторингових панелей. Портал Spending.gov.ua, оновлений у 2025 році, додав модуль Civic Insights, що автоматично порівнює видатки проєктів відбудови з відкритими даними DREAM і Prozorro. Це стало елементом системи Public Accountability Dashboards, яку уряд інтегрує у регіональні адміністрації [344]. Паралельно створено публічні карти відбудови в реальному часі, що відображають дані про інфраструктурні об’єкти, підрядників і донорів - інструмент, який суттєво підвищує довіру до державних процесів.

Науково узагальнюючи, можна констатувати, що поліцентричне співуправління в Україні набуває характеристик гнучкої інституційної екосистеми, яка функціонує за принципом «Дані – дія - зворотній зв’язок - корегування». Держава більше не виступає монополістом управління, а перетворюється на архітектора середовища, де управлінські рішення співтворяться із суспільством і технологічними партнерами. Це є ключовою

умовою побудови адаптивної, мережевої держави, здатної діяти в умовах невизначеності, швидко мобілізувати ресурси й підтримувати сталу взаємодію всіх рівнів управління [169].

Такі процеси демонструють, що інституційно-організаційні інновації - не лише технологічна модернізація, а й трансформація самої природи державності, яка в епоху цифрових публічних сервісів стає «платформою довіри» для громадян, бізнесу та партнерів розвитку.

Запровадження інноваційних інструментів у публічному управлінні критичною інфраструктурою наштовхується на бар'єри, що лежать не стільки в технічній, скільки в інституційній та когнітивній площині. Нормативна інерція проявляється в тому, що правила життєвого циклу проєктів, закупівель і звітності залишаються процедуроцентричними, тоді як інноваційні інструменти - цифрові платформи, «цифрові двійники», аналітичні панелі, ризик-орієнтовані метрики - потребують результатоорієнтованих і адаптивних норм [261]. Жорстко окреслені етапи погоджень і уніфіковані тендерні специфікації фактично блокують гнучкі методи розроблення, поетапне масштабування та оновлювані технічні вимоги, що властиві сучасним IT-сервісам для управління інфраструктурою. У підсумку інновація редукується до «пілоту без наступного впровадження», оскільки процедура не має вбудованого механізму переходу від експерименту до промислової експлуатації з гарантіями якості, кіберстійкості та підтримуваності [202].

Фрагментація цифрових систем віддзеркалює історичну залежність від попереднього шляху: галузеві реєстри, регіональні інформаційні системи, SCADA й ГІС розвивалися ізольовано та використовують різні моделі даних, що унеможливлює наскрізну телеметрію «планування-закупівля-виконання-експлуатація» [192]. Відсутність обов'язкових стандартів інтероперабельності та каталогів метаданих спричиняє розриви в даних, дублювання вводів, помилки відповідності і, як наслідок, - невідтворювані аналітичні висновки. Коли «цифровий двійник» території не синхронізований із первинними сенсорними потоками, а проєктні кошториси - із фактичними актами виконаних робіт, управлінські рішення втрачають доказовість, а контроль якості - оперативність.

Додається й проблема vendor lock-in: закриті специфікації, пропрієтарні формати і ліцензійні обмеження ускладнюють міграцію даних і нарощування функціональності, підвищуючи повну вартість володіння та послаблюючи конкуренцію рішень [343].

Слабка культура управління даними робить навіть технологічно спроможні інструменти малоефективними. Поза рамкою формальних «посадових інструкцій» рідко визначені ролі й відповідальність за якість даних: хто є data steward, хто затверджує схеми і словники, хто проводить валідацію та аудит змін [203]. Без керування головними даними і версіонування моделей «цифрові двійники» швидко втрачають актуальність, а аналітичні панелі починають відображати синтетичні, неузгоджені показники. Додайте розрив між капітальними та операційними бюджетами: інституції спроможні оплатити «побудову» інструмента в межах інвестпроєкту, але не мають стабільної моделі фінансування експлуатації - хостингу, кіберзахисту, техпідтримки, оновлень і навчання персоналу. У результаті платформи деградують саме тоді, коли переходять із донорського фінансування на рутину державного бюджету.

Довіра до цифрових сервісів і екосистем відкритих даних формується повільніше, ніж технології. Без прозорих механізмів аудит-трейлів, незалежної верифікації алгоритмів, пояснюваності моделей та зрозумілих політик приватності користувачі - як службовці, так і громадяни - сприймають цифрові рішення як «чорні скриньки». Репутаційні ризики зростають у середовищі інтенсивних кібератак: коли відмовостійкість і план безперервності діяльності прописані декларативно, будь-який інцидент трансформується у кризу довіри до всієї цифрової архітектури управління. Додатковим обмеженням є нерівномірність підключення і якості електроживлення у прифронтових і деокупованих громадах: навіть найкращі інструменти втрачають сенс, якщо немає гарантованих каналів зв’язку, локальних буферів даних і протоколів офлайн-роботи з подальшою синхронізацією [375].

Кадрова спроможність відстає від вимог інноваційного циклу. Управління «за даними» потребує компетенцій, яких традиційна система підвищення кваліфікації майже не формує: моделювання політик і вимірювання впливу,

управління продуктом, проєктування сервісів, управління модельним ризиком, кібергігієна, сучасні практики закупівель GovTech. Без цих навичок інституції повертаються до процесоцентричної логіки, де головною метою стає «правильний документ», а не перевірюваний результат для бенефіціарів. Крос-секторальна взаємодія теж залишається слабкою: правовласники даних, IT-підрозділи, фахівці з безпеки, фінансисти і політикоаналітики функціонують у «сайлах», що унеможливлює швидке узгодження змін у схемах даних, KPI, бюджетах та контрактах.

Окремим блоком стоять правові невизначеності щодо обміну даними й етичного використання алгоритмів. Страх порушити персональні дані або комерційну таємницю блокує міжвідомчі інтеграції навіть там, де вони законні та необхідні; водночас відсутність єдиних стандартів та мінімізації даних породжує або зайву обережність, або надмірне відкриття. Баланс безпеки й відкритості досягається лише через формалізовані політики доступу, незалежний нагляд і сертифікацію процесів - але ці механізми ще не стали звичним операційним стандартом.

Нарешті, інституційна інерція й асиметрія стимулів підривають портфельне управління інноваціями. Для керівника підрозділу ризик запустити зміну, яка тимчасово знизить продуктивність або вимагатиме перерозподілу бюджету, часто перевищує потенційну вигоду в середньостроковій перспективі. Коли система оцінювання фокусується на «дотриманні регламенту», а не на досягнутих ефектах, інноваційні інструменти сприймаються як джерело додаткових перевірок, а не як засіб зменшення невизначеності та пришвидшення рішень. У поєднанні з нерівномірним доступом громад до технічної підтримки, відсутністю державних пісочниць і типовими SLA для цифрової взаємодії це формує контур, у якому поодинокі успіхи не масштабуються, а системні уроки не капіталізуються.

Сукупно зазначені бар’єри обмежують потенціал інновацій тим, що розривають причинно-наслідковий ланцюг «дані - інсайт - рішення - доведений ефект». Без інтероперабельних даних і зрозумілої відповідальності за їхню якість аналітика стає декоративною; без довіри до цифрових сервісів і кіберстійких

процесів зникає готовність покладатися на автоматизовані рішення; без кадрової та бюджетної моделі експлуатації інструменти не долають «долину смерті» між пілотом і рутинною практикою. Подолання цих розривів вимагатиме не лише нових технологій, а насамперед змін у правилах, стимулів і компетенціях - тобто переформатування самої управлінської архітектури, у межах якої інновація перестає бути подією і стає нормою операційного циклу.

Запропонований трикомпонентний інструментарій дозволяє частково подолати зазначені бар'єри саме тому, що він функціонує як цілісний управлінський контур, а не як набір розрізнених технологічних рішень. По-перше, цифрові платформи моніторингу створюють єдине інформаційне поле, яке зменшує фрагментацію даних і забезпечує інтероперабельність між відомствами на рівні базового шару. По-друге, аналітичні модулі оцінювання стану об'єктів переводять управління з процедурної логіки на логіку сигналів, що дозволяє долати нормативну інерцію через оперативне виявлення відхилень і ризиків. По-третє, алгоритми підтримки рішень формують обґрунтовані альтернативи, які зменшують когнітивне навантаження на суб'єктів управління та знижують імовірність помилкових рішень в умовах невизначеності. Водночас ефективність інструментарію залежить від усунення інституційних бар'єрів: без формалізованих ролей data stewards, єдиних стандартів метаданих, стабільного фінансування експлуатації та навчання персоналу навіть технологічно досконалі компоненти втрачають управлінську цінність. Таким чином, інструментарій слід розглядати не як заміну інституційних реформ, а як їхній каталізатор – він створює операційну основу, на якій інституційні зміни стають вимірюваними та відтворюваними.

Розбудова інноваційної екосистеми публічного управління у сфері трансформації критичної інфраструктури потребує переходу від проєктної логіки окремих цифрових рішень до системної моделі співтворення, де держава, громади, бізнес і наукові інституції спільно продукують управлінські та технологічні інновації. Центральним завданням є створення єдиного інституційного контуру, який забезпечує як координацію стратегічних пріоритетів, так і відтворюваність операційних інструментів. У цьому контексті

ключову роль має відігравати урядовий офіс інновацій у сфері публічного управління, уповноважений координувати проєкти цифрової трансформації, формувати стандарти інтероперабельності, проводити оцінювання ефективності пілотів та організовувати пісочниці для тестування нових рішень.

Передумовою функціонування такої екосистеми є створення інтегрованої цифрової тканини управління (data fabric) - єдиного середовища даних, що об'єднує державні реєстри, сенсорні мережі, цифрові двійники об'єктів інфраструктури, платформи закупівель і фінансові трекери. Це дозволяє синхронізувати дані в режимі реального часу, забезпечити їх цілісність і одночасний доступ для різних рівнів управління. У поєднанні з competence-based системою навчання державних службовців та програмами партнерського GovTech-розвитку така архітектура створює умови для швидкого впровадження інновацій без надлишкових адміністративних бар'єрів (рис. 5.8).



Рис. 5.8. Алгоритм формування інноваційної екосистеми публічного управління трансформацією критичної інфраструктури

Джерело: власна розробка автора

У запропонованій схемі взаємодія елементів побудована за принципом поступового розгортання від інституційного ядра до операційної синергії. На інституційному рівні урядовий офіс інновацій виступає координаційним

центром, який об’єднує державні органи, місцеве самоврядування, бізнес і наукові організації в єдину інноваційну мережу.

Інтеграція трикомпонентного інструментарію в запропоновану екосистему дозволяє забезпечити повний управлінський цикл, у якому кожен елемент виконує свою функцію в межах єдиної логіки. На етапі збору інформації цифрові платформи моніторингу забезпечують безперервне надходження верифікованих даних про стан об'єктів критичної інфраструктури, інтегруючи технічні, фінансові та просторові виміри. На етапі обробки аналітичні модулі оцінювання перетворюють ці дані на аналітичні сигнали – індекси стану, показники ризику, індикатори відхилень, – які передаються суб'єктам управління у формі, придатній для безпосереднього використання. На етапі прийняття рішень алгоритми підтримки на основі прогнозних моделей визначають сценарії розвитку ситуації та формують рекомендації щодо оптимальних управлінських дій, оцінюючи наслідки кожної альтернативи. На етапі верифікації результати реалізованих рішень повертаються в систему моніторингу, замикаючи цикл зворотного зв'язку та забезпечуючи самонавчання системи. Така циклічна логіка дозволяє перейти від практики одиничних управлінських актів до практики безперервного адаптивного управління, у якому кожне рішення ґрунтується на попередньому досвіді та прогнозних оцінках. Очікуваним результатом упровадження інструментарію є не лише підвищення швидкості та точності рішень, а й формування нової управлінської культури, у якій дані, аналітика та прогнозування стають базовими елементами професійної діяльності, а не допоміжними інструментами. У довгостроковій перспективі це забезпечує стійкість критичної інфраструктури, зменшення ризиків неузгоджених рішень і підвищення довіри суспільства до державного управління.

Його завдання - створити регуляторні рамки для безпечного тестування нових підходів, уніфікації API-протоколів та інтеграції аналітичних інструментів у процеси прийняття рішень.

На технологічному рівні впровадження data fabric забезпечує наскрізну взаємодію між усіма цифровими платформами - від систем моніторингу стану об’єктів до управління закупівлями та фінансами. Це створює можливість

об’єднання оперативних і аналітичних даних, що дозволяє здійснювати не лише реактивний, а й проактивний контроль ризиків.

На кадровому рівні competence-based підхід до навчання фокусується на розвитку конкретних компетентностей: управління даними, аналіз ефективності політик, робота з цифровими двійниками, кібергігієна, інноваційне бюджетування. Така система дозволяє підготувати управлінців, здатних діяти в умовах швидкої технологічної динаміки.

На експериментальному рівні партнерські sandboxи (регуляторні пісочниці) стають простором для випробування нових технологій - від платформ кіберзахисту до енергетичних модулів автономності - без ризику порушення чинних норм, але під контролем органів публічного управління.

На нормативному рівні відкриті API-стандарти та вимоги до інтероперабельності забезпечують можливість інтеграції різних систем незалежно від постачальників технологій. Це сприяє конкуренції, зниженню витрат і підвищенню довіри до цифрової інфраструктури держави.

На фінансово-стимулюючому рівні запуск програм підтримки GovTech-рішень – грантів, прискорювачів і конкурсів - формує ринок державних технологій, орієнтований на вирішення реальних завдань відбудови. Таке поєднання публічного та приватного секторів створює ефект масштабування, коли розроблені рішення можуть бути застосовані у різних регіонах і галузях.

Очікуваним результатом впровадження цього механізму стане формування стійкої екосистеми управління, у якій рішення ухвалюються швидше завдяки аналітичній інтеграції, ризики зменшуються через прогнозну аналітику, прозорість посилюється відкритими стандартами даних, а довіра суспільства - через демонстрацію вимірюваних ефектів. У довгостроковій перспективі така модель дозволить перейти від реактивного управління кризами до адаптивного розвитку інфраструктури, що базується на інноваціях, даних і партнерстві.

5.3. Перспективи відновлення об’єктів критичної інфраструктури в Україні (у т. ч. на деокупованих територіях)

Деокуповані території України формують унікальний об’єкт державної політики, де відновлення критичної інфраструктури відбувається у надзвичайно складних безпекових, соціально-економічних і просторових умовах. Масштаб руйнувань, порушення логістичних зв’язків, демографічні деформації та екологічні ризики створюють середовище, у якому класичні підходи до реконструкції втрачають ефективність. Просторово-ресурсна характеристика цих територій виступає не лише діагностичною основою для планування, а й аналітичним індикатором управлінської готовності держави діяти в умовах постокупаційного середовища. Вона відображає реальний баланс між відновлюваним потенціалом, безпековими бар’єрами та спроможністю інституцій забезпечити життєздатність базових функцій. На практиці це означає необхідність переосмислення поняття «ресурс» - від матеріального запасу до здатності системи швидко адаптуватися, інтегрувати зовнішню допомогу та перетворювати локальні ініціативи у сталі управлінські рішення (табл. 5.9).

Таблиця 5.9

Просторово-ресурсна характеристика деокупованих територій України як база для управління відновленням критичної інфраструктури*

Показник	Характеристика стану (2025 р.)	Потенціал відновлення / управлінське значення
Ступінь фізичних руйнувань інфраструктури	Високий (40–80 % об’єктів частково або повністю зруйновані)	Пріоритетність екстреного енергетичного та транспортного відновлення; потреба у швидких типових рішеннях
Демографічна структура	Скорочення постійного населення на 30–50 %, домінування літніх груп	Вплив на трудову мобільність, потреба у залученні зовнішніх фахівців і стимулюванні повернення громадян
Трудовий потенціал і зайнятість	Нестача робочої сили у сфері будівництва, енергетики, ЖКГ	Формування регіональних програм перекваліфікації, залучення мобільних ремонтних підрозділів
Рівень мінної небезпеки та екологічні ризики	Замінування до 30 % територій, пошкодження ґрунтів, водних ресурсів	Потреба у поєднанні інфраструктурних проєктів із програмами розмінування та екологічної реабілітації

Стан енергопостачання і комунікацій	Часткове функціонування, часті збої у зв'язку та електропостачанні	Необхідність децентралізованої генерації, мобільних енергомодулів, альтернативних джерел живлення
Соціальна інфраструктура	Руйнування 40–60 % закладів освіти, охорони здоров'я, соціального захисту	Відновлення як фактор повернення населення і стабілізації громади
Транспортна доступність і логістика	Руйнування мостів, колій, доріг, порушення маршрутів постачання	Формування тимчасових транспортних коридорів, відновлення вузлових об'єктів як базових для економічної активності
Інституційна спроможність місцевого самоврядування	Ослаблена структура управління, дефіцит кадрів, фрагментація функцій	Необхідність зовнішнього адміністрування через регіональні офіси відновлення або міжвідомчі штаби
Доступ до фінансування	Обмежений власний ресурс, залежність від донорських програм	Пріоритезація грантових механізмів, прозорі системи обліку і моніторингу використання коштів
Психосоціальний стан громади	Високий рівень травматизації, недовіра до державних інститутів	Розвиток програм соціальної згуртованості, залучення громад у процес планування відновлення

*Джерело: сформовано автором на основі [33; 36; 56; 72; 157; 248; 262]

У сучасних умовах повномасштабної війни просторово-ресурсна характеристика деокупованих територій України перетворюється на інтегральний індикатор реального стану державної відновлювальної спроможності. Вона виконує роль аналітичного профілю, який поєднує кількісні й якісні параметри середовища – рівень фізичних руйнувань, демографічні зміни, трудовий потенціал, ступінь безпеки, стан інфраструктури, екологічні ризики та інституційну спроможність. Такий профіль відображає не лише наслідки воєнних дій, а й можливості до швидкої адаптації та трансформації локальних систем у стійкі середовища розвитку. У його основі лежить принцип багаторівневої взаємодії: дані про ресурси території накладаються на показники соціальної динаміки та безпеки, формуючи тривимірну модель потенціалу відновлення.

На практиці це проявляється у створенні регіональних карт відновлення, які демонструють не лише масштаб руйнувань, а й життєздатність окремих секторів. Так, у Херсонській області після звільнення від російської окупації було зафіксовано, що понад 30 % територій залишаються замінованими, 60 % житлової інфраструктури зазнали руйнувань, а близько половини населення вимушено евакуйовано [33]. Проте на основі просторових даних і польових

обстежень визначено зони, придатні для поетапного повернення мешканців і запуску комунальних сервісів. У цих локаціях відновлення розпочиналося не з відбудови об’єктів, а зі створення мобільних енергетичних та водних модулів, що забезпечували базовий рівень життєздатності громад. Подібні підходи апробовані й на північному сході країни, де в Ізюмському районі Харківської області використовується система геопросторової інвентаризації для визначення пріоритетів відновлення [36]. На основі супутникового моніторингу і локальних звітів створено матрицю «інтенсивність руйнувань – рівень демографічних втрат – доступ до енергопостачання», що дозволила вибудувати черговість реконструкції об’єктів. За оцінками Київської школи економіки, реалізація подібних рішень скорочує середній час повернення функціональної спроможності громад на 35–40 % [258]. Таким чином, просторово-ресурсна характеристика не є описом стану руйнувань - це дієвий профіль управління, який фіксує не лише рівень втрат, а й здатність території до самовідновлення. Взаємозв’язки між ключовими складовими можна представити узагальненою структурно-функціональною схему профілю (рис. 5.9).

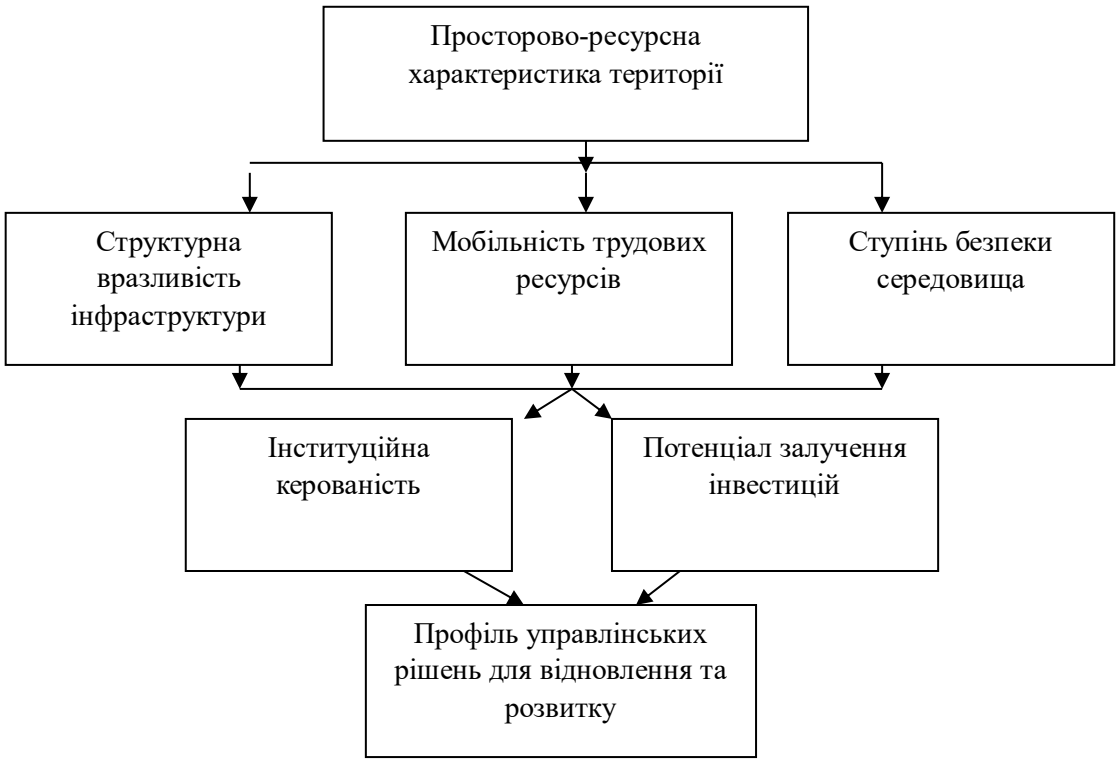


Рис. 5.9. Структурно-функціональний профіль просторово-ресурсної характеристики деокупованих територій*

*Джерело: власна розробка автора

Схема відображає системну логіку побудови просторово-ресурсного профілю. На верхньому рівні формується загальна характеристика території як аналітична рамка. Далі вона розкладається на п’ять взаємопов’язаних параметрів, що утворюють своєрідний «вектор відновлювальної стійкості». Структурна вразливість визначає технічні обмеження, мобільність трудових ресурсів - кадровий потенціал, ступінь безпеки - умови для початку робіт, інституційна керованість - можливості локального адміністрування, а потенціал залучення інвестицій - фінансову спроможність. На перетині цих п’яти вимірів формується інтегрований профіль управлінських рішень, який уможливлює пріоритизацію відбудовчих проєктів і прогнозування темпів функціонального відновлення. У практичному вимірі така схема дозволяє визначати не лише території найбільшої потреби, а й ті, де комбінація параметрів створює передумови для сталого розвитку після завершення базового відновлення.

Відновлення критичної інфраструктури на деокупованих територіях України є процесом, що має поетапну логіку, де кожен етап визначає характер управлінських рішень, часові горизонти та рівень залучення ресурсів. Сценарний підхід дозволяє описати цю динаміку не як сукупність ізольованих дій, а як послідовну траєкторію - від мінімальної життєздатності систем до їх повноцінного інноваційного перезавантаження. У такій логіці екстрене стабілізаційне відновлення виступає базовим етапом відновлення критичних функцій держави, функціональне відновлення забезпечує повернення до сталого функціонування базових секторів, а інноваційне перезавантаження створює нову якість інфраструктурного розвитку через впровадження сучасних технологій, «зелених» стандартів і цифрових рішень (табл. 5.10).

Таблиця 5.10

Сценарії відновлення критичної інфраструктури в повоєнному періоді*

Сценарій	Основна мета	Часовий горизонт	Характер управління	Ключові механізми реалізації
Екстрене реагування	Усунення безпосередніх загроз життю, ліквідація руйнувань критичних об’єктів, забезпечення базових послуг (вода,	0–3 місяці після деокупації	Централізоване кризове управління (ДСНС, військові адміністрації, Нацполіція)	Розмінування, відновлення енергопостачання тимчасовими модулями, аварійний ремонт

	енергія, медична допомога)			мостів, розгортання мобільних госпіталів
Стабілізаційне відновлення	Відновлення систем життєзабезпечення, повернення населення, налагодження логістики та комунікацій	3–9 місяців	Координаційне (уряд + місцеві штаби)	Запуск комунальних сервісів, забезпечення палива, ремонт доріг і мостів, підключення громад до електро- та водопостачання
Функціональне відновлення	Відновлення економічної активності, соціальної інфраструктури, робочих місць і податкових надходжень	9–24 місяці	Змішане (державні органи, громади, міжнародні партнери)	Відновлення підприємств, будівництво житла, ремонт лікарень і шкіл, цифровізація муніципалітетів
Адаптивно-інтеграційне відновлення	Поєднання реконструкції з модернізацією, інтеграція у європейські стандарти сталого розвитку	2–4 роки	Поліцентричне (державні агентства, громади, приватний сектор)	Формування енергетичних кластерів, створення індустріальних парків, впровадження систем DREAM і BIM
Інноваційне перезавантаження	Перехід до високотехнологічної, «зеленої» і цифрової інфраструктури	4–7 років	Децентралізоване партнерське управління	Використання IoT-систем у моніторингу, 3D-друку в будівництві, впровадження відновлюваної енергетики, smart-logistics

*Джерело: сформовано автором на основі [134; 195; 252]

Реалізація наведених сценаріїв у практиці відбудови України засвідчує перехід державної політики від реактивної моделі ліквідації наслідків до стратегічно-керованої траєкторії відновлення, що спирається на аналітику, цифровізацію та поліцентричну взаємодію. Кожен сценарій не лише окреслює часовий горизонт, а й відображає різний рівень управлінської зрілості системи.

На етапі екстреного реагування реалізуються механізми швидкої мобілізації ресурсів - від енергетичних контейнерних станцій до мобільних систем очищення води. За даними урядового порталу *Rebuild Ukraine*, станом на

серпень 2025 року понад 740 об’єктів критичної інфраструктури було відновлено у режимі оперативного реагування, зокрема 230 підстанцій та 118 мостів тимчасового типу, що забезпечили базове транспортне сполучення у Херсонській, Чернігівській та Харківській областях. Такий формат демонструє новий тип управління – *швидкоадаптивне кризове реагування*, у якому ключову роль відіграють алгоритми пріоритизації на основі даних з систем моніторингу DREAM та супутникової аналітики PlanetScope [198].

На фазі стабілізаційного відновлення акцент зміщується з усунення наслідків на формування операційної спроможності територій. Це означає відновлення мереж життєзабезпечення з елементами гнучкої модернізації. У 2024–2025 рр. у межах урядової програми *Fast Recovery* на деокупованих територіях реалізовано 2 167 локальних проєктів, з яких понад 60 % стосувалися реконструкції систем теплопостачання, ще 22 % – відновлення водних мереж. Вперше застосовано механізм мультиканального фінансування, коли кошти від державного бюджету, донорів і громадських фондів акумулювалися на єдиній платформі управління. Це стало інституційною інновацією, яка забезпечила зменшення затримок у фінансуванні з 90 до 14 днів [71].

Функціональне відновлення відзначається переходом від стабілізації до економічного перезапуску. Тут ключовим індикатором є частка відновлених підприємств та робочих місць. Станом на середину 2025 р. у звільнених регіонах відновлено понад 38 % об’єктів промислової інфраструктури, а рівень зайнятості у секторах транспорту й будівництва сягнув 72 % довоєнного рівня. Новизна цього сценарію полягає у використанні моделі *community-driven recovery*, за якою громади самі формують пріоритети через цифрові консультаційні майданчики [218]. Це не лише підвищує ефективність, а й створює горизонтальні зв’язки між громадянами, бізнесом та владою, перетворюючи відбудову на форму колективного управління.

У фазі адаптивно-інтеграційного відновлення спостерігається перехід до синергетичної моделі розвитку. Відбудова починає інтегруватися в європейські логістичні, енергетичні та технологічні мережі. Зокрема, у 2025 р. розпочато створення 12 міжрегіональних енергетичних кластерів з часткою відновлюваної

енергії понад 35 %, а також ініційовано 5 індустріальних парків на базі деокупованих територій. Інноваційність цього етапу полягає у застосуванні систем BIM-моделювання, які дозволяють планувати реконструкцію в реальному часі, враховуючи технічний стан і ризики руйнувань. Уперше на регіональному рівні впроваджено *індикатори резильєнтності територій*, що оцінюють відновлюваність не лише інфраструктури, а й соціального капіталу.

Нарешті, сценарій інноваційного перезавантаження передбачає формування інфраструктури нового покоління – цифрової, сталої та енергоефективної. Тут управлінський вектор зміщується від ремонту до інноваційного розвитку. У рамках пілотних проєктів у Львівській, Сумській та Київській областях запроваджено технології 3D-друку конструкційних елементів для швидкого спорудження адміністративних будівель і житла, що знизило витрати часу на будівництво на 40 %, а матеріальні – на 28 %. Активно впроваджуються системи IoT-моніторингу, які збирають дані про навантаження на інженерні мережі в режимі реального часу, що дозволяє оптимізувати використання енергії та прогнозувати ризики пошкоджень.

Таким чином, сценарний підхід формує нову парадигму публічного управління відновленням – від вертикального реагування до поліцентричного партнерства. Його наукова новизна полягає у тому, що відновлення розглядається не як кінцева фаза післявоєнного циклу, а як динамічний процес розвитку, де кожен сценарій стає фазою еволюції державної спроможності. У цьому підході інтеграція технологій, цифрових індикаторів і соціального капіталу утворює систему, здатну не лише відбудовувати, а й передбачати майбутні ризики, формуючи основу для сталого розвитку та європейської інтеграції України. Інтеграція процесів відбудови у систему державної політики є ключовим завданням сучасного етапу управління. Якщо початкові програми мали проектний і переважно технічний характер, то нині формується нова управлінська парадигма, у якій відновлення розглядається як структурна складова державного розвитку. Йдеться не лише про відбудову об’єктів, а про створення інституційної сталості, де відновлення стає частиною циклу державного управління, інтегрованого з бюджетним плануванням, аналітикою

ризиків і стратегічним прогнозуванням. У цьому контексті перехід від «реконструкції до перетворення» означає зміну самого типу управлінського мислення - від короткострокового реагування до довгострокової політики формування стійкості (табл. 5.11).

Таблиця 5.11

Управлінські механізми інтеграції процесів відбудови у систему державної політики*

Рівень інтеграції	Управлінський механізм	Зміст і функції	Ключові інституційні інструменти	Очікуваний результат
Стратегічний	Політична інституалізація відновлення	Перехід від проєктного підходу до постійної державної політики; включення питань реконструкції до національних стратегій розвитку	Державна стратегія відбудови, довгострокові цільові програми, міжвідомча рада з відновлення	Формування стійкої політики відновлення, узгодженої з бюджетними циклами
Координаційний	Міжсекторальна взаємодія	Узгодження дій державних органів, громад, бізнесу, міжнародних донорів; уникнення дублювання функцій	Координаційні офіси, угоди між секторами, єдині протоколи обміну даними	Ефективна взаємодія учасників процесу, скорочення транзакційних витрат
Операційний	Програмно-цільове управління	Формування пакетів проектів за єдиними стандартами моніторингу, фінансування й оцінки	Цільові програми реконструкції, багаторічні бюджети, паспорти об’єктів	Перехід від розрізнених ініціатив до системного управління проєктами
Аналітичний	Моніторинг і оцінка впливу	Вимірювання результативності відновлення, корекція політик, створення баз даних ризиків	Системи державного моніторингу, аналітичні панелі, звіти ефективності	Зворотний зв’язок між управлінськими рішеннями й фактичними результатами
Соціально-комунікаційний	Партнерська участь громад і донорів	Залучення громадян до спільного управління та контролю, публічна підзвітність	Консультативні ради, громадські платформи, механізми соціального аудиту	Підвищення довіри до державної політики, легітимізація рішень

*Джерело: сформовано автором на основі [246; 252; 282]

Інтеграційні механізми відбудови сьогодні виконують роль інституційного мосту між надзвичайним реагуванням і сталим державним управлінням. На практиці це означає, що відбудова перестає бути винятково технічною функцією і переходить у категорію політичної сталості, де проєкти реконструкції узгоджуються з бюджетними циклами, структурою національних стратегій і системою регіонального розвитку. На стратегічному рівні ключовою новацією стало формування багатошарової моделі управління, в якій рішення про відновлення ухвалюються не лише в межах міністерств, а в координаційних контурах між секторами. У результаті створено систему, де фінансові, технічні та соціальні інструменти працюють у спільному управлінському полі.

Показовим прикладом є діяльність Національної ради з відновлення України, яка стала платформою для інституціоналізації міжвідомчої взаємодії. На практиці ця структура виконує функції не просто координації, а синтезу стратегічних і бюджетних рішень, перетворюючи ініціативи окремих відомств у єдині програми державної дії. Зокрема, у 2024–2025 рр. саме через цей механізм понад 60 % проєктів реконструкції транспортної та енергетичної інфраструктури були включені до середньострокових бюджетних програм. Таким чином відбувся перехід від грантової логіки до бюджетно-програмної, що створило передумови для інституційної стійкості управлінських рішень [181].

Другий рівень інтеграції – аналітично-моніторинговий - забезпечує зворотний зв’язок між політикою та фактичним прогресом. Система оцінки ефективності, запроваджена у 2025 р. у межах *Reforms Delivery Office* при Міністерстві відновлення, дала можливість не лише фіксувати відсоток виконаних об’єктів, а й аналізувати їх соціально-економічний ефект. Наприклад, моніторинг впливу інвестицій у транспортну інфраструктуру показав, що громади, у яких реконструкція доріг відбулася протягом перших шести місяців після деокупації, демонструють зростання внутрішньої мобільності населення на 38 %, а рівень ділової активності малого бізнесу - на 24 % порівняно з регіонами без інтегрованої моделі управління [93]. Ці дані вперше використано для корекції державних програм фінансування, що свідчить про перехід до цифрово-аналітичного циклу управління.

Координаційний і соціально-комунікаційний рівні механізмів функціонують як практичні платформи партнерства. Наприклад, у Херсонській області запроваджено пілотну модель *Recovery Governance Framework*, у якій громади, обласна військова адміністрація та міжнародні донори діють за єдиними процедурами оцінки впливу. Внаслідок цього середній час затвердження проєктів скоротився з 42 до 11 днів, а обсяг залученого співфінансування зріс на 33 %. Аналогічно, на рівні Чернігівщини через інтеграцію місцевих рад до державних програм відбудови вдалося підвищити рівень використання коштів розвитку з 58 до 87 %, що свідчить про підвищення фінансової спроможності системи [347].

Найгострішим викликом є демілітаризація простору, що передбачає не лише розмінування, а й перетворення територій війни на безпечні середовища розвитку. У багатьох районах, де відбулися бойові дії, продовжують діяти залишкові воєнні ризики – нерозірвані боєприпаси, зруйновані склади боєприпасів, пошкоджені системи трубопроводів і енергомереж [263]. Це створює постійну небезпеку для відновлювальних команд і стримує повернення населення. Водночас демілітаризація потребує нового типу управління - воєнно-громадянської синхронізації, коли процеси розмінування, відновлення інфраструктури та соціальної реінтеграції координуються між оборонними структурами, місцевими органами влади й міжнародними партнерами.

Не менш складною є проблема деформації просторово-майнових відносин. На деокупованих територіях значна частина кадастрових і реєстрових даних втрачена або спотворена, що унеможливлює підтвердження права власності. Це створює феномен «територій без титулу», де рішення про відбудову затримуються через юридичну невизначеність [134; 253]. Відсутність електронних кадастрів також ускладнює планування землекористування, особливо для промислових і сільськогосподарських об’єктів, що підлягають реконструкції. Без відновлення правового континууму власності реалізація стратегічних проєктів лишається обмеженою.

Суттєвим ризиком є деформована структура власності, коли через воєнні дії й окупацію змінився баланс між приватним, державним і комунальним

секторами. Частина підприємств перейшла у стан банкрутства або фактичної безгосподарності, що викликало концентрацію активів у руках обмеженого кола суб'єктів [71]. Це породжує нові соціальні напруження, ризики неформального перерозподілу ресурсів і ускладнює повернення інвесторів. Питання справедливого відновлення майнових прав стає критерієм не лише економічної, а й моральної легітимності державної політики.

Водночас ключовим чинником є соціальна травматизація населення. Мешканці деокупованих територій зазнали тривалого впливу окупаційного режиму, що призвело до втрати відчуття безпеки, руйнування горизонтальних зв'язків і недовіри до інститутів влади. Дослідження гуманітарних організацій свідчать, що понад 65 % жителів таких громад не беруть участі у публічних консультаціях або проєктах відбудови, вважаючи їх «символічними» [157]. Це створює феномен «мовчазних територій», де державні програми не мають соціальної підтримки. Відновлення тут вимагає не лише будівництва, а й психологічної реконсолідації суспільства – створення центрів підтримки, освітніх і медіаініціатив, які сприяють поверненню довіри до держави.

Особливої уваги потребує криза ідентичності локальних спільнот, спричинена розривом між довоєнними соціальними практиками та новою реальністю. Частина громад втратила історичну спадкоємність управління, що унеможливлює опору на традиційні місцеві еліти чи форми самоврядування. У результаті процес відновлення нагадує не реконструкцію, а «перезаснування» – створення нових соціальних і культурних структур із нуля. Цей процес вимагає глибокої інституційної рефлексії, тобто усвідомлення того, що повернення до довоєнного стану є неможливим, а нова модель розвитку має будуватись на принципах участі, відкритості й колективної відповідальності.

Нарешті, варто наголосити, що управлінські виклики у таких умовах виходять за межі адміністративної логіки. Йдеться про цивілізаційний тип кризи, коли завдання держави – не лише організувати відновлення, а створити простір довіри, нової соціальної справедливості й територіальної інтеграції. Без відновлення морального, правового й культурного фундаменту деокупованих територій навіть найефективніші програми реконструкції ризикують

залишитися формальними. Тому управління відновленням має трансформуватись у політику гуманітарного перетворення, де інфраструктура є не самоціллю, а інструментом повернення людини у власний соціальний і цивілізаційний простір.

Формування системи постокупаційного відновлення має виходити з логіки резильєнтного державного управління: від разових проєктів – до постійної політики, від механічної реконструкції – до інституційного перетворення. Рекомендовано запустити Національну програму «Resilient Recovery» як єдиний каркас координації політик, фінансування та моніторингу; затвердити регіональні плани відновлення з ризик-орієнтованою пріоритизацією критичних об'єктів; запровадити цифрові «відновлювальні паспорти» активів для наскрізного контролю «кошти-роботи-ефект»; синхронізувати розмінування, екоаудит і відбудову в єдиний процес; розгорнути партнерські платформи «громади-уряд-донори-бізнес» для співфінансування; інституціоналізувати центр відновлювальної аналітики для безперервного вимірювання результатів і корекції політик; вирішити земельно-кадастрові та майнові спори прискореними адміністративними процедурами; забезпечити кадрову спроможність через регіональні центри перекваліфікації; запровадити стандарти прозорості та соціального аудиту, що повертають довіру й залучають населення до планування. Очікуваний системний ефект - прискорення темпів відновлення на 30–40 %, зниження втрат ресурсів щонайменше на 20 %, вирівнювання регіональних диспропорцій, зростання довіри до публічних інститутів.

Наукове обґрунтування системи відновлення можна звести до інтегрованих стратегічних орієнтирів представлених у табл. 5.12. Так, інституційна інтеграція задає «довгу рамку»: рішення про відновлення плануються не під грантовий цикл, а під багаторічні бюджетні зобов'язання; у результаті підрядники отримують передбачуване фінансування, а регіони– стабільний темп робіт.

Таблиця 5.12

Стратегічні орієнтири системи повоєнного відновлення та очікувані результати*

Орієнтир	Мета та управлінський сенс	Ключові інструменти реалізації	Індикатори/KPI та очікувані результати
Інституційна інтеграція «Resilient Recovery»	Перетворити відбудову на постійну державну функцію	Національна програма; міжвідомча рада; багаторічні бюджетні зобов'язання. *Інноваційний інструментарій*: урядовий офіс інновацій; Delivery Units при міністерствах; Ukraine Donor Platform (портфельне управління); цифрова платформа координації проєктів (DREAM як «єдине вікно»); аналітичні панелі моніторингу виконання бюджетних зобов'язань	Узгодження 90% проєктів із бюджетним циклом; скорочення часу погоджень на 25–30%
Регіональні плани з ризик-пріоритизацією	Вирівняти просторову асиметрію темпів відновлення	Карти ризиків/потреб; кластерні «коридори» відновлення. *Інноваційний інструментарій*: ГІС-платформи з просторовою аналітикою; супутниковий моніторинг (Copernicus EMS, UN-SPIDER); аналітичні модулі пріоритизації об'єктів за соціальною важливістю; цифрові двійники територій для сценарного моделювання	Збільшення частки проєктів у деокупованих районах до ≥50% регіонального портфеля; зменшення «прогалин» між областями на 40%
Цифрові «відновлювальні паспорти» активів	Забезпечити наскрізну прозорість і контроль	Паспорт об'єкта (стан, кошти, підрядник, ефект), інтегрований із DREAM та Prozorro. *Інноваційний інструментарій*: цифрова платформа моніторингу DREAM 2.0; модуль DOZORRO для аналізу тендерів; аналітичні модулі автоматичної валідації даних; API-інтерфейси для незалежного аудиту; «цифрові підписи» результатів	Автоматичне оновлення статусів; скорочення звітного циклу з 14 до 3 днів; повний ланцюг відстежуваності
Єдине вікно «Розмінування-Екоаудит-Відбудова»	Усунути критичні вузькі місця старту робіт	Спільні протоколи UNMAS/ДСНС/міністерств; обов'язковий еко-чек. *Інноваційний інструментарій*: цифрова платформа координації міжвідомчих протоколів; ГІС-карти забруднених територій; аналітичні модулі оцінювання ризиків (мінна небезпека + екологічний стан); алгоритми підтримки рішень щодо послідовності операцій	100% проєктів на деокупованих територіях проходять мін-кліренс та еко-скринінг; нуль інцидентів на майданчиках
Фінансова диверсифікація та співфінансування	Зменшити залежність від коротких грантів	Резерви регіонів; resilience-/recovery-bonds; співфінансування «Team Europe». *Інноваційний інструментарій*: Performance-Based Budgeting / Results-Based Financing (RBF); портфельне управління Stage-Gate; ESG-рамки та «зелена відбудова»; аналітичні модулі оцінювання ефективності витрат; цифрові трекери фінансових потоків	Частка довгих грошей (3–5 р.) ≥60%; мультиплікація кожної грн бюджету до 1,4–1,6 грн

Кадрова спроможність і мобільні інженерні підрозділи	Закрити дефіцит компетенцій на місцях	Регіональні центри перекваліфікації; мобільні інженерні «task-forces». *Інноваційний інструментарій*: competence-based програми навчання (data literacy, risk management, BIM-технології); національна школа публічного лідерства; мікрокваліфікації; цифрові платформи навчання; communities of practice; наставництво та knowledge transfer	2–3 місяці на виведення об'єкта в експлуатацію після проєктування; ≥1 тис. фахівців/рік перекваліфікації у прифронтових регіонах
Правова реконсолідація земель і майна	Розблокувати інвестиції через правову визначеність	Відновлення кадастрів; прискорені адмін-процедури; компенсаційні реєстри. *Інноваційний інструментарій*: цифрова платформа «єдиного вікна» адмін-процедур; інтеграція кадастрових реєстрів із DREAM; аналітичні модулі виявлення конфліктів титулів; алгоритми автоматизованого погодження; blockchain-верифікація прав	100% відбудовчих майданчиків із чинними титулами; скорочення спорів на 50%
Соціальна реконсолідація та участь громад	Легітимізувати пріоритети та підвищити ефективність	Публічні консультації; соціальний аудит; програми ПТСР/зайнятості. *Інноваційний інструментарій*: платформи краудсорсингу та партисипативного планування; Public Accountability Dashboards; цифрові панелі моніторингу (Spending.gov.ua, Civic Insights); інструменти е-консультацій; «citizen scorecards»; партисипативне бюджетування	≥60% ВПО повернулись у «якірні» громади; приріст участі мешканців у відборі проєктів до 40%
Екологічна резильєнтність	Запобігти «зеленому відставанню»	Обов'язкова LCA/енерго-моделювання; зелена генерація; відновлення ґрунтів. *Інноваційний інструментарій*: аналітичні модулі екологічного моніторингу; ГІС-карти деградованих площ; цифрові двійники для енерго-моделювання; ESG-критерії у відборі проєктів; алгоритми оптимізації енергоспоживання (Energy Resilience Dashboard)	−15% енерговитрат об'єктів; відновлення/рекультивація деградованих площ ≥10%/рік
Аналітика результатів і політичне навчання	Перейти від виконання до керування ефектами	Наццентр відновлювальної аналітики; панелі KPI; щорічний «policy update». *Інноваційний інструментарій*: трикомпонентний інноваційний інструментарій (цифрові платформи моніторингу + аналітичні модулі оцінювання + алгоритми підтримки рішень); прогнозні моделі та сценарний аналіз; цифрові двійники; evidence-based policy tools; «rapid-cycle evaluation»; незалежна верифікація алгоритмів	Корекція портфеля щопівріччо; приріст «ефекту на 1 грн» ≥20% за 2 роки

*Джерело: власна розробка автора

Регіональні плани з ризик-пріоритизацією трансформують просторово-ресурсну діагностику у черговість дій: наприклад, зони з критичним дефіцитом води й електрики переходять у перший кошик, транспортні «вузли-акселератори» - у другий, соціальна інфраструктура - у третій; це вирівнює асиметрію та пришвидшує повернення населення. Цифрові «відновлювальні паспорти» зшивають розрізнені реєстри в єдиний контур: у паспорті фіксуються технічний стан, бюджет, хід робіт, приймання, введення в експлуатацію та ефект (наприклад, зменшення часу доїзду швидкої на 12 хвилин чи скорочення втрат у мережі на 8 %). Завдяки повній відстежуваності зникають «сірі» зони між коштами, актами й результатами.

Єдине вікно «Розмінування-Екоаудит-Відбудова» розблоковує старт робіт: розмінування ділянки, еко-скринінг і технічне завдання проходять одним пакетом, що зменшує паузи між етапами і гарантує безпеку на майданчиках; в типових громадах це скорочує «час до першої коперти» з 90–120 до 30–45 днів. Фінансова диверсифікація додає «довгі гроші»: частина портфеля фінансується через облігації стійкості й співфінансування з «Team Europe», отже проєкти з багаторічним циклом (мости, підстанції, водогони) не «висять» між траншами, а виконуються без розривів. Кадрова спроможність забезпечується через двошаровий підхід: короткі інтенсивні програми перекваліфікації для місцевих кадрів і розгортання мобільних інженерних груп, які заходять «пакетом» у кластер пріоритетів і передають майданчики місцевим експлуатаційникам.

Правова реконсолідація земель і майна прибирає найболючіший стоп-фактор: кадастрові прогалини і спірні титули. Відновлення електронних кадастрів, прискорені адмінпроцедури та компенсаційні реєстри роблять майданчик «чистим» для інвестора; це безпосередньо впливає на леверидж - приватний капітал заходить у партнерські моделі з меншим ризиком. Соціальна реконсолідація повертає легітимність: громади беруть участь у визначенні пріоритетів через відкриті консультації та соціальний аудит, а паралельні програми ПТСР і зайнятості зменшують соціальне напруження; це прямо корелює зі швидкістю повернення ВПО і стабільністю попиту на послуги інфраструктури. Екологічна резильєнтність не дозволяє «будувати старе»: кожен

проєкт проходить LCA/енерго-моделювання, що дає економію енергії 10–15 % уже на етапі проєктування; у водних та ґрунтових проєктах закладаються рекультивація і біоінженерія, що знижує довгострокові витрати на утримання.

Нарешті, аналітика результатів і політичне навчання замикають цикл. Національний центр відновлювальної аналітики агрегує дані з паспортів і регіональних планів, розраховує «ефект на 1 грн» у розрізі секторів і щопівроку пропонує корекції: переміщення коштів у швидші напрямки, оновлення стандартів, зміни до регламентів. Це переводить управління відбудовою у режим постійної адаптації: портфель рішень не «замерзає», а підлаштовується під фактичні результати, ризики та можливості співфінансування. У підсумку система працює як єдина архітектура -стратегічна рамка, регіональні плани, цифрові паспорти, блок «розмінування-еко-відбудова», фінансові й кадрові механізми та аналітика - що разом забезпечує прогнозоване прискорення темпів, контроль якості, прозорість і відновлення довіри на деокупованих територіях.

Функціонування системи постокупаційного відновлення критичної інфраструктури реалізується через Resilient Recovery Package - інтегрований управлінський пакет, який поєднує нормативні, фінансові, технологічні та соціальні інструменти у єдину динамічну систему. Його структура базується на принципі «відновлення як управлінський цикл», де всі елементи - від діагностики до моніторингу ефекту - працюють у синхронному режимі даних і зворотного зв’язку. Пакет не є статичною програмою, а функціонує як операційна екосистема, що реагує на зміни середовища, ризики та потреби громад у режимі реального часу.

Resilient Recovery Package покликаний забезпечити безперервність управління відбудовою критичної інфраструктури, інтегруючи просторові карти руйнувань, дані розмінування, аналітику ресурсів і цифрові паспорти об’єктів у єдиний управлінський контур. Завдяки цьому система відновлення стає самонавчальною: кожне рішення, виконання і наслідок створюють нові дані, що повертаються у планування наступного циклу. Така логіка відповідає європейським підходам «evidence-based recovery» і перетворює процес відбудови на постійну державну функцію (рис. 5.10).

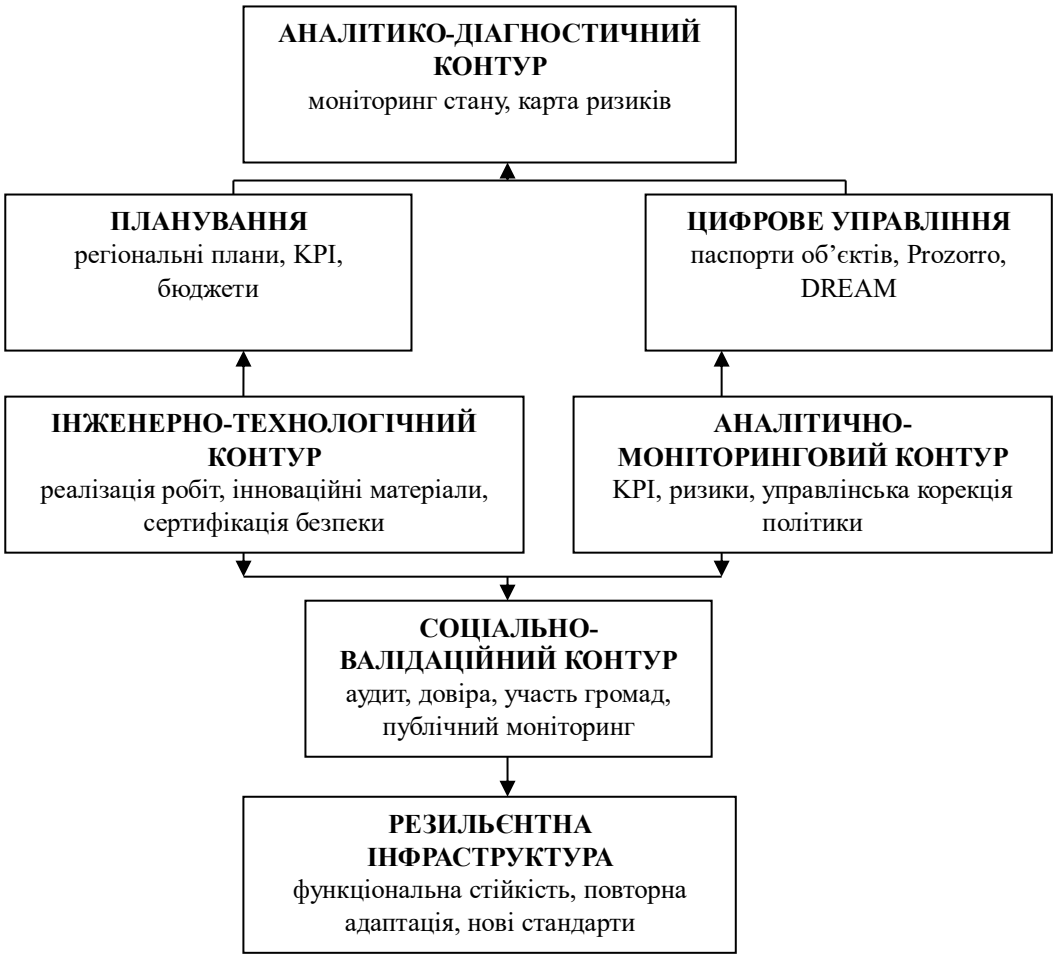


Рис. 5.10. Операційна архітектура пакету «Resilient Recovery Package» (цикл управління відновленням критичної інфраструктури)*

*Джерело: власна розробка автора

Запропонований Resilient Recovery Package – це не просто набір інструментів, а керований алгоритм дій, який замикає повний управлінський цикл у сфері критичної інфраструктури.

На першому етапі створюється аналітико-діагностичний контур, який формує цифрову карту пошкоджень і рівнів стійкості територій. Це дозволяє виявити вузли, без яких функціонування системи неможливе – енергетичні підстанції, мости, логістичні центри, очисні споруди.

Далі працює планувально-програмний контур, де приймаються стратегічні рішення: регіональні плани інтегруються у Національну програму, визначаються пріоритети, бюджети й виконавці. Важливо, що планування відбувається з урахуванням ризиків повторного ураження, техногенних загроз і кліматичних чинників, а не лише за принципом черговості руйнувань.

Цифровий контур забезпечує прозорість - через систему «відновлювальних паспортів» кожен об’єкт має повний цифровий профіль, доступний для моніторингу урядом, громадами й міжнародними донорами. На цьому рівні відбувається автоматичний контроль виконання, бюджетного використання і соціального ефекту.

Під час інженерно-технологічного контуру реалізуються роботи із застосуванням сучасних рішень: модульного будівництва, 3D-друку бетонних елементів, використання ультра високоефективних матеріалів, автономних енергетичних систем. Завдяки цьому об’єкти не просто відновлюються, а стають більш стійкими, з енергоефективністю на 20–30 % вищою за довоєнний рівень.

Аналітично-моніторинговий контур функціонує як «мозок системи» – він збирає всі дані, аналізує ефективність, визначає ризики і пропонує управлінські корекції. Цей рівень дозволяє уряду й громадам діяти не реактивно, а прогнозно.

Соціально-валідаційний контур завершує цикл - саме тут відбувається перевірка результатів з боку громад і суспільства. Проводяться відкриті консультації, соціальні опитування, оцінюється рівень довіри, формується громадський аудит. Цей механізм гарантує не лише прозорість, а й соціальну легітимність державної політики.

Фінальний результат - резильєнтна інфраструктура, тобто система, здатна не лише відновитись, а й утримувати функціональність у кризових умовах. У практичному вимірі реалізація пакету дозволяє скоротити середній час від технічної діагностики до повного введення об’єкта в експлуатацію з 18–24 до 10–12 місяців, знизити втрати енергії на 15–20 %, а також підвищити довіру населення до процесів відновлення на 30–35 %.

Висновки до розділу 5

1. У процесі дослідження обґрунтовано, що трансформація публічного управління у сфері критичної інфраструктури потребує переосмислення базових принципів і переходу від адміністративно-командної моделі до адаптивної,

аналітично обґрунтованої та поліцентричної системи управління. Встановлено, що ефективність державних рішень у воєнний та післявоєнний період визначається здатністю органів влади забезпечувати безперервність управлінського циклу «дані – аналіз – дія – оцінювання – корекція» та підтримувати інтеграцію між секторами безпеки, економіки й соціальної стабільності.

Розроблено Концепцію публічного управління трансформацією об’єктів критичної інфраструктури, побудовану на принципах resilience, adaptive та collaborative governance, що забезпечує координацію дій центральних, регіональних і місцевих інституцій у межах єдиного цифрово-аналітичного контуру. Доведено, що запровадження систем типу DREAM, Rebuild Ukraine Platform, інтегрованих аналітичних панелей і механізмів зворотного зв’язку між громадами та державою створює нову якість управлінських рішень, орієнтованих на результат і довіру.

Сформовано методичні засади інтеграції даних, нормативів і фінансових ресурсів у межах операційної моделі “data–coordination–adaptation–evaluation”, яка дозволяє прогнозувати вразливості системи, моделювати сценарії реагування та оперативно коригувати політику. Результати дослідження підтверджують, що впровадження нової концепції дає змогу підвищити керованість і прозорість процесів трансформації критичної інфраструктури, знизити часові втрати при ухваленні рішень і сформувати основу для стабільного функціонування державних інституцій у середовищі невизначеності.

2. У ході дослідження ідентифіковано та систематизовано ключові інструменти інноваційного управління, що забезпечують модернізацію системи державного управління критичною інфраструктурою. Визначено, що впровадження інновацій має відбуватися через створення інтегрованої екосистеми, у якій уряд, бізнес, наукові установи та громади взаємодіють на основі відкритих даних, спільних стандартів і компетентнісного підходу.

Розроблено модель поетапного впровадження інноваційних механізмів, яка передбачає створення урядового офісу інновацій, побудову інтегрованої data fabric для обміну управлінською інформацією, формування мереж sandbox-

проєктів і програм підготовки кадрів за принципом competence-based learning. Показано, що реалізація такої моделі дозволяє долати нормативну інерцію, фрагментацію цифрових систем і кадровий дефіцит, забезпечуючи водночас гнучкість та адаптивність рішень.

Встановлено, що ефективне використання інноваційних інструментів сприяє скороченню часу ухвалення управлінських рішень, підвищенню якості публічних послуг, прозорості фінансових потоків і зростанню довіри громадян до держави. Досягнуто концептуального узагальнення, згідно з яким інноваційність у сфері управління критичною інфраструктурою розглядається не лише як технологічна, а й як управлінська категорія, що формує основу для динамічної адаптації державних інституцій до змінних зовнішніх умов.

3. Дослідження процесів відновлення критичної інфраструктури на деокупованих територіях України засвідчило, що головним викликом є необхідність поєднання технічного відновлення з інституційним, соціальним і безпековим відродженням. Встановлено, що ефективність політики відновлення залежить від здатності держави створити багаторівневу систему управління, де місцеві органи влади, міжнародні донори, приватний сектор і громади діють у координованому режимі з використанням цифрових платформ моніторингу та аналітичних інструментів оцінювання ризиків.

Розроблено структурну модель управління відбудовою, яка включає етапи гуманітарного розмінування, оцінювання руйнувань, пріоритизації інвестицій, проєктування за принципами «build back better» і подальшої інтеграції відновлених об’єктів у національні мережі енергетики, транспорту та комунікацій. Наголошено на необхідності врахування принципів енергоефективності, екологічної безпеки та інклюзивності при розробленні проєктів відновлення.

Виявлено, що поєднання локальної автономії територіальних громад із державним стратегічним контролем створює оптимальну модель управління, яка забезпечує гнучкість та узгодженість дій. Доведено, що системна координація відновлення через єдиний цифровий простір підвищує ефективність використання ресурсів і прискорює процес повернення функціональності

критичних об’єктів до 70–80 % у середньостроковій перспективі. У результаті визначено, що саме комплексне управління, побудоване на принципах стійкості, безпеки та соціальної відновлюваності, є ключовим чинником формування довготривалого потенціалу розвитку деокупованих територій і консолідації державної політики відбудови.

ВИСНОВКИ

У дисертаційному дослідженні обґрунтування комплексу концептуальних положень та формування практичних рекомендацій щодо удосконалення публічного управління у сфері трансформації об'єктів критичної інфраструктури. Отримані в процесі дослідження результати дали змогу сформулювати такі висновки та пропозиції:

1. Вивчено стан наукової розробки проблематики та ключові концепції публічного управління у сфері трансформації об’єктів критичної інфраструктури. Це зроблено шляхом поєднання трьох груп ознак функціональних, секторних і ризик-орієнтованих. Виокремлено критерії критичності, що враховують, як саме об’єкт інфраструктури впливає на суспільні процеси, наскільки глибокими є його міжсекторальні залежності та яких масштабів втрат можна очікувати в майбутньому. Запропоновано структуризацію об’єктів КІ за ієрархічними та мережевими характеристиками, а також встановлено прямий зв’язок між типом об’єкта та набором управлінських інструментів. Виявлено взаємозалежності між різними секторами критичної інфраструктури України складають основу її стійкості, стабільності та функціональної надійності. З’ясовано, що чим вищим є рівень інтеграції енергетичних, логістичних і цифрових систем, тим складнішими стають процеси управління. Виокремлено наукові підходи до публічного управління критичною інфраструктурою: системний; гнучкий підхід; ризик-орієнтований; централізований; фрагментований; інституційне забезпечення; державно-приватне партнерство; міжнародне партнерство.

2. Обґрунтовано функції та вивчено загрози публічного управління у сфері трансформації об’єктів критичної інфраструктури та розкрито їх змістові особливості. Функції: за сферами впливу: політико-адміністративна; економічна; соціальна; оборонна; загальні функції: планування; регулювання; координація; облік; контроль; допоміжні функції: кадрова; матеріально-технічна; діловодство. Запропоновано класифікацію загроз із прив’язкою до конкретних типів інфраструктури та характеру впливу: кібератаки; залежність від технологій;

фізичні атаки; пандемії та надзвичайні ситуації у сфері охорони здоров'я; проблеми у ланцюзі поставок; гібридні загрози та цільові атаки; дестабілізація суспільства; стихійні лиха. Головною особливістю публічного управління критичною інфраструктурою є те, що воно має багатокомпонентну структуру, впровадження якої обумовлено необхідністю забезпечення безперервності функціонування стратегічно важливих об'єктів, їх захищеності та здатності прогнозувати та уникати різноманітні загрози. Основними напрямками публічного управління критичною інфраструктурою визначено: стратегічне планування; управління активами; аналіз даних і прогнозне технічне обслуговування; системи збору даних; системи резервування та резервного копіювання; безпека і захист інформації; моніторинг і безпека мережі; віддалений моніторинг і контроль; системний моніторинг та оцінка ризиків; запобігання кризам та надзвичайним ситуаціям; ризик-орієнтовний підхід; реагування на інциденти та аварійне відновлення; співпраця та обмін інформацією; публічно-приватне партнерство.

3. Сформовано комплексний механізм публічного управління трансформацією об’єктів критичної інфраструктури України. Його основу становить нормативно-правовий, інституційний, організаційно-інформаційний, фінансово-економічний, технологічний та цифровий механізми. Нормативно-правовий механізм, що визначає правові засади функціонування інфраструктури, повноваження суб’єктів управління та вимоги до безпеки. У межах механізму виділено взаємопов’язані блоки: а) блок стратегічного планування, б) блок координації та в) блок операційного реагування. Додатково введено компонент управління міжсекторальними залежностями, який дозволяє враховувати ефекти взаємного впливу інфраструктурних систем. Така будова підвищує узгодженість рішень, скорочує часові лаги реагування та забезпечує адаптацію системи до змін безпекового середовища. Визначено функціональні зв’язки між стратегічним плануванням, координаційними процедурами та операційними діями. Побудовано організаційний підхід до розподілу повноважень, де враховано рівень відповідальності суб’єктів управління та їхній доступ до ресурсів.

4. Узагальнено пропозиції щодо доповнення нормативно-правового забезпечення функціонування захисту, безпеки, стійкості та трансформації об’єктів критичної інфраструктури в сучасних умовах. Дослідження правового забезпечення публічного управління критичною інфраструктурою показало необхідність інтеграції безпекових та управлінських компонентів. Чинна нормативна база, як встановлено в роботі, створює загальний каркас інституційної взаємодії, визначає процедури категоризації, моніторингу та захисту об’єктів. Однак виявлено суттєві розриви між секторальними регуляціями та механізмами кризового реагування, що ускладнює узгодження дій. Пріоритетними напрямками удосконалення правового забезпечення публічного управління об’єктами критичної інфраструктури визначено: оновлення оцінок ризиків з урахуванням поточних загроз (адаптація національних оцінок ризиків до сучасних викликів за спільними принципами ЄС); проведення стрес-тестів у ключових секторах (перевірка готовності критичних об'єктів до екстремальних ситуацій); розробка національного плану реагування на значні інциденти в критичній інфраструктурі (дорожня карта міжвідомчого реагування на кризи, зокрема транскордонні); посилення міжнародного співробітництва з питань безпеки критичної інфраструктури (співпраця та обмін інформацією з ЄС, НАТО, США та Канадою); залучення до європейських дослідницьких програм із безпеки критичної інфраструктури (участь у Horizon Europe для фінансування та розроблення інноваційних рішень); формування єдиного управлінського механізму щодо захисту критичної інфраструктури (ієрархічна система координації, нагляду й контролю на рівні державної політики); створення національної довідкової мережі захисту критичної інфраструктури (платформа обміну досвідом і найкращими практиками на зразок ERNCIP).

5. Розроблено організаційно-управлінську модель функціонування системи публічного управління трансформацією об’єктів критичної інфраструктури. У результаті проведеного дослідження деталізовано складові структури інтегрованого організаційно-управлінського механізму публічного управління у сфері трансформації об’єктів критичної інфраструктури, до якого

функціонально включено п’ять ключових блоків: інвентаризаційний – відповідальний за систематизацію наявного стану інфраструктурних об’єктів за участю Міністерства розвитку громад, територій та інфраструктури України; координаційний – що забезпечує міжвідомчу взаємодію між такими суб’єктами, як Державна служба з надзвичайних ситуацій України, Державна служба спеціального зв’язку та захисту інформації України, Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг, а також обласними військовими адміністраціями; прогнозно-плановий – який реалізується через участь центральних і місцевих органів виконавчої влади у формуванні рішень щодо технічного переоснащення інфраструктурних об’єктів; ресурсно-технічний – орієнтований на забезпечення інженерної, матеріальної та кадрової спроможності системи; та інформаційно-аналітичний – що базується на зборі, обробці та обміні управлінською інформацією в рамках дії національної системи забезпечення функціонування критичної інфраструктури.

6. Досліджено та запропоновано маркери імплементації міжнародного досвіду забезпечення кібербезпеки критичної інфраструктури. Комплексний аналіз міжнародного досвіду (країни ЄС, США, Канада, Ізраїль, Австралія) засвідчив, що ефективні системи забезпечення стійкості та кіберзахисту критичної інфраструктури базуються на трьох компонентах: нормативне регулювання, цифрові платформи обміну даними та чіткі процедури координації між державою й приватними операторами. Досліджено трирівневі моделі оцінювання ризиків, які дають змогу виявляти загрози на ранніх стадіях і формувати сценарії реагування. Встановлено, що централізовані інформаційні платформи забезпечують безперервний моніторинг і передачу аналітичних сигналів між рівнями управління. Запропоновано імплементувати механізми державно-приватного партнерства для формування спільної відповідальності за захист інфраструктури. Визначено параметри адаптації міжнародних стандартів до національних умов із урахуванням безпекових викликів та технологічних можливостей. Сформовано та доповнено систему маркерів імплементації зарубіжного досвіду, що охоплюють інституційні, технологічні та процедурні параметри адаптації і включає рівень готовності нормативного середовища,

ступінь інтеграції цифрових платформ, наявність механізмів обміну інформацією та швидкість реагування на кіберзагрози.

7. Запропоновано класифікаційні ознаки оцінювання стану пошкодження та руйнувань об’єктів критичної інфраструктури у період воєнного стану, серед них: функціональні втрати об’єкта; глибина структурних пошкоджень; тривалість відновлення; ступінь критичності порушення; масштаб впливу на суміжні сектори; каскадність поширення збоїв; просторові особливості руйнувань. Оцінка стану критичної інфраструктури України в умовах війни (2024-2026 рр.) показала, що найбільших руйнувань зазнав енергетичний сектор: пошкоджено як генеруючі потужності, так і мережі передачі електроенергії. Дослідження фіксує руйнування Каховської ГЕС, пошкодження теплових електростанцій, порушення логістичних зв’язків і функціонування транспортної системи. Ступінь руйнувань, як виявлено, прямо залежить від інтенсивності бойових дій і територіального розташування об’єктів. Обґрунтовано необхідність створення системи безперервного моніторингу стану об’єктів критичної інфраструктури, яка б формувала актуальну аналітику для ухвалення управлінських рішень.

8. Розроблено методичний підхід до оцінювання рівня ефективності публічного управління об’єктами критичної інфраструктури в Україні. Сформовано методику та систему індикаторів ефективності публічного управління об'єктами КІ за рівнями управління та індикаторами: частка часу безперебійного надання життєво важливих послуг; середня тривалість відновлення після масованих атак; обсяг економічних втрат від порушень функціонування критичної інфраструктури; частка населення, забезпеченого базовими послугами під час кризи; час відновлення послуг у регіоні; кількість громад із тривалими перебоями; коефіцієнт готовності об'єкта; кількість інцидентів, що призвели до припинення послуги; частка відновленої функції за нормативний строк; здатність до відновлення функціонування. На основі аналітичних оцінок і фінансових прогнозів обґрунтовано наукові підходи до формування політики відбудови критичної інфраструктури України. Встановлено відсутність узгодженої системи стратегічних документів, що

ускладнює реалізацію відновлювальних процесів і розподіл ресурсів. Звіти типу RDNA, хоч і дають точну оцінку втрат і потреб у фінансуванні, не пропонують механізмів практичної реалізації відбудови. Виявлено розрив між аналітичними даними та реальними управлінськими рішеннями, що знижує ефективність планування. Запропоновано сформувати систему стратегічних документів, яка включатиме дорожні карти, індикатори пріоритетності та механізми координації між різними рівнями управління, з обов'язковою інтеграцією міжнародного досвіду. Розроблено методичний підхід до управління проєктами відновлення критичної інфраструктури, який поєднує структуровані та адаптивні методології. Пропонується використовувати стандарти PMBoK для формалізації етапів реалізації, розподілу відповідальності та контролю ресурсів, а також гнучкі підходи (Agile) для швидкого коригування рішень у разі зміни умов.

9. Обґрунтовано Концепцію публічного управління у сфері змін об'єктів критичної інфраструктури, як інтегрованої системи взаємодії управлінських контурів із безперервним циклом обробки даних та ухвалення рішень. Методологічною основою триконтурної Концепції публічного управління у сфері змін об'єктів критичної інфраструктури виступає сценарне планування. У межах запропонованого підходу виділено щонайменше чотири базові сценарії: 1) стабілізаційний – помірний рівень загроз, поступове відновлення та модернізація; 2) кризовий – періодичні атаки та локальні руйнування, що вимагають оперативного реагування та резервування; 3) надзвичайний – масовані удари по критичних об'єктах, що потребують негайної мобілізації ресурсів і тимчасового переходу до централізованого управління; 4) трансформаційний – постконфліктне відновлення з акцентом на інноваційну модернізацію та інтеграцію до європейських стандартів. Визначено механізм узгодження рішень між рівнями влади через цифрові платформи, що синхронізують інформаційні потоки та забезпечують зворотний зв'язок. Запропонована операційна модель інтегрує ресурси, нормативні вимоги та аналітичні інструменти в єдину систему, змінюючи логіку управління від фрагментарних дій до цілісного адаптивного процесу.

10. Розроблено інноваційний інструментарій публічного управління трансформацією об’єктів критичної інфраструктури Інноваційний інструментарій публічного управління трансформацією об’єктів критичної інфраструктури, який функціонує через 1) цифрові платформи моніторингу, 2) аналітичні модулі оцінювання стану об’єктів та 3) алгоритми підтримки управлінських рішень. Інструментарій забезпечує збір і обробку інформації про стан інфраструктури, формування аналітичних сигналів та передачу їх суб’єктам управління. Запропоновано цифрову архітектуру обміну даними, що забезпечує доступ до актуальної інформації для формування управлінських рішень. Запропоновано механізм реалізації інновацій через поетапне впровадження інструментів: експериментальні проєкти, навчальні програми та стандарти обробки даних. Така конструкція забезпечує гнучке впровадження нових рішень, скорочує час адаптації системи до змін і підвищує узгодженість дій учасників.

11. Обґрунтовано заходи публічного управління по відновленню об’єктів критичної інфраструктури України у повоєнному періоді. Розроблено управлінську архітектоніку інтеграції відбудови у систему державної політики, що сформована на таких рівнях: стратегічний рівень: інституціалізація відбудови у державну політику; координаційний рівень: узгодження між секторами, регіонами та донорами; операційний рівень: програмно-цільове управління проєктами; аналітичний рівень: моніторинг, оцінка впливу, аналітика даних; соціальний рівень: участь громад, комунікація, соціальний аудит; основа: політика відновлювальної резильєнтності. Запропоновано модель публічного управління відновленням критичної інфраструктури яка поєднує етапи оцінювання, планування та реалізації відбудови. Кожен етап має чітко визначені процедури – від аналізу пошкоджень до інтеграції відновлених об’єктів у національні системи. Передбачено використання цифрових платформ для координації дій між державними органами, місцевими громадами та приватним сектором. Визначено механізм розподілу ресурсів, що враховує рівень пошкодження об’єктів, їхню значущість і взаємозалежність між системами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Азаренко О. Шляхи підвищення ефективності системи фізичного захисту об’єктів критичної інфраструктури держави, що охороняються / О. Азаренко, Ю. Гончаренко, М. Дівізіньюк, В. Мирненко, В. Стрілець // Журнал наукових праць. Соціальний розвиток і безпека [Текст]. — 2021. — № 11. — С. 200—213.

2. Андрієнко Д., Горюнов Д., Грудова В., Маркуц Ю., Маршалок Т., Нейтер Р., Піддубний І., Студеннікова І., Топольськов Д. Звіт про прямі збитки інфраструктури від руйнувань внаслідок військової агресії Росії роти України станом на листопад 2024 року // Київська школа економіки (KSE) [Електронний ресурс]. — Режим доступу : https://kse.ua/wp-content/uploads/2025/02/KSE_Damages_Report-November-2024-UA.pdf

3. Арсенович Л. А. Деякі питання запровадження системи підготовки фахівців у сфері захисту критичної інфраструктури / Л. А. Арсенович // Таврійський науковий вісник. Серія: Публічне управління та адміністрування [Текст]. — 2023. — № 5. — С. 3—14.

4. Балан А. А. Критична інфраструктура в контексті виживання територіальної громади / А. А. Балан // Економічний журнал [Текст]. — 2024. — № 4. — С. 127—133.

5. Безпека критичної інфраструктури в Україні: теоретико прикладні засади державного управління [Текст]: монографія / авт. С. Домбровська, В. Шведун. — НУЦЗУ, 2024. — С. 227.

6. Бірюков Д. С. Захист критичної інфраструктури в Україні: від наукового осмислення до розробки засад політики / Д. С. Бірюков // Науково-інформаційний вісник Академії національної безпеки [Текст]. — 2015. — № (3–4). —С. 155—170.

7. Бірюков Д. С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Аналітична доповідь // Національний інститут стратегічних досліджень [Електронний ресурс]. — Режим доступу : https://niss.gov.ua/sites/default/files/2013-02/Sots_zahust-86178.pdf

8. Бірюков Д. С., Кондратов С. І., Насвіт О. І., Суходоля О. М. Зелена книга з питань захисту критичної інфраструктури в Україні // Національний інститут стратегічних досліджень [Електронний ресурс]. — Режим доступу : https://cdn.regulation.gov.ua/6a/69/2a/fa/regulation.gov.ua_File_188.pdf.

9. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі / Д. Г. Бобро // Стратегічні пріоритети. Серія: Економіка [Текст]. — 2015. — № 4. — С. 83—93.

10. Богдан Б. В. Актуальні питання нормативно-правового регулювання захисту критичної інфраструктури в умовах воєнного стану в Україні / Б. В. Богдан // Проблеми сучасних трансформацій. Серія : право, публічне управління та адміністрування [Текст]. — 2022. — № 6.

11. Бубела Т. З., Мельник М. Я., Назаровець О. Б., Рудик Ю. І. Аналіз визначень та нормативних вимог системи захисту об’єкта критичної інфраструктури / Т. З. Бубела // Вісник Львівського державного університету безпеки життєдіяльності [Текст]. — 2024. — № 29. — С. 119—127.

12. Бурик З. М., Ромахова О. О. Проблеми публічного управління відбудовою та відновленням пошкодженої і зруйнованої інфраструктури. *Інвестиції: практика та досвід*. 2024. № 8. С. 212–218. DOI: 10.32702/2306-6814.2024.8.212.

13. Войтович Л., Федик М. Стратегія повоєнного відновлення економіки України в умовах євроінтеграції / Л. Войтович, М. Федик // Економіка та суспільство [Текст]. — 2024. — № 65.

14. Гаврись А. П., Філіппова В. В., Тур Н. Ю. Інформаційний аналіз систем захисту об’єктів критичної інфраструктури в період дії воєнного стану. Регіональна економіка [Текст]. — 2023. — № 2. — С. 173—187.

15. Герасименко О. М. Загрози об’єктам критичної інфраструктури України в умовах воєнного стану. Науковий вісник Ужгородського Національного Університету. Серія: Право [Текст]. — 2024. — № 84(3). — С. 257— 263.

16. Гнатюк С. О., Бердибаєв Р. Ш., Сидоренко В. М., Жигаревич О. К., Смірнова Т. В. Система корелювання подій та управління інцидентами кібербезпеки на об’єктах критичної інфраструктури / С. О. Гнатюк //

Кібербезпека: освіта, наука, техніка [Текст]. — 2023. — Т. 3. — № 19. — С. 176–196.

17. Гора І. В., Батюк О. В. Окремі питання захисту об’єктів критичної інфраструктури: зарубіжний досвід / І. В. Гора, О. В. Батюк // Соціально-правові студії [Текст]. — 2021. — № 1 (11). — С. 132—139.

18. Грабар Н. С. Формування культури кібербезпеки в суспільстві-актуальне завдання сучасності [Електронний ресурс]. — Режим доступу :http://repositsc.nuczu.edu.ua/bitstream/123456789/12389/1/stGrabar1.pdf.

19. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки [Текст]: аналіт. доп. / за ред. О. М. Суходолі. — Київ : НІСД, 2020.

20. Деякі питання об'єктів критичної інфраструктури [Електронний ресурс] : Постанова Кабінету Міністрів України № 1109-2020-п від 24.09.2024 р. — Режим доступу : https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

21. Деякі питання оптимізації системи центральних органів виконавчої влади [Електронний ресурс] : Постанова Кабінету Міністрів України № 29-2023-п від 08.03.2023 р. — Режим доступу : https://zakon.rada.gov.ua/laws/show/29-2023-%D0%BF#Text.

22. Деякі питання паспортизації об’єктів критичної інфраструктури [Електронний ресурс] : Постанова Кабінету Міністрів України № 818 від 04.08.2023 р. — Режим доступу : https://zakon.rada.gov.ua/laws/show/1109-2020-п#Text.

23. Деякі питання подання інформації у сфері захисту критичної інфраструктури [Електронний ресурс] : Постанова Кабінету Міністрів України № 1175 від 14.10.2022 р. — Режим доступу : https://zakon.rada.gov.ua/laws/show/1175-2022-п#Text.

24. Директива Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту [Електронний ресурс]. — Режим доступу : https://zakon.rada.gov.ua/laws/show/984_002-08#Text.

25. Довгая Г. Реєстр об’єктів критичної інфраструктури: відповіді на головні питання [Електронний ресурс]. — Режим доступу :https://radnuk.com.ua/voiennyj-stan/reiestr-ob-iektiv-krytychnoiinfrastruktury-vidpovidi-na-holovni-pytannia/.

26. Домарацький М. Б. Актуальні проблеми державного управління захистом критичної інфраструктури в Україні / М. Домарацький // Публічне управління та адміністрування у процесах економічних реформ: збірник тез доповідей IV Всеукраїнської науково-практичної конференції [Текст]. — ДВНЗ «ХДАУ», 2020. — С. 172—173.

27. Євсєев В. О. Нормативно-правове забезпечення публічного управління у сфері захисту критичної інфраструктури: еволюційний аспект / В. О. Євсєев // Вісник ХНТУ [Текст]. — 2025. — № 4. — С. 413—418.

28. Єрменчук О. Оцінка загроз критичній інфраструктурі як важлива складова частина діяльності із захисту державної безпеки / О. Єрменчук // Jurnalul juridic national: teorie şi practică [Текст]. — 2018. — № 34(6). — С. 50—54.

29. Єрменчук О. П. Аналіз організації захисту об’єктів критичної інфраструктури на стратегічному рівні нормативно-правового регулювання як важлива складова забезпечення національної безпеки / О. П. Єрменчук // Бюлетень Мін'юсту України [Текст]. — 2019. — № 4. — С. 41—45.

30. Жукова І., Трушкіна Н. Державно-приватне партнерство як ключовий принцип функціонування національної системи захисту критичної інфраструктури в Україні / І. Жукова, Н. Трушкіна // Наукові інновації та передові технології [Текст]. — 2023. — № 7(21). — С. 11—26.

31. Жукова І., Трушкіна Н. Сутність поняття «механізм державного регулювання розвитку критичної інфраструктури» / І. Жукова, Н. Трушкіна // Věda a perspektivy [Текст]. — 2023. — № 6(25). — С. 8—23.

32. За два роки рф здійснила 25 масованих атак на енергетику України // Dixi Group [Електронний ресурс]. — Режим доступу : https://dixigroup.org/en/over-two-years-russia-has-carried-out-25-massive-attacks-on-ukraines-energy-sector/.

33. Загальна сума прямих збитків, завдана інфраструктурі України через війну, сягає $151,2 млрд — оцінка станом на 1 вересня 2023 року // Kyiv School of Economics [Electronic resource]. — Access mode : https://kse.ua/ua/about-the-school/news/zagalna-suma-pryamih-zbitkiv-zavdana-infrastrukturi-ukrayini-cherez-viynu-syagaye-151-2-mlrd-otsinka-stanom-na-1-veresnya-2023-roku/

34. Загоєння ран окупації: складна реальність деокупації територій України // UkraineWorld [Electronic resource]. — Access mode : https://ukraineworld.org/uk/articles/basics/deoccupying-ukraines-territories.

35. Засідання робочої групи щодо реалізації Концепції забезпечення національної системи стійкості // Вища школа публічного управління [Електронний ресурс]. — Режим доступу : https://hs.gov.ua/zasidannya-robochoyi-grupi-shhodo-realizacziyi-konczepcziyi-zabezpechennya-naczionalnoyi-sistemi-stijkosti/

36. Звіт про пошкодження інфраструктури внаслідок руйнування будівель і житлового фонду в Україні // Київська школа економіки (KSE Institute) [Електронний ресурс]. — Режим доступу : https://kse.ua/ua/about-the-kse-institute/news/zvit-pro-zavdanu-shkodu-ukraini-stanom-na-1-sichnya-2024-roku.

37. Іваницька О., Возненко О. Управління ризиками об’єктів критичної інфраструктури / О. Іваницька, О. Возненко // Фінанси України [Текст]. — 2024. — № (6). — С. 93—107.

38. Іванченко Є., Корченко О., Зарицький О., Зибін С., Вишневська Н. Аналіз поняття кіберстійкості критичної інфраструктури / Є. Іванченко // Захист інформації [Текст]. — 2023. — Т. 25. — № 4. — С. 221—233.

39. Івко А. В. Підходи синкретичного управління в проєктах відновлення дорожньої інфраструктури / А. В. Івко // Вісник Національного транспортного університету. Серія «Технічні науки» [Текст]. — 2022. — Вип. 3. — С. 53—62.

40. Казьмірук С. Д., Леонов Б. Д., Омельян О. С. Забезпечення кібербезпеки об’єктів критичної інфраструктури на основі використання штучного інтелекту в умовах воєнного стану / С. Д. Казьмірук // Юридичний науковий електронний журнал [Текст]. — 2024. — № 6. — С. 68—81.

41. Кібератаки, артилерія, пропаганда. Загальний огляд вимірів російської агресії [Електронний ресурс]. — Режим доступу :https://cip.gov.ua/ua/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimirivrosiiskoyi-agresiyi.

42. Клименко К. В., Савостьяненко М. В. Посилення захисту критичної інфраструктури: вітчизняні реалії та міжнародне співробітництво / К. В. Клименко, М. В. Савостьяненко // Економічна безпека [Текст]. — 2021. — № 2(95). — С. 44—68.

43. Конев В. Відновлення критичної інфраструктури: нестача грошей, «совок», корупція і плутанина // Дзеркало Тижня [Електронний ресурс]. — Режим доступу : https://zn.ua/ukr/reforms/vidnovlennja-kritichnoji-infrastrukturi-nestacha-hroshej-sovok-koruptsija-i-plutanina.html.

44. Кормишкіна І. В. Концептуальні основи та принципи формування системи управління комплексним відновленням територій / І. В. Кормишкіна // Modern Economics [Текст]. — 2024. — № 47. — С. 46—52.

45. Коцюруба В. І., Білик А. С., Веретнов А. О., Гайдарли Г. С., Борта Р. М., Тертишний Б. І. Методика розрахунків та обґрунтування вимог до інженерного захисту об’єктів критичної інфраструктури від БпЛА типу баражуючий боєприпас / В. Коцюруба // Опір матеріалів і теорія споруд [Текст]. — 2022. — № 109. — С. 164— 183.

46. Круглов В. В. Державно-приватне партнерство як інструмент інфраструктурного відновлення українських міст / В. В. Круглов // Актуальні проблеми державного управління [Текст]. — 2022. — № 1(60). — С. 63— 77.

47. Кузьменко Ю. В., Коропатов О. М., Думанський Р. В. Адміністративно-правове забезпечення захисту об’єктів критичної інфраструктури України під час воєнного стану / Ю. В. Кузьменко // Юридичний бюлетень [Текст]. — 2022. — С. 59-66.

48. Кушніренко О. М., Гахович Н. Г. Імплементація європейських принципів в стратегічному плануванні повоєнного відновлення України / О. М. Кушніренко, Н. Г. Гахович // Науковий вісник міжнародної асоціації

науковців. Серія: економіка, управління, безпека, технології [Текст]. — 2023. — Т. 2. — № 2.

49. Лазор О. Я., Юник І. Г. Перспективи розвитку державно-приватного партнерства у сфері захисту критичної інфраструктури в Україні / О. Я. Лазор // Наукові перспективи [Текст]. — 2024. — № 4(46). — С. 246—258.

50. Лазор О. Я., Юник І. Г., Заболотний А. В. Державна стратегія повоєнного відновлення та розвитку критичної інфраструктури в Україні / О. Я. Лазор // Державне управління: удосконалення та розвиток [Текст]. — 2024. — № 4. — С. 1—19.

51. Лелеченко А. П. Інструменти формування та реалізації універсальної моделі автономії місцевого самоврядування. *Інвестиції: практика та досвід*. 2024. № 21. С. 169–174. DOI: 10.32702/2306-6814.2024.21.169

52. Лук'яненко І. Г., Мар'янович М. Е. Роль державно-приватного партнерства в розбудові критичної інфраструктури для досягнення Цілей сталого розвитку в Україні / І. Г. Лук'яненко, М. Е. Мар'янович // Бізнес Інформ [Текст]. — 2020. — № 1. — С. 291—297.

53. Лук'янчук К. П., Самарченко І. І. Адміністрування кадрового складу підприємства та організацій критичної інфраструктури в умовах епідемії та воєнного стану: Аналітичне дослідження // ОдесаПортсмут: Одеська політехніка [Електронний ресурс]. — Режим доступу : https://economics.net.ua/files/analytics/UUT_24_Analytics_U.pdf.

54. Магомедов А. О. Особливості публічного управління об'єктами критичної інфраструктури / А. О. Магомедов // Наукові перспективи [Текст]. — 2024. — № 7(49). — С. 412—427.

55. Магомедов А. О. Публічне управління процесами трансформації критичної інфраструктури в країнах Європи / А. О. Магомедов // Успіхи і досягнення у науці [Текст]. — 2024. — № 6(6). — С. 520—537.

56. Магомедов А. О. Ризики та загрози для об'єктів критичної інфраструктури та шляхи їх подолання / А. О. Магомедов // Інвестиції: Практика та Досвід [Текст]. 2024. — 2024. — № 15. — С. 216—221.

57. Магомедов А.О. Аналіз втрат і руйнувань інфраструктури України, що підлягає відновленню. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування.* 2023. № 6. С. 62-72. DOI https://doi.org/10.32782/tnv-pub.2023.6.9.

58. Магомедов А.О. Відбудова об'єктів критичної інфраструктури України після війни: стратегія та перспективи. *Економіка, фінанси, менеджмент: актуальні питання науки і практики.* 2024. № 1 (67). С. 100-116. DOI https://doi.org/10.37128/2411-4413-2024-1-7.

59. Магомедов А.О. Державне регулювання повоєнного відновлення економіки. *Публічне адміністрування та національна безпека.* 2023. № 10. DOI https://doi.org/10.25313/2617-572X-2023-10-9397.

60. Магомедов А.О. Зарубіжний досвід економічного відновлення після війни. *Наукові перспективи.* 2023. № 11 (41). URL: http://perspectives.pp.ua/index.php/np/article/view/7658.

61. Магомедов А.О. Інновації в публічному управлінні сферою критичної інфраструктури. *Публічне адміністрування та національна безпека.* 2024. № 7. DOI https://doi.org/10.25313/2617-572X-2024-7-10106.

62. Магомедов А.О. Корпоратизація державних підприємств критичної інфраструктури України: інституційні проблеми та міжнародні уроки. *Публічне управління і політика.* 2026. № 4 (20). DOI https://doi.org/10.70651/3041-2498/2026.4.20.

63. Магомедов А.О. Механізм публічного управління розвитком об'єктів критичної інфраструктури: законодавчі, організаційні та управлінські виміри. *Державне управління: удосконалення та розвиток.* 2024. № 5. DOI https://doi.org/10.32702/2307-2156.2024.5.12.

64. Магомедов А.О. Особливості публічного управління об'єктами критичної інфраструктури. *Наукові перспективи.* 2024. № 7 (49). С. 412-427. DOI https://doi.org/10.52058/2708-7530-2024-7(49)-412-427.

65. Магомедов А.О. Оцінка економічних наслідків війни та втрат економіки України. *Актуальні питання у сучасній науці.* 2024. № 1 (19). С. 191-206. DOI https://doi.org/10.52058/2786-6300-2024-1(19)-191-206.

66. Магомедов А.О. Публічне управління процесами трансформації критичної інфраструктури в країнах Європи. *Успіхи і досягнення у науці.* 2024. № 6 (6). С. 520-537. DOI https://doi.org/10.52058/3041-1254-2024-6(6)-520-537.

67. Магомедов А.О. Ризики та загрози для об'єктів критичної інфраструктури та шляхи їх подолання. *Інвестиції: практика та досвід.* 2024. № 15. С. 216-221. DOI https://doi.org/10.32702/2306-6814.2024.15.216.

68. Магомедов А.О. Стан, проблеми публічного управління та стратегічні пріоритети відновлення критичної інфраструктури України (2022–2025). *Філософія та управління.* 2026. № 4 (20). DOI https://doi.org/10.70651/3041-248X/2026.4.07.

69. Магомедов А.О. Стійкість об'єктів критичної інфраструктури в контексті публічного управління. *Modern Economics.* 2024. № 46. С. 69-76. DOI https://doi.org/10.31521/modecon.V46(2024)-10.

70. Магомедов А.О. Стратегічне планування повоєнної відбудови критичної інфраструктури України: еволюція підходів, фінансові розриви та цифрові інструменти. *Філософія та управління.* 2026. № 3 (19). DOI https://doi.org/10.70651/3041-248X/2026.3.21.

71. Магомедов А.О. Стратегічне управління трансформацією об'єктів критичної інфраструктури: організаційні та управлінські виклики та можливості. *Публічне управління і адміністрування в Україні.* 2024. Вип. 41. С. 84-89. DOI https://doi.org/10.32782/pma2663-5240-2024.41.13.

72. Магомедов А.О. Стратегічні документи і заходи повоєнної відбудови України. *Публічне управління: концепції, парадигма, розвиток, удосконалення.* 2023. № 4. С. 61-75. DOI https://doi.org/10.31470/2786-6246-2023-4-61-75.

73. Магомедов А.О. Фінансове забезпечення повоєнної відбудови та відновлення економіки: теоретичні засади. *Публічне управління: концепції, парадигма, розвиток, удосконалення.* 2023. № 5. С. 60-77. DOI https://doi.org/10.31470/2786-6246-2023-5-60-76.

74. Мальчикова Д. С., Пилипенко І. О., Остапенко П. О. Просторові та суспільні виклики відновлення деокупованих територій Херсонщини /

Д. С. Мальчикова // Український географічний журнал [Текст]. — 2025. — № 2. — С. 67—77.

75. Мельник Д. С. Створення моделі загроз національній критичній інфраструктурі України як основи забезпечення її безпеки та стійкості / Д. С. Мельник // Вісник Харківського національного університету внутрішніх справ [Текст]. — 2024. — № 104 (1(1)). — С. 237—250.

76. Мельниченко Б. Б. Функції публічного управління: поняття та види / Б. Б. Мельниченко // Адміністративне право і адміністративний процес, інформаційне право [Текст]. — 2019. — № 5(2). — С. 55—61.

77. Мельничук О. Управління критичною інфраструктурою: модель та її впровадження. / О. Мельничук // Актуальні проблеми державного управління [Текст]. — 2020. — № 1(81). — С. 64—74.

78. Мельничук О. Правові механізми управління критичною інформаційною інфраструктурою України // *Збірник наукових праць НАДУ.* 2018. № 1. С. 42–60.

79. Микитенко В. В. Повоєнне відновлення та розвиток критичної інфраструктури України / В. В. Микитенко // Вісник економічної науки України [Текст]. — 2023. — № 1 (44). — С. 124—138.

80. Миколайчук М. М., Лесик О. В. Інструменти розвитку та повоєнного відновлення територій України: аналітичний огляд / М. М. Миколайчук, О. В. Лесик // Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування [Текст]. — 2023. — № 7.

81. Мороз Н., Косик В. Відновлення інфраструктури України: проблеми і напрямки / Н. Мороз, В. Косик // Галицький економічний вісник [Текст]. — 2025. — Т. 92. — № 1. — С. 77—85.

82. Мохор В. В., Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури / В. В. Мохор, С. Ф. Гончар // Електронне моделювання [Текст]. — 2019. — № 41(6). — С. 65—76.

83. Національна економіка [Текст]: навч. посіб. / авт. : В. Мельникова, О. Мельникова, Т Сідлярук [та ін.]. — ХАІ. : [б. в.], 2009. — С. 197.

84. Нєма О. С. Системний підхід до організації процесу управління об’єктами нерухомості державної власності / О. С. Нєма // Теорія та практика державного управління [Текст]. — 2009. — № 4. — С. 238—247.

85. НІСД (2024). Оцінка потреб України на відновлення та відбудову [Електронний ресурс]. — Режим доступу :https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/otsinka-potreb-ukrayiny-na-vidnovlennya-ta-vidbudovu.

86. Оновлена оцінка потреб України на відновлення та відбудову // World Bank Group. [Електронний ресурс]. — Режим доступу https://www.worldbank.org/uk/news/press-release/2025/02/25/updated-ukraine-recovery-and-reconstruction-needs-assessment-released.

87. Осипчук І. І. Адміністративна діяльність Служби безпеки України як основа забезпечення критичної інфраструктури / І. І. Осипчук // Law and Safety [Текст]. — 2020. — № 78(3). — С. 32—37.

88. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України [Текст] : монографія / авт. О. П. Єрменчук. — Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. — С. 180.

89. Оцінка швидких збитків і потреб в Україні (RDNA4) // Світовий банк [Електронний ресурс]. — Режим доступу : https://www.worldbank.org/uk/news/press-release/2025/02/25/updated-ukraine-recovery-and-reconstruction-needs-assessment-released.

90. План відновлення України [Електронний ресурс]. — Режим доступу: https://recovery.gov.ua/.

91. Помаза-Пономаренко А. Л. Розвиток публічного управління у сфері правозахисних інститутів (громадянського суспільства й омбудсмана). *Вісник НУЦЗУ. Серія «Державне управління»*. 2025. DOI: 10.52363/2414-5866-2025-2-3.

92. Портна О. В., Магдисюк С. В. Удосконалення управління розвитком критичної інфраструктури України на регіональному рівні / О. В. Портна, С. В. Магдисюк // Проблеми економіки [Текст]. — 2025. — № 1. — С. 151—157.

93. Потій О., Семенченко А., Бакалинський О., Мялковський Д. Публічне управління інституціональним розвитком у сфері кіберзахисту / О. Потій //

Науковий вісник: Державне управління [Текст]. — 2021. — № 3(9). — С. 136—162.

94. Про боротьбу з тероризмом [Електронний ресурс] : Закон України № 638-IV від 28.04.2023 р. — Режим доступу: https://zakon.rada.gov.ua/laws/show/638-15#Text.

95. Про державну таємницю [Електронний ресурс] : Закон України № 3855-XII від 01.01.2024 р. — Режим доступу: https://zakon.rada.gov.ua/laws/main/3855-12#Text.

96. Про затвердження Методичних рекомендацій щодо категоризації об’єктів критичної інфраструктури [Електронний ресурс] : Наказ Державної служби спеціального зв'язку та захисту інформації України № v0023519-21 від 26.09.2023. — Режим доступу : https://zakon.rada.gov.ua/rada/show/v0023519-21#Text.

97. Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури [Електронний ресурс] : Розпорядження Кабінету Міністрів України № 825-р від 19.09.2023 р. — Режим доступу : https://zakon.rada.gov.ua/laws/show/825-2023+-p#Text.

98. Про затвердження Порядку ведення Реєстру об’єктів критичної інфраструктури, включення таких об’єктів до Реєстру, доступу та надання інформації з нього [Електронний ресурс] : Постанова Кабінету Міністрів України № 415-2023-п від 28.04.2023 р. — Режим доступу : https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text.

99. Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури [Електронний ресурс] : Постанова Кабінету Міністрів України № 821-2022-п від 22.07.2022 р. — Режим доступу : https://zakon.rada.gov.ua/laws/show/821-2022-п#Text.

100. Про затвердження Регламенту обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури [Електронний ресурс] : Постанова Кабінету Міністрів України № 1174 від 14.10.2022 р. — Режим доступу : https://zakon.rada.gov.ua/laws/show/1174-2022-п#Text.

101. Про інформацію [Електронний ресурс] : Закон України № 2657-XII від 27.07.2023 р. — Режим доступу : https://zakon.rada.gov.ua/laws/show/2657-12#Text.

102. Про критичну інфраструктуру [Електронний ресурс] : Закон України № 1882-IX від 21.09.2024 р. — Режим доступу : https://zakon.rada.gov.ua/laws/show/1882-20#Text.

103. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Закон України № 2163-VIII від 28.06.2024 р. — Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

104. Про Положення про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України [Електронний ресурс] : Указ Президента України № 379/99 від 11.06.2022 р. — Режим доступу : https://zakon.rada.gov.ua/laws/show/638-15#Text.

105. Про Положення про робочу групу з проведення реформи місцевих органів виконавчої влади, органів місцевого самоврядування та державної служби [Електронний ресурс] : Указ Президента України № 1001/98 від 21.07.2001 р. — Режим доступу : https://zakon.rada.gov.ua/laws/show/1001/98#Text.

106. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» [Електронний ресурс] : Указ Президента України № 447/2021 від 21.08.2021 р. — Режим доступу : https://zakon.rada.gov.ua/laws/show/447/2021#Text.

107. Про схвалення Концепції створення державної системи захисту критичної інфраструктури [Електронний ресурс] : Розпорядження Кабінету Міністрів України № 1009-р. від 06.12.2017 р.— Режим доступу : https://zakon.rada.gov.ua/laws/show/1009- 2017-%D1%80#n8.

108. Пушак Я. Я., Хаустова В. Є., Трушкіна Н. В. Безпекова стратегія розвитку критичної інфраструктури в умовах повоєнної відбудови економіки України / Я. Я. Пушак // Науковий вісник Львівського державного університету внутрішніх справ (серія економічна) [Текст]. — 2023. — № 1. — С. 68—78.

109. Регіональна презентація екосистеми DREAM відбулась в Чернігові [Електронний ресурс]. — Режим доступу : https://dream.gov.ua/ua/news/123.

110. Рудюк Я., Русин-Гриник Р., Федорчак О. Види розвитку інноваційної діяльності підприємств в умовах екстремальних ситуацій / Я. Рудюк // Наукові інновації та передові технології [Текст]. — 2024. — № 6(34). — С. 253—269.

111. Саврацький О.О. Адаптація системи управління об'єктами критичної інфраструктури до сучасних безпекових викликів / О. О. Саврацький // Трансформаційна економіка [Текст]. — 2024. — №1(6). — С. 53—57.

112. Семенко О., Гаврилюк І., Соломіцький О., Кліат Ю., Добровольський Ю., Гетьман А. Стратегія повоєнного відновлення України: системна модель інтеграції економіки та управління / О. Семенко // Social Development and Security [Текст]. — 2025. — Т. 15. — № 2. — С. 12—19.

113. Суходоля О. М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України / О. М. Суходоля // Стратегічні пріоритети. Серія: Політика [Текст]. 2016. — № 3(40). — С. 65—67.

114. Трушкіна Н. Розвиток критичної інфраструктури в умовах війни: проблеми та шляхи їх вирішення / ра заг. ред. Н. В. Павліхи // REBUILD UKRAINE: справа всього цивілізованого світу : збірник тез доповідей II Міжнар. наук-практ. конф. (Луцьк, 15 березня 2023 р.) [Текст]. — Луцьк, 2023. — С. 30–36.

115. Трушкіна Н. Цифрова стратегія розвитку критичної інфраструктури: бібліометричний та трендовий аналіз / Н. Трушкіна // International Science Journal of Management, Economics & Finance [Текст]. — 2024. — Vol. 3. — № 4. — P. 79—100.

116. Уряд затвердив Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури [Електронний ресурс]. — Режим доступу : https://cip.gov.ua/ua/news/uryad-zatverdiv-nacionalnii-plan-zakhistu-ta-zabezpechennya-bezpeki-ta-stiikosti-kritichnoyi-infrastrukturi.

117. Уряднікова І. В., Заплатинський В. М. Наукові підходи до визначення терміну «критична інфраструктура» / І. В. Уряднікова, В. М. Заплатинський // Вісті Донецького гірничого інституту [Текст]. — 2020. — № 2(47).

118. Федик В., Денисенко Г. Теоретико-методологічні підходи до управління ризиками кібербезпеки на об’єктах критичної інфраструктури: реагування на кіберінциденти та менеджмент кризових ситуацій / В. Федик, Г. Денисенко // Інформація і право [Текст]. — 2024. — № 1(48). — С. 195—202.

119. Фонд відновлення регіонів: результати 2025 року // Міністерство розвитку громад, територій та інфраструктури України [Електронний ресурс]. — Режим доступу : https://minregion.gov.ua/news/fond-vidnovlennya-regioniv-rezultaty-2025/.

120. Франчук В. І., Пригунов П. Я., Мельник С. І. Безпека об’єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи / В. І. Франчук // Соціально-правові студії [Текст]. — 2021. — №3 (13). — С. 142—148.

121. Шиповський В. Система показників оцінювання кіберстійкості інформаційних систем об’єктів критичної інфраструктури / В. Шиповський // Ukrainian Information Security Research Journal [Текст]. — 2023. — № 25(1). — С. 37—45.

122. Шпатакова О., Іваненко Р., Погребицький Р. Перспективи відновлення критичної інфраструктури на деокупованих територіях України / О. Шпатакова // Економіка та суспільство [Текст]. — 2022. — № 40.

123. Шульга В. П., Іванченко Є. В., Вишневська Н. С., Бербер А. С. Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави / В. П. Шульга // Сучасний захист інформації [Текст]. — 2024. — № 3. — С. 6—19.

124. Яременко О. І., Страхніцький Я. О. Теоретико-методичні основи забезпечення системи захисту критичної інфраструктури держави / О. І. Яременко, Я. О. Страхніцький // Державне управління: удосконалення та розвиток [Текст]. — 2022. — № 1. — С. 177—189.

125. Ящук В. І. Принципи проектування автоматизованих інформаційних систем управління об’єктами критичної інфраструктур [Електронний ресурс]. — Режим доступу : https://sci.ldubgd.edu.ua/bitstream/123456789/9829/1/1.%20%D0%9B%D0%A2%D0%95%D0%A3%20%D0%9F%D0%A0%D0%98%D0%9D%D0%A6%D0%98%D0

%9F%D0%98%20%D0%9F%D0%A0%D0%9E%D0%95%D0%9A%D0%A2%D0%A3%D0%92%D0%90%D0%9D%D0%9D%D0%AF%20%D0%90%D0%92%D0%A2%D0%9E%D0%9C%D0%90%D0%A2%.

126. A guidebook on public-private partnership in infrastructure // ESACP [Electronic resource]. — Access mode : https://www.unescap.org/sites/default/files/ppp_guidebook.pdf.

127. A pre-winter assessment — Ukraine's Energy Security // International Energy Agency [Electronic resource]. — Access mode : https://www.iea.org/reports/ukraines-energy-security/a-pre-winter-assessment.

128. About the Norwegian National Security Authority // The Norwegian National Security Authority (NSM) [Electronic resource]. — Access mode : https://nsm.no/about-nsm/about-the-norwegian-national-security-authority/.

129. Agius J., Karagiannis G. M., Pescaroli G., Galbusera L., Theocharidou M., Krausmann E., Chaudhari K. 'Critical Infrastructures', in: Casajus Valles, A., Marin Ferrer, M., Poljanšek, K., Clark, I. (eds.) // Science for Disaster Risk Management 2020: acting today, protecting tomorrow, Publications Office of the European Union, Luxembourg, 2020. [Electronic resource]. — Access mode : https://doi.org/10.2760/571085.

130. Ahmed M. E., Massoudi A. H. Reconstructing Syrian Economy through Public and Private Sectors Partnership / M. E. Ahmed, A. H. Massoudi // Cihan University-Erbil Scientific Journal [Text]. — 2018. — №2(Special 2-B). — P. 38—62.

131. Aivazian V., Ge Y., Qiu J. Can corporatization improve the performance of state-owned enterprises even without privatization? / V. Aivazian // Journal of Corporate Finance [Text]. — 2025. — № 11(5). — P. 791—808.

132. Alcaraz C., Zeadally S. Critical infrastructure protection: Requirements and challenges for the 21st century / C. Alcaraz, S. Zeadally // International journal of critical infrastructure protection [Text]. — 2015. — № 8. — P. 53—66.

133. Al-Saidi, M., Roach, E. L., & Al-Saeedi, B. A. H. (2020). Conflict resilience of water and energy supply infrastructure: Insights from Yemen / M. Al-Saidi // Water [Text]. — 2020. — № 12(11).

134. Andres A., Biller D., Blades C., Bloomgarden D.R., Bright D., Escalante M.C., Calvo J., Carboni G., Casabianca B.A., Chaudry O., Donchev D. The Economic

Impact of Public-Private Partnerships in the Infrastructure Sector: Literature Review // WBG [Electronic resource]. — Access mode : https://ppp.worldbank.org/sites/default/files/2022-02/LiteratureReviewInfrastructurePPPs_Mar2016.pdf.

135. Andrieiev D., Lyhun O., Drozd A., Ponochnovna O. Monitoring System for Critical Infrastructure Objects Based on Digital Twins / D. Andrieiev // Computer Systems and Information Technologies [Text]. — 2025. — № 2. — P. 27–35.

136. Anglmayer I. European critical infrastructure Revision of Directive 2008/114/EC: Implementation Appraisal // European Parliament [Electronic resource]. — Access mode : https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf.

137. Argyroudis S. A. Resilience metrics for transport networks: a review and practical examples for bridges / S. A. Argyroudis // Proceedings of the Institution of Civil Engineers-Bridge Engineering [Text]. — 2022. — №175(3). — P. 179—192.

138. Argyroudis S. A., Mitoulis S. A. Vulnerability of bridges to individual and multiple hazards-floods and earthquakes / S. A. Argyroudis, S. A. Mitoulis // Reliability Engineering & System Safety [Text]. — 2021. — № 210.

139. Assessment of EIP as part of Green Recovery of Ukraine // GEIPP Ukraine [Electronic resource]. — Access mode : https://geipp-ukraine.org/wp-content/uploads/2024/06/Assessment-of-EIP-as-part-of-Green-Recovery-of-Ukraine.pdf.

140. Attacks on Ukraine’s electricity infrastructure threaten key aspects of life – winter approaches // United Nations in Ukraine [Electronic resource]. — Access mode : https://ukraine.un.org/en/278995-attacks-ukraines-electricity-infrastructure-threaten-key-aspects-life-winter-approaches-%E2%80%93.

141. Axelsdóttir E., Jonason Bjärenstam R. Critical Infrastructure Resilience–Comparing Swedish critical infrastructures based on interruption data // Division of Risk Management and Societal Safety, Faculty of Engineering Lund University [Electronic resource]. — Access mode :

https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8954871&fileOId=8954872.

142. Back to school — 4.6 млн дітей в Україні стикаються з освітніми викликами // UNICEF [Electronic resource]. — Access mode : https://www.unicef.org/ukraine/en/press-releases/back-to-school.

143. Barbero Vignola G., Acs S., Borchardt S., Sala S., Giuntoli J., Smits P., Marelli L. Modelling for sustainable development goals (SDGs): overview of JRC models [Text] / G. Barbero Vignola. — Publication Office of the European Union EU Science Hub-European Commission: Luxembourg, 2020. — 90 p.

144. Barquet K., Englund M., Inga K., André K., Segnestam L. Conceptualising multiple hazards and cascading effects on critical infrastructures / K. Barquet // Disasters [Text]. — 2024. — № 48(1).

145. Benítez-Ávila C., Hartmann A., Dewulf G. Contractual and relational governance as positioned practices in ongoing public-private partnership projects / C. Benítez-Ávila // Project Management Journal [Text]. — 2019. —№ 50(8). — P. 716—733. http://dx.doi.org/10.1177/8756972819848224.

146. Bennett B. T. Understanding, assessing, and responding to terrorism: Protecting critical infrastructure and personnel [Text] / B. T. Bennett. — John Wiley & Sons, 2018. — 512 p.

147. Berezovska N., Zahorskyi V., Kalashnyk N., Novak-Kalyayeva L., Lipentsev A., Olefirenko O., Sushynskyi O. Implementing an ecosystem approach in public administration: achieving sustainable development goals in crisis and recovery / N. Berezovska // Cadernos de Educação Tecnologia e Sociedade [Text]. — 2024. — Vol. 17. — № se4. — P. 334—347.

148. Berkeley A. R., Wallace M., Coo C. A framework for establishing critical infrastructure resilience goals. Final report and recommendations by the council, national infrastructure advisory council // A Framework for Establishing Critical Infrastructure Resilience Goals [Electronic resource]. — Access mode : https://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf.

149. Bıçakçı A. S. Digital Europe Program: Nurturing Technological Sovereignty for a Resilient European Digital Ecosphere / A. S. Bıçakçı // Ankara Avrupa Çalışmaları Dergisi [Text]. — 2024. — № 23. — P. 135—174.

150. Bilodeau N., Laurin C., Vining A. Choice of Organizational Form Makes a Real Difference: The Impact of Corporatization on Government Agencies in Canada / N. Bilodeau // Journal of Public Administration Research and Theory [Text]. —2007. — № 17(1). — P. 119—147.

151. Bjarte R., Lange D., Marianthi T., Pursiainen C. From risk management to resilience management in critical infrastructure / R. Bjarte // Journal of Management in Engineering [Text]. — 2020. — Vol. 36. — № 4.

152. Boelens R., Vos J. The danger of naturalizing water policy concepts: Water productivity and efficiency discourses from field irrigation to virtual water trade / R. Boelens, J. Vos // Agricultural Water Management [Text]. — 2012. — № 108. — P. 16—26.

153. Bohdan B., Kuzmenko O., Chorna V. Economic measures for managing critical infrastructure facilities in Ukraine / B. Bohdan // Baltic Journal of Economic Studies [Text]. —2023. — Vol. 9. — № 3. — P. 22—32.

154. Bohun V., Magomedov A., Hromyka O., Kovshun N., Fedorchuk Y. Assessing the Impact of Infrastructure Damage on National Investment Attractiveness During Martial Law. *Pakistan Journal of Life and Social Sciences,* 2024, 22(2), p.100379-100385. DOI: 10.57239/PJLSS-2024-22.2.00784.

155. Boloorani A. D., Darvishi M., Weng Q., Liu X. Post-war urban damage mapping using InSAR: the case of Mosul City in Iraq / A. D. Boloorani // ISPRS International Journal of Geo-Information [Text]. — 2021. — № 10(3). — P. 140.

156. Bowerman M., Francis G. Benchmarking as a Tool for the Modernisation of Local Government / M. Bowerman, G. Francis // Financial Accountability & Management [Text]. —2001. —№17(4). — P. 321—329.

157. Brodecki Z., Jaskiewicz-Kaminska S. "Ukraine on Fire": Remarks on Causes and Effects of the Russian Aggression against Ukraine and Its Impact on the Right to Safe Critical Infrastructure / Z. Brodecki, S. Jaskiewicz-Kaminska // Krytyka Prawa [Text]. — 2023. — № 3. — P. 59—109.

158. Bruneau M., Chang S. E., Eguchi R. T., Lee G. C., O'Rourke T. D., Reinhorn A. M., Von Winterfeldt D. A framework to quantitatively assess and enhance the seismic resilience of communities / M. Bruneau // Earthquake Spectra [Text]. — 2003. —№ 19(4). — P. 733—752.

159. Building Blocks for Ukraine's Recovery and Long-Term Development (includes RDNA4) // World Bank [Electronic resource]. — Access mode : https://documents1.worldbank.org/curated/en/099430504172540289/pdf/IDU-27384831-502e-466d-907e-d497bdd5132d.pdf.

160. Bujones A. K., Jaskiewicz K., Linakis L., McGirr M. A framework for analyzing resilience in fragile and conflict-affected situations // Columbia/SIPA. Economic and political development [Electronic resource]. — Access mode : https://www.sipa.columbia.edu/sites/default/files/migrated/migrated/documents/USAID%2520Final%2520Report.pdf.

161. Canada's Cyber Security Strategy: For a stronger and more prosperous Canada [Electronic resource]. — Access mode : https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-cbr-scrt-strtgy/archive-cbr-scrt-strtgy-eng.pdf.

162. Canada's Digital Ambition 2022 [Electronic resource]. — Access mode : https://www.canada.ca/en/government/system/digital-government/government-canada-digital-operations-strategic-plans/canada-digital-ambition.html.

163. Canadian Centre for Cyber Security [Electronic resource]. — Access mode : https://www.cyber.gc.ca/en.

164. Cantelmi R., Di Gravio G., Patriarca R. Reviewing qualitative research approaches in the context of critical infrastructure resilience / R. Cantelmi // Environmental Systems and Decisions [Text]. — 2021. — Vol. 41. — № 3. — P. 341—376.

165. Carballo J. A., Bonilla J., Fernández-Reche J., Avila-Marin A. L., Díaz B. Modern SCADA for CSP Systems Based on OPC UA, Wi-Fi Mesh Networks, and Open-Source Software / J. A. Carballo // Energies [Text]. — 2024. — Vol. 17. — № 24.

166. Cariolet J. M., Vuillet M., Diab Y. Mapping urban resilience to disasters A review / J. M. Cariolet // Sustainable Cities and Society [Text]. — 2019. — № 51.

167. Casciati F., Casciati S., Fuggini C., Faravelli L., Tesfai I., Vece M. Framing a satellite based asset tracking (SPARTACUS) within smart city technology / F. Casciati // Journal of Smart Cities [Text]. — 2019. — № 2(2). — P. 40—48.

168. Cedergren A., Johansson J., Hassel H. Challenges to critical infrastructure resilience in an institutionally fragmented setting / A. Cedergren // Safety science [Text]. — 2018. —№ 110. — p. 51—58.

169. Centre for Environmental and Energy Research: Mapping Ukraine's ecologically important areas // CEOBS [Electronic resource]. — Access mode : https://ceobs.org/mapping-ukraines-ecologically-important-areas/.

170. CERT-UA зафіксувала 4315 кібератак у 2024 році // Державна служба спеціального зв'язку та захисту інформації України [Electronic resource]. — Access mode : https://cip.gov.ua/en/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv.

171. Chavez D. (2014). An exeptional electicity company in an atypical social democracy: Costa Rica's ICE, in: D. McDonald (ed.) // Rethinking corporatization: Public utilities in the Global South, Zed Books, 2014. — P. 31—61.

172. Chavez D., Torres S. Reorienting development: State-owned enterprises in Latin America and the world [Text] / D. Chavez, S. Torres — Transnational Institute (TNI), 2014. — 218 p.

173. Chen C. R., Chang C. J., Lee C. H. A time-driven and event-driven approach for substation feeder incident analysis / C. R. Chen // International Journal of Electrical Power & Energy Systems [Text]. — 2016. — № 74.— P. 9—15.

174. Chen Y., Ji W. Enhancing situational assessment of critical infrastructure following disasters using social media /Y. Chen, W. Ji // Journal of Management in Engineering [Text]. — 2021. — № 37(6).

175. Chen Z., Hutchinson T. C. Urban damage estimation using statistical processing of satellite images / Z. Chen, T. C. Hutchinson // Journal of Computing in Civil Engineering [Text]. — 2007. — № 21(3). — P. 187—199.

176. Cherdantseva Y., Burnap P., Blyth A., Eden P., Jones K., Soulsby H., Stoddart K. A review of cyber security risk assessment methods for SCADA systems / Y. Cherdantseva // Computers & security [Text]. — 2016. — № 56. — P. 1—27.

177. Clarvis M. H., Bohensky E., Yarime M. Can resilience thinking inform resilience investments? / M. H. Clarvis // Learning from resilience principles for disaster risk reduction. Sustainability (Switzerland) [Text]. — 2015. — № 7(7). P. 9048—9066.

178. Commission welcomes increased electricity export capacity to Ukraine and Moldova for this winter // European Commission (DG NEAR) [Electronic resource]. — Access mode : https://enlargement.ec.europa.eu/news/commission-welcomes-increased-electricity-export-capacity-ukraine-and-moldova-2024-10-29_en.

179. Commonwealth Procurement Rules // Australian Government Department of Finance [Electronic resource]. — Access mode : https://www.finance.gov.au/government/procurement/commonwealth-procurement-rules.

180. Commonwealth Risk Management Policy // Australian Government Department of Finance [Electronic resource]. — Access mode : https://www.finance.gov.au/government/comcover/risk-services/management/commonwealth-risk-management-policy.

181. Coordination of Reconstruction and Recovery with the National Recovery Plan // U-LEAD with Europe [Electronic resource]. — Access mode : https://u-lead.org.ua/storage/admin/files/3d2f6c654ea3384ca017ca6848ea59ef.pdf.

182. Copernicus Emergency Management Service monitors wildfires in Ukraine. European Space Agency // UN-SPIDER [Electronic resource]. — Access mode : https://www.un-spider.org/news-and-events/news/copernicus-emergency-management-service-monitors-wildfires-ukraine.

183. Cordesman A. H. The New U.S. National Defense Strategy for 2022 // Center for Strategic and International Studies (CSIS) [Electronic resource]. — Access mode : https://www.csis.org/analysis/new-us-national-defense-strategy-2022.

184. Corporate plan for grid development and ENTSO-E integration (extract) // NPC «Укренерго» [Electronic resource]. — Access mode : https://ua.energy/wp-content/uploads/2025/04/Korporatyvnyj_plan_zi_zberezhennya_eng-1.docx.

185. Corruption Perceptions Index 2025 // Transparency International Україна [Electronic resource]. — Access mode : https://ti-ukraine.org/news/cpi-2025-results/.

186. Council Directive (EU) 2022/542 of 5 April 2022 amending Directives 2006/112/EC and (EU) 2020/285 as regards rates of value added tax // European Union [Electronic resource]. — Access mode : https://eur-lex.europa.eu/eli/dir/2022/542.

187. Critical Infrastructure and Key Resources Support Annex // Department of Homeland Security [Electronic resource]. — Access mode : https://www.fema.gov/pdf/emergency/nrf/nrf-support-cikr.pdf.

188. Critical Infrastructure Information Act of 2002 as Amended [Electronic resource]. — Access mode : https://www.cisa.gov/sites/default/files/2023-03/critical-infrastructure-information-act-of-2002-012014.pdf.

189. Critical Infrastructure Risk Management Program (CIRMP) // Department of the Prime Minister and Cabinet [Electronic resource]. — Access mode : https://oia.pmc.gov.au/published-impact-analyses-and-reports/critical-infrastructure-risk-management-program.

190. Critical Infrastructure Sectors // U.S. Department of Homeland Security [Electronic resource]. — Access mode : https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

191. Del Castillo G. Rebuilding war-torn states: The challenge of post-conflict economic reconstruction [Text] / G. Del Castillo. — OUP Oxford, 2008. — 460 p.

192. Di Pietro R., Raponi S., Caprolu M., Cresci S. Critical Infrastructure. In: New Dimensions of Information Warfare / R. Di Pietro // Advances in Information Security [Text]. — 2021. — Vol. 84.

193. Diagnostics and development of a digital platform for the reconstruction of Chernihiv // Egis Group [Electronic resource]. — Access mode : https://www.egis-group.com/projects/diagnostics-and-development-of-a-digital-platform-for-the-reconstruction-of-chernihiv.

194. Digital State UA — Ukraine's International Platform for GovTech Innovation // IT Ukraine Association [Electronic resource]. — Access mode : https://itukraine.org.ua/en/digital-state-ua-a-global-platform-for-digital-solutions-and-govtech-innovation-launched/.

195. Digital Transformation of Ukraine's Economy // NISS Expert Comments [Electronic resource]. — Access mode : https://niss.gov.ua/en/news/komentari-ekspertiv/digital-transformation-ukraines-economy-september-2025.

196. Direct damage to Ukraine's infrastructure from the war reached $170 billion Прямі збитки інфраструктури України від війни сягнули $170 млрд – KSE // GMK Center [Electronic resource]. — Access mode : https://gmk.center/ua/news/pryami-zbitki-infrastrukturi-ukraini-vid-vijni-syagnuli-170-mlrd-kse/.

197. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC [Electronic resource]. — Access mode : http://data.europa.eu/eli/dir/2022/2557/oj.

198. DREAM покаже все: як іде відбудова України, скільки це коштує і хто платить // Вокс Україна [Electronic resource]. — Access mode : https://voxukraine.org/dream-pokazhe-vse-yak-ide-vidbudova-ukrayiny-skilky-tse-koshtuye-i-hto-platyt.

199. DREAM: While fighting for its future, Ukraine invented a better way to make investments that benefit people and the planet // Open Contracting Partnership: вебсайт [Electronic resource]. — Access mode : https://www.open-contracting.org/2025/07/10/dream-while-fighting-for-its-future-ukraine-invented-a-better-way-to-make-investments-that-benefit-people-and-the-planet/.

200. Earnest J. Post-conflict reconstruction – a case study in Kosovo / J. Earnest // International Journal of Emergency Services [Text]. — 2015. — № 4(1). — P. 103—128.

201. EIB delivers almost €100 million to Ukraine for recovery projects // European Investment Bank [Electronic resource]. — Access mode : https://www.eib.org/en/press/all/2023-533-eib-delivers-almost-eur100-million-to-ukraine-for-recovery-projects.

202. El Rayess M., Moretti D., Tanberg E., Kurniawan R. Managing the Fiscal Risks of Infrastructure Investment by Public Corporations // IMF PFM [Electronic

resource]. — Access mode : https://blog-pfm.imf.org/en/pfmblog/2023/04/managing-the-fiscal-risks-of-infrastructure-investment-by-public-corporations.

203. Electronic government helps communities solve problems, access resources in wartime Ukraine // Mott Foundation [Electronic resource]. — Access mode : https://www.mott.org/news/articles/electronic-government-helps-communities-solve-problems-access-resources-in-wartime-ukraine/.

204. El-Maissi A. M., Kassem M. M., Nazri F. M. Resilient critical infrastructures: An innovative methodological perspective for critical infrastructure (CI) integrated assessment models by inducing digital technologies during multi-hazard incidents / A. M. El-Maissi // MethodsX [Text]. — 2024. — Vol. 12.

205. ENISA Threat Landscape 2025 // European Union Agency for Cybersecurity (ENISA) [Electronic resource]. — Access mode : https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

206. EU and Ukraine deepen cooperation on cyber security at the 4th Cyber Dialogue // European Commission — DG NEAR [Electronic resource]. — Access mode : https://enlargement.ec.europa.eu/news/eu-and-ukraine-deepen-cooperation-cyber-security-4th-cyber-dialogue-2025-10-20_en.

207. EU and UNDP secure access to safe drinking water for over 95,000 residents in southern Ukraine // UNDP [Electronic resource]. — Access mode : https://www.undp.org/european-union/press-releases/eu-and-undp-secure-access-safe-drinking-water-over-95000-residents-southern-ukraine.

208. EU Cybersecurity NIS2 Directive to be transposed National Law by October 2024 // International Trade Administration [Electronic resource]. — Access mode : https://www.trade.gov/market-intelligence/eu-cybersecurity-nis2-directive-be-transposed-national-law-october-2024.

209. Evolving anti-corruption practice in rebuilding Ukraine: The Agency for Restoration and Infrastructure Development // U4 Anti-Corruption Resource Centre [Electronic resource]. — Access mode : https://www.u4.no/publications/evolving-anti-corruption-practice-in-rebuilding-ukraine-the-agency-for-restoration-and-infrastructure-development.pdf.

210. Fabre A., Straub S. The economic impact of public private partnerships (PPPs) in infrastructure, health and education: a review // Toulouse School of Economics [Electronic resource]. — Access mode : https://core.ac.uk/download/pdf/300465882.pdf.

211. Fantini C. Infrastructure for Peacebuilding: The Role of Infrastructure in Tackling the Underlying Drivers of Fragility // UNOPS [Electronic resource]. — Access mode : https://content.unops.org/publications/Infrastructure_Peacebuilding_EN_Web.pdf.

212. Fedderke J., Garlick R. Infrastructure development and economic growth in South Africa: A review of the accumulated evidence / J. Fedderke, R. Garlick // Working Paper [Text]. — 2008. — № 8967. — P. 1—47.

213. Fekete A., Lauwe P., Geier W. Risk management goals and identification of critical infrastructures / A. Fekete // International journal of critical infrastructures [Text]. — 2012. — № 8(4). — P. 336—353.

214. Ferreira L. S., Nobre F. S. Agile project management under the perspective of dynamic capabilities / L. S. Ferreira, F. S. Nobre // Gestão & Produção [Text]. — 2022. — № 29.

215. Ficoń K. Inżynieria zarządzania kryzysowego: podejście systemowe [Text] / K. Ficoń. — BEL Studio Sp. z o. o., 2007. — 501 p.

216. Førde J. S., Lægreid P., Rubecksen K., Rykkja L. H. Organizing for societal security and crisis management in Germany, The Netherlands, Norway, Sweden and the UK // Societal security and crisis management: Governance Capacity and Legitimacy [Electronic resource]. — Access mode : https://doi.org/10.1007/978-3-319-92303-1_2.

217. Forum to foster an inclusive and community-driven recovery of Ukraine brings together nearly 500 people in Kyiv today // United Nations Ukraine [Electronic resource]. — Access mode : https://ukraine.un.org/en/268318-forum-foster-inclusive-and-community-driven-recovery-ukraine-brings-together-nearly-500.

218. Foster J. S., Gjelde E., Graham W. R., Hermann R. J., Kluepfel H. M., Lawson R. L., Woodard J. B. Report of the commission to assess the threat to the United States from electromagnetic pulse (EMP) attack // Critical National

Infrastructures Report [Electronic resource]. — Access mode : https://static1.squarespace.com/static/57bc8a4a414fb50147550a88/t/589e00042994ca3e9f55f8cd/1486749702165/2008+EMP+Commission+excerpts+re+E3.pdf.

219. Four ways to embed anti-corruption in Ukraine's Donor Coordination Platform // U4 Blog [Electronic resource]. — Access mode : https://www.u4.no/blog/four-ways-to-embed-anti-corruption-in-ukraines-donor-coordination-platform.

220. Garzón F. A. M., Valánszki I. Environmental armed conflict assessment using satellite imagery / F. A. M. Garzón, I. Valánszki // Journal of Environmental Geography [Text]. — 2020. — № 13(3-4). — P. 1—14.

221. George A. S., Baskar T., Srikaanth P. B. Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors / A. S. George // Partners Universal International Innovation Journal [Text]. — 2024. — № 2(1). — P. 51—75.

222. Girod D. Explaining post-conflict reconstruction [Text] / D. Girod. — Oxford University Press, 2015. — 224 p.

223. Gitelman L., Kozhevnikov M., Visotskaya Y. Diversification as a method of ensuring the sustainability of energy supply within the energy transition / L. Gitelman // Resources [Text]. — 2023. — № 12(2). — P. 19.

224. Gjesvik L. Comparing Cyber Security. Critical Infrastructure protection in Norway, the UK and Finland. NUPI Report // Norwegian Institute of International Affairs [Electronic resource]. — Access mode : http://hdl.handle.net/11250/2598280

225. Good Governance for Critical Infrastructure Resilience // OECD Reviews of Risk Management Policies [Electronic resource]. — Access mode : https://doi.org/10.1787/02f0e5a0-en.

226. Government at a Glance 2025: Performance budgeting // OECD iLibrary [Electronic resource]. — Access mode : https://www.oecd.org/en/publications/2025/06/government-at-a-glance-2025_70e14c6c/full-report/performance-budgeting_eb0a21ea.html.

227. Government of Canada's Enterprise Cyber Security Strategy [Electronic resource]. — Access mode : https://www.canada.ca/en/government/system/digital-government/online-security-privacy/enterprise-cyber-security-strategy.html.

228. Green paper on a European programme for critical infrastructure protection (COM/2005/576 final) dated 11/17/2005 [Electronic resource]. — Access mode : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576.

229. Grzywna Z. Critical infrastructure security in Poland and the surrounding area. Legislation analysis / Z. Grzywna // Security and Defence Quarterly [Text]. — 2014. — № 2(1). — P. 155—172.

230. Havrys A., Yakovchuk R., Pekarska O., Tur N. Use of the computer modelling for the analysis of dangerous areas during flooding of territories / A. Havrys // Ecological Engineering & Environmental Technology [Text]. —2024. — Vol. 25. — № 4.

231. Hay A., Karney B., Martyn N. Reconstructing infrastructure for resilient essential services during and following protracted conflict: A conceptual framework // International Review of the Red Cross [Electronic resource] / A. Hay. — Access mode : https://international-review.icrc.org/sites/default/files/pdf/1602948923/IRC101_3b/S1816383120000053a.pdf.

232. Henriques J., Caldeira F., Cruz T., Simões P. A survey on forensics and compliance auditing for critical infrastructure protection / J. Henriques // IEEE Access [Text]. —2024. — № 12. — P. 2409—2444.

233. Herrera V., Post A. Can Developing Countries Both Decentralize and Depoliticize Urban Water Services? / V. Herrera, A. Post // Evaluating the Legacy of the 1990s Reform Wave. World Development [Text]. — 2014. — № 64. — P. 621—641.

234. Hiteva R., Watson J. Governance of interactions between infrastructure sectors: The making of smart grids in the UK / R. Hiteva, J. Watson // Environmental Innovation and Societal Transitions [Text]. — 2019. — № 32. — P. 140—152.

235. Hoeffler A. Challenges of Infrastructure Rehabilitation and Reconstruction in War-affected Economies // African Development Bank [Electronic resource]. — Access mode :

https://www.afdb.org/fileadmin/uploads/afdb/Documents/Publications/00157630-EN-ERP-48.PDF.

236. How Copernicus is unveiling the impact of war on Ukrainian agriculture // ASD Europe [Electronic resource]. — Access mode : https://www.asd-europe.org/news-media/news-events/get-inspired/how-copernicus-is-unveiling-the-impact-of-war-on-ukrainian-agriculture/

237. Hynes W., Trump B. D., Kirman A., Haldane A., Linkov I. Systemic resilience in economics / W. Hynes // Nature Physics [Text]. — 2022. — № 18(4). — P. 381—384.

238. Hyun S., Park D., Tian G. Determinants of Public–Private Partnerships in Infrastructure in Asia: Implications for Capital Market Development, in A. Deep (ed.) // Asian Development Bank Economics Working Paper Series [Text], Manila: Asian Development Bank, 2019.

239. IMF strategy for fragile and conflict-affected states (FCS), imf policy paper no. 2022/004 // Washington, D.C. [Electronic resource]. — Access mode : https://www.imf.org/en/Publications/Policy-Papers/Issues/2022/03/14/The-IMF-Strategy-for-Fragile-and-Conflict-Affected-States-515129.

240. Imran M., Elbassuoni S., Castillo C., Diaz F., Meier P. Practical extraction of disaster-relevant information from social media, in D. Shwabe, V. Almeida // Proceedings of the 22nd international conference on world wide web [Text]. — Rio de Janeiro Brazil, 2013. — P. 1021—1024.

241. Investing in Ukraine’s Future — community project portfolios (Sumy, Chernihiv, Kharkiv, Chernivtsi) // UNDP [Electronic resource]. — Access mode : https://www.undp.org/sites/g/files/zskgke326/files/2025-07/english-portfolio-undp_3.pdf.

242. Jagusiak B., Kaczmarek W. Selected Issues Concerning Critical Infrastructure Security Management / B. Jagusiak, W. Kaczmarek // Polish Political Science Yearbook [Text]. — 2024. — № 2(53). — P. 221—242.

243. Ji A., He R., Chen W., Zhang L. Computational methodologies for critical infrastructure resilience modeling: A review / A. Ji // Advanced Engineering Informatics [Text]. — 2024. — № 62.

244. Jimada-Ojuolape B., Teh J. Impact of the integration of information and communication technology on power system reliability: A review / B. Jimada-Ojuolape, J. Teh // IEEE Access[Text]. —2020. — №.8. — P. 24600—24615.

245. Joint Statement – Omnibus initiative: Sustainability rules are essential for a competitive and sustainable EU economy // Eurosif / IIGCC / PRI [Electronic resource]. — Access mode : https://image.e-marketing.unpri.org/lib/fe3911707564047574 1272/m/1/51567c74-f633-43ea-b70c-fda59345cde4.pdf.

246. Kharazishvili Y., Bugayko D., Yashchyshyna I., Butorina V., Androshchuk I., Sribnyi O. Strategic scenarios of post-war recovery of sustainable development of Poltava region of Ukraine: Innovative and environmental aspects / Y. Kharazishvili // IOP Conference Series: Earth and Environmental Science [Text]. — 2023. — Vol. 1126. — № 1. — P. 012007.

247. Kjell W. Bergan. The Norwegian Certification Scheme Presentation for ENISA – Commision Workshop on security certification of Smart Grid Components: Scheme Director // Norwegian National Security Authority/SERTIT [Electronic resource]. — Access mode : https://www.enisa.europa.eu/events/smart-grid-certification-components/sertit_presentation.

248. Knapp E. D. Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems [Text] / E. D. Knapp. — Elsevier, 2024. — P. 1—483.

249. Knoth C., Slimani S., Appel M., Pebesma E. Combining automatic and manual image analysis in a web-mapping application for collaborative conflict damage assessment / C. Knott // Applied Geography [Text]. — 2018. — № 97. — P. 25—34.

250. Kottmann F., Kyriakidis M., Dang V. N., Sansavini G. Enhancing infrastructure resilience by using dynamically updated damage estimates in optimal repair planning: The power grid case / F. Kottmann // ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering [Text]. —2021. — № 7(4).

251. Kulyk V. V. Modeling the Inter-Industry Economy as a Critical Infrastructure: Generating Scenarios for the Development of the Economy of Ukraine

under the Conditions of War and the Post-War Recovery / V. V. Kulyk // Cybernetics and Systems Analysis [Text]. — 2023. — T. 59. — P. 967—985.

252. Kushnirenko O., Gakhovich N., Venger L. Strategic scenarios for sustainable industrial development of Ukraine in the post-war period / O. Kushnirenko // Baltic Journal of Economic Studies [Text]. — 2023. — T. 9. — № 1. — P. 89—99.

253. Kyprianou I., Serghides D., Carlucci S. Urban vulnerability in the EMME region and sustainable development goals: A new conceptual framework / I. Kyprianou // Sustainable Cities and Society [Text]. —2022. — № 80.

254. Leal Filho W. Industry, Innovation and Infrastructure [Text] / A. Azul, L. Brandli, A. Lange Salvia, T. Wall (eds). — Cham: Springer International Publishing, 2021.

255. Levin N., Ali S., Crandall D. Utilizing remote sensing and big data to quantify conflict intensity: The Arab Spring as a case study / N. Levin // Applied Geography [Text]. — 2018. — №94. — P. 1—17.

256. Magomedov A., Ivanov A., Pron L., Trostianska K., Forkun I. Administrative oversight of critical infrastructure and social security protection. *AD ALTA: Journal Of Interdisciplinary Research (14/01-XLII.)* 2024, p. 16-20. URL: https://doi.org/10.5281/zenodo.11816980.

257. Mahoney E., Golan M., Kurth M., Trump B. D., Linkov I. Resilience-by-Design and Resilience-by-Intervention in supply chains for remote and indigenous communities / E. Mahoney // Nature Communications [Text]. — 2022. — № 13(1).

258. Malchykova D. S., Pylypenko I. O., Ostapenko P. O. Spatial and Human Challenges of Recovery the De-Occupied Territories of Kherson Region / D. S. Malchykova // Український географічний журнал [Text]. — 2025. — № 2. — P. 67—77.

259. Mapping Ukraine’s democratic space in 40 localities // Kyiv School of Economics [Electronic resource]. — Access mode : https://kse.ua/kse-research/mapping-ukraine-s-democratic-space-in-40-localities/.

260. Mark A. Ehlen, Vargas V. Multi-hazard, multi-infrastructure, economic scenario analysis / A. Mark // Environment, Systems & Decisions [Text]. — 20213. — № 33(1). — P. 60— 75.

261. Martin R., Unsworth S., Valero A., Verhoeven D. Innovation for a strong and sustainable recovery. Centre for Economic Performance // London School of Economics and Political Science [Electronic resource]. — Access mode : https://cep.lse.ac.uk/pubs/download/cepcovid-19-014.pdf.

262. Martynovych N., Boichenko E., Dielini M. Rebuilding of Ukraine after war: Special restoration regimes and stimulation of sustainable development of territories / N. Martynovych // International Review for Spatial Planning and Sustainable Development [Text]. — 2023. — T. 11. — № 4. — P. 54—70.

263. Maxwell D., Stites E., Robillard S. C., Wagner M. Conflict and resilience: A synthesis of Feinstein International Center work on building resilience and protecting livelihoods in conflict-related crises // Boston: Feinstein International Center, Tufts University [Electronic resource]. — Access mode : https://fic.tufts.edu/wp-content/uploads/FIC-Publication-Q2_web_2.26s.pdf.

264. McAuley W. The Realm of More or Less: Critical Infrastructure and Public Order Factors for Pandemic Strategy / W. McAuley // Journal of Military and Strategic Studies [Text]. — 2022. — № 21(3). — P. 22—65.

265. McDonald D. To corporatize or not to corporatize (and if so, how?) / D. McDonald // Utilities Policy [Text]. — 2016. — № 40. — P. 107—114.

266. Measuring the Impact of Sustainability-related Investments on the Real Economy // Eurosif [Electronic resource]. — Access mode : https://www.eurosif.org/wp-content/uploads/2025/06/Measuring-the-Impact-of-Sustainability-related-Investments-on-the-Real-Economy.pdf.

267. Memorandum of Understanding on collaboration on Ukrainian energy system resilience // U.S. Embassy in Ukraine [Electronic resource]. — Access mode : https://ua.usembassy.gov/memorandum-of-understanding-between-ukraine-and-the-usa-regarding-collaboration-on-ukrainian-energy-system-resilience/.

268. Mitoulis S. A., Argyroudis S. A., Loli M., Imam B. Restoration models for quantifying flood resilience of bridges / S. A. Mitoulis // Engineering Structures [Text]. — 2021. — № 238.

269. Mitoulis S. A., Argyroudis S., Panteli M., Fuggini C., Valkaniotis S., Hynes W., Linkov I. Conflict Resilience Framework for Critical Infrastructure Peacebuilding / S. A. Mitoulis // Sustainable Cities and Society [Text]. —2023. — № 91.

270. Monstadt J., Schmidt M. Urban resilience in the making? The governance of critical infrastructures in German cities / J. Monstadt, M. Schmidt // Urban Studies [Text]. — 2019. — № 56 (11). — P. 2353—2371.

271. Mottahedi A., Sereshki F., Ataei M., Nouri Qarahasanlou A., Barabadi A. The resilience of critical infrastructure systems: a systematic literature review / A. Mottahedi // Energies [Text]. — 2021. — Vol. 14. — № 6. — P. 1571.

272. Moynihan D. Managing for Results in State Government: Evaluating a Decade of Reform / D. Moynihan // Public Administration Review. — 2006. — № 66(1). — P. 77—89.

273. Multi-agency Donor Coordination Platform for Ukraine launched to coordinate support // European Commission – Press corner [Electronic resource]. — Access mode : https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1921

274. Nadvi K., Waltring F. (2004). Making sense of global standards, in H. Schmitz (ed.) // Local Enterprises in the Global Economy [Text], Wiley, 2004. — 113 p.

275. National Cyber Security Strategy [Electronic resource]. — Access mode : https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.

276. National Defense Strategy // U.S. Department of Defense [Electronic resource]. — Access mode : https://www.defense.gov/National-Defense-Strategy/

277. National Infrastructure Protection Plan // United States Department of Homeland Security [Electronic resource]. — Access mode : https://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf.

278. National Strategy for Critical Infrastructure Protection (CIP Strategy) // Bundesministerium des Innern und für Heimat [Electronic resource]. — Access mode

:

https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=1.

279. Neikova M. Legal Approach To Implementing Security Measures For Combatting Threats To National Critical Infrastructures / M. Neikova // Environment. Technologies. Resources. Proceedings of the International Scientific and Practical Conference [Text]. — 2024. — № 4. — P. 190-193.

280. New IEA report outlines key steps to build more resilient and decentralised power system in Ukraine // International Energy Agency [Electronic resource]. — Access mode : https://www.iea.org/news/new-iea-report-outlines-key-steps-to-build-more-resilient-and-decentralised-power-system-in-ukraine.

281. Norwegian National Cyber Security Centre (NCSC) and NorCERT [Electronic resource]. — Access mode : https://nsm.no/areas-of-expertise/cyber-security/norwegian-national-cyber-security-centre-ncsc/.

282. Novikova I., Zabarna E., Volkova O., Fedotova I., Korolkov V. Economic prospects of post-war recovery: challenges and opportunities for sustainable development in Ukraine / I. Novikova // Financial and Credit Activity: Problems of Theory and Practice [Text]. — 2023. — Vol. 3. — Issue 50. — P. 298—307.

283. Office of the Prime Minister [Electronic resource]. — Access mode : https://www.regjeringen.no/en/dep/smk/organization-map/id901/.

284. Ola T. Why You Should Think Twice About It // Medium [Electronic resource]. — Access mode : https://medium.com/@olaisrael.official/agile-method-the-future-of-infrastructure-projects-heres-why-you-should-think-twice-about-it-0a57540c46bb.

285. Omelyanenko V., Omelianenko O. Infrastructure and service methodology for the development of innovative hromadas: general idea and example of smart city infrastructure / V. Omelyanenko, O. Omelyanenko // Three Seas Economic Journal [Text]. — 2023. — Vol. 4. — № 1. — P. 49—57.

286. Osborne D., Hutchinson P. The price of government: Getting the results we need in an age of permanent fiscal crisis [Text] / D. Osborne, P. Hutchinson. — Basic Books (AZ), 2006. — 384 p.

287. Palei T. Assessing the impact of infrastructure on economic growth and global competitiveness / T. Palei // Procedia Economics and Finance [Text]. — 2015. — № 23. — P. 168—175.

288. Panos E., Hassan A. Accelerating the Performance of Large-Scale TIMES Models in the Modelling of Sustainable Development Goals, in M. Labriet, K. Espegren, G. Giannakidis, B. Ó Gallachóir (eds) // Aligning the Energy Transition with the Sustainable Development Goals: Key Insights from Energy System Modelling [Text], Cham: Springer Nature Switzerland, 2024. — P. 67—95.

289. Parkes K. Partnering with Google to help protect Australians from cyberattacks // CSIRO [Electronic resource]. — Access mode : https://www.csiro.au/en/news/all/articles/2024/september/google-x-cipr-software-security.

290. Participatory Democracy in Ukrainian Hromadas — Analysis of 2024 Indicators // Centre for Insights Development (CID) [Electronic resource]. — Access mode : https://cid.center/en/analytics/demokratiya-uchasti-v-ukrayinskyh-hromadah-analiz-pokaznykiv-2024-roku-en-translation/ (дата звернення: 31.10.2025).

291. Patrascu P., Nicoara G. Public administration and critical infrastructure protection / P. Patrascu [Electronic resource]. — Access mode : http://jurisprudentia.uab.ro/upload/9_20_annales_nr25.pdf#page=99

292. Pescaroli G., Alexander D. Critical infrastructure, panarchies and the vulnerability paths of cascading disasters / G. Pescaroli, D. Alexander // Natural Hazards [Text]. — 2016. — № 82. — P. 175—192.

293. Petit F., Verner D., Brannegan D., Buehring W., Dickinson D., Guziel K., Haffenden R., Phillips J., Peerenboom P. J. Analysis of critical infrastructure dependencies and interdependencies // Argonne National Lab. [Electronic resource]. — Access mode : https://www.researchgate.net/publication/299525808_Analysis_of_Critical_Infrastructure_Dependencies_and_Interdependencies.

294. PGPA legislation, associated instruments and policies // Australian Government Department of Finance [Electronic resource]. — Access mode : https://www.finance.gov.au/government/managing-commonwealth-resources/pgpa-

legislation-associated-instruments-and-policies#:~:text=The%20Public%20Governance%2C%20Performance%20and,on%20planning%2C%20performance%20and%20reporting.

295. Polovenko V., Magomedov A., Kravtsev O., Krasnostanova N., Kryzhanovskyi S. Regulatory and Institutional Frameworks for Ensuring Financial Security in Ukraine's Energy Sector: Challenges and Future Outlook. *Grassroots Journal of Natural Resources,* 2024, 7(3): s313-s330. DOI: https://doi.org/10.33002/nr2581.6853.0703ukr16.

296. Prakash A., Potoski M. Racing to the Bottom? Trade, Environmental Governance, and ISO 14001 / A. Prakash, M. Potoski // American Journal of Political Science [Text]. — 2006. — № 50(2). — P. 350—364.

297. Project Management Institute. A Guide to the Project Management Body of Knowledge (PMBOK® Guide) (5th ed.) [Text]. Newtown Square, PA, 2013.

298. Public Governance Research Grid Initiative. Національне агентство із забезпечення якості вищої освіти [Electronic resource]. — Access mode : https://naqa.gov.ua/research-grid-initiative.

299. Public Governance, Performance and Accountability Rule 2014 // Transparency Portal [Electronic resource]. — Access mode : https://www.transparency.gov.au/publications/industry-science-and-resources/australian-nuclear-science-and-technology-organisation/australian-nuclear-science-and-technology-organisation-annual-report-2019-20/index-of-compliance-with-reporting-guidelines/.

300. Public Law 107–296: An Act 116 STAT. 2135 of November 25, 2002 [Electronic resource]. — Access mode : https://www.congress.gov/107/plaws/publ296/PLAW-107publ296.pdf.

301. Public Safety Canada Departmental Plan 2023–24 [Electronic resource]. — Access mode : https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-pln-2023-24/index-en.aspx.

302. Pursiainen C. Critical infrastructure resilience: A Nordic model in the making? / C. Pursiainen // International Journal of Disaster Risk Reduction [Text]. — 2018. — № 27. — P. 632—641.

303. Pursiainen C., Kytömaa E. From European critical infrastructure protection to the resilience of European critical entities: what does it mean? / C. Pursiainen, E. Kytömaa // Sustainable and Resilient Infrastructure [Text]. — 2022. — Vol. 8. — No 1. — P. 85—101.

304. Qian Z. H., Yuan J. S., Shi J., Cao X. Y. Recent Developments and Innovations in Resilient Infrastructure: Exploring Cutting-Edge Strategies, Technologies, and Practices / Z. Qian // Buildings [Text]. — 2025. — Vol. 15. — № 5. — P. 792.

305. Ravia H., Hammer D., Amir A. Cybersecurity: Definitive global law guides offering comparative analysis from top-ranked lawyers // Pearl Cohen Zedek Latzer Baratz [Electronic resource]. — Access mode : https://www.law.co.il/media/knowledge-centers/chambers-cybersecurity-israel-2021.pdf.

306. Regulator Performance // Australian Government Transparency Portal [Electronic resource]. — Access mode : https://www.transparency.gov.au/publications/health/australian-radiation-protection-and-nuclear-safety-agency-arpansa/australian-radiation-protection-and-nuclear-safety-agency-annual-report-2021-22/part-3%3A-report-on-performance/regulator-performance.

307. Regulator Performance Framework // Australian Government: The Treasury [Electronic resource]. — Access mode : https://treasury.gov.au/the-department/accountability-reporting/regulator-performance-framework#:~:text=The%20Regulator%20Performance%20Framework%20commenced,through%20their%20administration%20of%20regulation.

308. Rehbohm T., Sandkuhl K., Cap C. H., Kemmerich T. Integrated Security Management of Public and Private Sector for Critical Infrastructures – Problem Investigation, in: W. Abramowicz, S. Auer, M. Stróżyna (eds) // Business Information Systems Workshops [Text], Springer, Cham, 2021. — P. 291—303.

309. Review of Regulation (EU) 2019/2088 on sustainability-related disclosures in financial services // European Parliament – Policy Briefing [Electronic resource]. — Access mode :

https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/774660/EPRS_BRI%28
2025%29774660_EN.pdf.

310. Rimutis S. Lessons of War: Ukraine's Energy Infrastructure Damage, Resilience and Future Opportunities // Eastern Europe Studies Center [Electronic resource]. — Access mode : https://www.gssc.lt/wp-content/uploads/2024/05/v04_Rimutis_Ukrainos-energetikos-sektoriaus-zala_EN_A4.pdf.

311. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej [Electronic resource]. — Access mode : https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20100830542.

312. Santhosh T. V., Patelli E. Resilience engineering: principles, methods, and applications to critical infrastructure systems, in E. N. Farsangi (ed.) // Reliability-Based Analysis and Design of Structures and Infrastructure [Text], CRC Press, 2021. — P. 65–78.

313. Sathurshan M., Saja A., Thamboo J., Haraguchi M., Navaratnam S. Resilience of critical infrastructure systems: a systematic literature review of measurement frameworks / M. Sathurshan // Infrastructures [Text]. — 2022. — Vol. 7. — № 5. — P. 67.

314. Schlör H., Venghaus S., Hake J. F. The FEW-Nexus city index–Measuring urban resilience / H. Schlör // Applied Energy [Text]. — 2018. — №210. — P. 382—392.

315. Security of Critical Infrastructure Act 2018 (SOCI) // Department of Home Affairs [Electronic resource]. — Access mode : https://www-cisc-gov-au.translate.goog/legislation-regulation-and-compliance/soci-act-2018?_x_tr_sl=en&_x_tr_tl=uk&_x_tr_hl=uk&_x_tr_pto=sc.

316. Security Project [Electronic resource]. — Access mode : https://energysecurityua.org/helping-ukraine/.

317. Shaji George A., Baskar T., Balaji Srikaanth P. Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors / A. Shaji George // Partners Universal International Innovation Journal [Text]. — 2024. — Vol. 2. — № 1. — P. 51—75.

318. Skolimowska A. Interdependence of Critical Infrastructure, in R. Wróbel (ed.) // Critical Infrastructure Protection System [Text], Warsaw, 2013.

319. Spronk S., Crespo C., Olivera M. Modernization and the boundaries of public water in Uruguay, in David A. McDonald // Rethinking corporatization and public services in the Global South [Text], Zed Books, 2014. — 240 p.

320. Stancu A. I., Pavel T. Unveiling Israel's Cyber Legal Landscape: A Comprehensive Analysis of Cybersecurity Regulations and Policies / A. I. Stancu // Perspectives of Law and Public Administration [Text]. — 2023. — № 12(4). — P. 643—650.

321. Strahnitskyi Y. Institutional transformations in the direction of increasing the effectiveness of the state policy of critical infrastructure protection / Y. Strahnitskyi // Public Administration and Regional Development [Text]. — 2024. — № 23. — P. 28—51.

322. Supporting Ukraine’s Vision — UNDP portfolio results 2024 [Electronic resource]. — Access mode : https://www.undp.org/sites/g/files/zskgke326/files/2025-07/undp-brochure_july2025_1.pdf.

323. Swiss Sustainable Investment Market Study 2025 // Sustainable Finance Observatory [Electronic resource]. — Access mode : https://www.sustainablefinance.ch/api/rm/3Q78TKT6Y3465YZ/ssf-sustinvt-market-study-2025-1.pdf.

324. Tabansky L., Ben Israel I. The Israeli National Cybersecurity Policy Focuses on Critical Infrastructure Protection (CIP) [Text] / L. Tabansky, I. Ben Israel // Cybersecurity in Israel. — SpringerBriefs in Cybersecurity Springer, Cham, 2015. — P. 35—41.

325. Terhorst P., Olivera M., Dwinell A. Social movements, left governments, and the limits of water sector reform in Latin America’s left turn / P. Terhorst // Latin American Perspectives [Text]. —2013. — № 40(4). — P. 55—69.

326. The 2022 National Defense Strategy (NDS) // Secretary of Defence [Electronic resource]. — Access mode : https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf.

327. The architecture of infrastructure recovery in Ukraine // OECD [Electronic resource]. — Access mode : https://www.oecd.org/en/publications/2022/07/the-architecture-of-infrastructure-recovery-in-ukraine_c09fffd4.html.

328. The Critical Infrastructure Protection in France // SGDSN [Electronic resource]. — Access mode : https://www.sgdsn.gouv.fr/files/files/Publications/plaquette-saiv-anglais.pdf.

329. The European Green Deal [Electronic resource]. — Access mode : https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en.

330. The Global Risks Report 2020: Insight Report. In partnership with Marsh & McLennan and Zurich Insurance Group (15th Edition) // World Economic Forum (WEF) [Electronic resource]. — Access mode : https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

331. The impact of the Prozorro procurement system on the Ukrainian economy. EBRD — Law in Transition Journal [Electronic resource]. — Access mode : https://www.ebrd.com/content/dam/ebrd_dxp/assets/pdfs/legal-transition/Law%20in%20Transition%20journal/LiTJ%202025/ebrd-lit25-the-impact-of-the-prozorro-procurement-system-on-the-ukrainian-economy.pdf.

332. The new Israeli Cyber Law paving the way for unlawful hacking and digital rights violations [Electronic resource]. — Access mode : https://7amleh.org/2018/07/12/the-new-israeli-cyber-law-paving-the-way-for-unlawful-hacking-and-digital-rights-violations.

333. The smart way to rebuild Ukraine? Recycle the rubble // The Times [Electronic resource]. — Access mode : https://www.thetimes.co.uk/article/smart-way-rebuild-recycle-rubble-mbbhgdl32.

334. TSOs launch new process to calculate net transfer capacity at the borders of Ukraine and Moldova // ENTSO-E [Electronic resource]. — Access mode : https://www.entsoe.eu/news/2025/06/18/tsos-launch-new-process-to-calculate-net-transfer-capacity-at-the-borders-of-ukraine-and-moldova/.

335. Tzifakis N. Post-conflict economic reconstruction, in W. F. Danspeckgruber (ed.) // Encyclopedia Princetoniensis: the Princeton Encyclopedia of self-determination [Text]. Princeton University, Liechtenstein Institute on Self-Determination, 2013.

336. Ukraine — European Civil Protection and Humanitarian Aid Operations (country page) [Electronic resource]. — Access mode : https://civil-protection-humanitarian-aid.ec.europa.eu/where/europe/ukraine_en.

337. Ukraine — Fourth Rapid Damage and Needs Assessment (RDNA4): Feb 2022 – Dec 2024 [Electronic resource]. — Access mode : https://documents1.worldbank.org/curated/en/099022025114040022/pdf/P180174-ca39eccd-ea67-4bd8-b537-ff73a675a0a8.pdf.

338. Ukraine Boosts Regional Digitalization – Digital State UA [Electronic resource]. — Access mode : https://digitalstate.gov.ua/news/govtech/onovlena-diiatsyfrova-hromada-bilshe-mozlyvostey-dlia-rehioniv.

339. Ukraine Donor Platform confirms continued strong support for Ukraine's recovery and reconstruction 2025-04-02 // European Commission – DG NEAR [Electronic resource]. — Access mode : https://enlargement.ec.europa.eu/news/ukraine-donor-platform-confirms-continued-strong-support-ukraines-recovery-and-reconstruction-2025-04-02_en.

340. Ukraine Facility – Programme performance statement (completed steps and tranches) // European Commission [Electronic resource]. — Access mode : https://commission.europa.eu/strategy-and-policy/eu-budget/performance-and-reporting/programme-performance-statements/ukraine-facility_en.

341. Ukraine Facility – Ukraine Plan and investment framework // European Commission — DG NEAR [Electronic resource]. — Access mode : https://enlargement.ec.europa.eu/funding-technical-assistance/ukraine-facility_en.

342. Ukraine Investment Framework under the Ukraine Facility // European Commission – Enlargement [Electronic resource]. — Access mode : https://enlargement.ec.europa.eu/document/download/c178ec0d-884f-436d-8445-9014a220b1d4_en?filename=C_2025_6324_1_EN_annexe_acte_autonome_nlw_part1_v2.pdf.

343. Ukraine launches Digital State UA: a global platform for digital solutions and GovTech // Embassy of Ukraine in Angola [Electronic resource]. — Access mode : https://angola.mfa.gov.ua/en/news/launch-digital-state-ua-platform.

344. Ukraine Overview – World Bank Group Support to Ukraine [Electronic resource]. — Access mode : https://www.worldbank.org/en/country/ukraine/overview

345. Ukraine recovery and reconstruction will cost $524bn over next decade, says report // Reuters [Electronic resource]. — Access mode : https://www.reuters.com/world/europe/ukraine-needs-524-billion-recover-rebuild-after-three-years-war-world-bank-says-2025-02-25/.

346. Ukraine Recovery Digest № 170 // Ukraine Recovery Digest [Electronic resource]. — Access mode : https://rdo.in.ua/sites/default/files/pdf/digest170_eng.pdf.

347. Ukraine Recovery Digest №160 // RDO [Electronic resource]. — Access mode : https://rdo.in.ua/sites/default/files/pdf/digest160_eng.pdf.

348. Ukraine showcases strategic role of open data during wartime at international e-governance conference in Estonia // EU4DigitalUA [Electronic resource]. — Access mode : https://eu4digitalua.eu/en/news/ukraine-showcases-strategic-role-of-open-data-during-wartime-at-international-e-governance-conference-in-estonia/.

349. Ukraine: Humanitarian Response and Funding Snapshot (January–May 2025) // OCHA [Electronic resource]. — Access mode : https://www.unocha.org/publications/report/ukraine/ukraine-humanitarian-response-and-funding-snapshot-january-may-2025-enuk.

350. Ukraine’s Digital Transformation: Innovation for Resilience // Harvard Kennedy School [Electronic resource]. — Access mode : https://www.hks.harvard.edu/centers/cid/voices/ukraines-digital-transformation-innovation-resilience.

351. Ukraine’s Energy Security – Analysis // International Energy Agency [Electronic resource]. — Access mode : https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter.

352. Ukraine’s energy system under attack // International Energy Agency [Electronic resource]. — Access mode : https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter/ukraines-energy-system-under-attack.

353. Unlocking Ukraine’s Hydrogen Opportunity: A Roadmap // International Energy Agency [Electronic resource]. — Access mode : https://www.iea.org/reports/unlocking-ukraines-hydrogen-opportunity-a-roadmap.

354. Updated Ukraine Recovery and Reconstruction Needs Assessment released // World Bank [Electronic resource]. — Access mode : https://www.worldbank.org/en/news/press-release/2025/02/25/updated-ukraine-recovery-and-reconstruction-needs-assessment-released.

355. USA PATRIOT Act // United States Government [Electronic resource]. — Access mode : https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act

356. USAID Energy Security Project: supporting resilience of Ukraine’s energy system // USAID ESP [Electronic resource]. — Access mode : https://energysecurityua.org/.

357. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym // Kancelaria Sejmu RP [Electronic resource]. — Access mode : https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20070890590.

358. Ustawa z dnia 3 czerwca 2005 r. o szczególnych uprawnieniach Skarbu Państwa oraz ich wykonywaniu w spółkach kapitałowych o istotnym znaczeniu dla porządku publicznego lub bezpieczeństwa publicznego [Electronic resource]. — Access mode : https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20051321108.

359. Van der Vleuten E. Critical Infrastructure: Europe’s vulnerability geography // Encyclopédie pour une histoire numérique de l'Europe [Electronic resource]. — Access mode : https://ehne.fr/en/encyclopedia/themes/material-civilization/major-technological-networks-and-sovereignty/critical-infrastructure-europe%E2%80%99s-vulnerability-geography.

360. Venkataraman A., Lim S. H. C., Hao L. J., Wee J. C. P. From Fragmentation to Integration in Emergency Medicine: Providing Care Our Patients Deserve / A. Venkataraman // Medical Research Archives [Text]. —2024. — № 12(4).

361. Wang Y., Zhao O., Zhang L. Multiplex networks in resilience modeling of critical infrastructure systems: A systematic review / Y. Wang // Reliability Engineering & System Safety [Text]. — 2024. — № 250.

362. Warner M., Gradus R. The Consequences of Implementing a Child Care Voucher Scheme: Evidence from Australia, the Netherlands and the USA / M. Warner, R. Gradus // Social Policy Administration [Text]. — 2011. — № 45(5). — P. 569—592.

363. Watkins G. G., Mueller S. U., Meller H., Ramirez M. C., Serebrisky T., Georgoulias A. Lessons from four decades of infrastructure project-related conflicts in Latin America and the Caribbean // Inter-American Development Bank [Electronic resource]. — Access mode : https://publications.iadb.org/en/lessons-four-decades-infrastructure-project-related-conflicts-latin-america-and-caribbean.

364. Weber, V., Pericàs Riera, M., & Laumann, E. (2023). Mapping the World's Critical Infrastructure Sectors: DGAP Policy Brief 35 // German Council on Foreign Relations [Electronic resource]. — Access mode : https://doi.org/10.60823/DGAP-23-39548-en.

365. Weir D., McQuillan D., Francis R. A. Civilian science: the potential of participatory environmental monitoring in areas affected by armed conflicts / D. Weir // Environmental Monitoring and Assessment [Text]. — 2019. — № 191(10). P. 618.

366. Why and how the public should monitor public procurement in 2025. Transparency International Ukraine // DOZORRO [Electronic resource]. — Access mode : https://ti-ukraine.org/en/blogs/why-and-how-the-public-should-monitor-public-procurement-in-2025/

367. Witmer F. D. Remote sensing of violent conflict: eyes from above / F. D. Witmer // International Journal of Remote Sensing [Text], — 2015. — № 36(9). — P. 2326—2352.

368. Wódkiewicz R. Podstawowe zagrożenia funkcjonowania obiektów infrastruktury krytycznej / R. Wódkiewicz // Zeszyty Naukowe SGSP [Text]. — 2022. — № 83. — P. 141—161.

369. Wróbel R. Dependencies of elements recognized as critical infrastructure of the state / R. Wróbel // Transportation Research Procedia [Text]. — 2019. — № 40. — P. 1625—1632.

370. Yadav G., Paul K. Architecture and security of SCADA systems: A review / G. Yadav, K. Paul // International Journal of Critical Infrastructure Protection [Text]. — 2021. — № 34.

371. Yang Y., Ng S. T., Xu F. J., Skitmore M. Towards sustainable and resilient high density cities through better integration of infrastructure networks / Y. Yang // Sustainable Cities and Society [Text], —2018. — № 42. — P. 407—422.

372. Yefimenko I., Sakovskyi A., Bilozorov Y. Protection of critical infrastructure as a component of Ukraine's national security / I. Yefimenko // Law Journal of the National Academy of Internal Affairs [Text]. — 2023. — Vol. 2. — № 13. — P. 74—85.

373. Zaidan S., El Fadel M. Sustainable development goals in energy system models: A systematic interlinkages mapping analysis / S. Zaidan, M. El Fadel // Journal of Cleaner Production [Text]. — 2024. — № 464.

374. Zatonatskiy D., Horiacheva K. Digitalization and cybersecurity of critical infrastructure enterprises according to EU standards / D. Zatonatskiy, K. Horiacheva // Finance of Ukraine [Text]. — 2025. — № 3. — P. 77—91.

375. 6 CFR Part 29: Rules and Regulations // Federal Register [Electronic resource]. — Access mode : https://www.cisa.gov/sites/default/files/2023-01/pcii-program-final-rule-technical-amendments-122022.pdf.

376. XVI Richelieu Public Service Forum 2024 took place in Kyiv (on transformation of public service and resilience) // НАДС [Electronic resource]. — Access mode : https://nads.gov.ua/en/news/xvi-richelieu-public-service-forum-2024-took-place-in-kyiv-summary.

ДОДАТОК А

БОРИСПІЛЬСЬКА РАЙОННА ДЕРЖАВНА АДМІНІСТРАЦІЯ
КИЇВСЬКОЇ ОБЛАСТІ

БОРИСПІЛЬСЬКА РАЙОННА ВІЙСЬКОВА АДМІНІСТРАЦІЯ
КИЇВСЬКОЇ ОБЛАСТІ

вул. Київський Шлях, 74, м. Бориспіль, 08305, тел. (04595) 6-12-58, (04595) 6-06-81,
e-mail: rda@raybori.gov.ua, сайт: www.raybori.gov.ua, код згідно з ЄДРПОУ 24209740

_____ № _____ **На №** _____ **від** _____

ДОВІДКА

про впровадження результатів дисертаційного дослідження
Магомедова Андрія Омаровича на тему: «Концептуальні засади публічного управління у сфері трансформації об'єктів критичної інфраструктури»
на здобуття ступеня доктора наук з державного управління за спеціальністю 25.00.02 «Механізми державного управління»

У діяльності Бориспільської районної державної (військової) адміністрації Київської області застосовано окремі результати досліджень Магомедова Андрія Омаровича «Концептуальні засади публічного управління у сфері трансформації об'єктів критичної інфраструктури».

Важливими є напрацювання дисертанта щодо функціональних блоків, які формують організаційно - управлінське забезпечення трансформаційних процесів у сфері відновлення критичної інфраструктури, до яких належать:

- інфраструктурно - обліковий блок, який відповідає за централізоване збирання, актуалізацію та верифікацію інформації про стан об'єктів критичної інфраструктури, їхній технічний ресурс, строк служби та рівень експлуатаційної придатності;

- міжвідомчо - координаційний блок, завданням якого є забезпечення скоординованих управлінських дій між Кабінетом Міністрів України, центральними органами виконавчої влади, військовими адміністраціями та органами місцевого самоврядування щодо реалізації державної політики трансформації об'єктів критичної інфраструктури;

- аналітично - прогностичний блок, що виконує функції формування варіантів розвитку інфраструктурних змін із урахуванням імовірнісного моделювання ризиків, потреб безпеки громад, індикаторів зношеності та адаптації до стратегічних викликів;

UB Бориспільська районна державна адміністрація
№12-10/21-д від 21.04.2026
арк.1

- ресурсно - забезпечувальний блок, який визначає джерела фінансування, формує резерви матеріально-технічних засобів, забезпечує кадрове наповнення та логістику реалізації інфраструктурних рішень;
- інформаційно-аналітичний блок, що забезпечує безперервний моніторинг стану реалізації управлінських заходів, оцінює динаміку їх ефективності та забезпечує прозорість результатів для всіх зацікавлених сторін.

Заступник голови адміністрації **Андрій СИНЯКОВ**

КИЇВСЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ

КИЇВСЬКА ОБЛАСНА ВІЙСЬКОВА АДМІНІСТРАЦІЯ

ДЕПАРТАМЕНТ ЖИТЛОВО-КОМУНАЛЬНОГО ГОСПОДАРСТВА ТА ЕНЕРГОЕФЕКТИВНОСТІ

вул. Юрія Іллєнка, 40, м. Київ, 04119, тел. (044) 206 74 46, E-mail: dekg@koda.gov.ua код згідно ЄДРПОУ 34695981

_____ № _____ на № _____ від _____

ДОВІДКА

про впровадження результатів дисертаційного дослідження
Магомедова Андрія Омаровича
на тему: «Концептуальні засади публічного управління у сфері трансформації об'єктів критичної інфраструктури»
на здобуття ступеня доктора наук з державного управління
за спеціальністю 25.00.02 «Механізми державного управління»

У діяльності Департаменту житлово-комунального господарства та енергоефективності Київської обласної військової адміністрації застосовано окремі результати досліджень Магомедова Андрія Омаровича «Концептуальні засади публічного управління у сфері трансформації об'єктів критичної інфраструктури».

Важливі положення дослідження Магомедова А. О. знайшли відображення в пропозиціях Департаменту щодо концептуальної логіки становлення інтегрованої системи публічного управління трансформацією критичної інфраструктури, що складається з етапів: I. Діагностика: об'єктивна оцінка втрат і вразливостей інфраструктури; пріоретизація портфелів відновлення; II. Координація у відновленні: усунення дублювання повноважень та відповідальності, синхронізація ресурсів і термінів; III. Цифровізація: забезпечення прозорості, прискорення прийняття рішень, контроль якості виконання; IV. Адаптація системи управління: стійкість сервісів, оптимізація витрат; V. Оцінювання результативності: відтворюваність політики, підзвітність, корекція «roadmap».

Директор департаменту Олександр ПОПРОЦЬКИЙ

Департамент житлово-комунального господарства та енергоефективності Київської обласної державної адміністрації
№7327/35/2026 від 16.06.2026
КЕП: ПОПРОЦЬКИЙ О. П. 16.06.2026
5E984D526F82F38F04000000F9F0FF00C0D89006
Сертифікат дійсний з 12.08.2025 до 12.08.2026 23:59

ГО «Східно-Європейська спілка науковців»
Код ЄДРПОУ 45512518
вул. Максимовича, 28-б/121, Київ, 03022
https://www.eu-scientists.com
e-mail: post@eu-scientists.com
тел. +38 067 894 38 07

Eastern European Union of Scientists NGO
USREOU code 45512518
28-b/121, Maksymovych St., Kyiv, 03022
https://www.eu-scientists.com
e-mail: post@eu-scientists.com
tel. +38 067 894 38 07

вих. № 08/2026 від 04.04.2026 р.

ДОВІДКА
про впровадження результатів дисертаційного дослідження
Магомедова Андрія Омаровича

У діяльності Громадської організації «Східно-Європейська спілка науковців» застосовано окремі результати дисертаційного дослідження Магомедова Андрія Омаровича при виконанні дослідницької роботи на тему: «Концептуальні засади публічного управління у сфері трансформації об'єктів критичної інфраструктури».

Важливі положення дослідження Магомедова Андрія Омаровича знайшли відображення в результатах обговорення громадських ініціатив щодо соціально-економічних трансформацій в умовах війни та у повоєнному періоді. Важливими виділено основні принципи механізму публічного управління відновленням критичної інфраструктури, до яких належать:

– багатофакторна оцінка спроможності об'єкта критичної інфраструктури функціонувати в умовах впливу дестабілізуючих чинників, що передбачає інтеграцію показників технічного стану, рівня захищеності, соціальної значущості та ступеня взаємозалежності з іншими інфраструктурними вузлами;

– узгодження інтересів ключових суб'єктів управління, включаючи органи виконавчої влади, місцеве самоврядування, спеціалізовані служби, що забезпечує скоординоване планування, розподіл відповідальності та уникнення конфліктів компетенцій;

– системна підтримка міжінституційної взаємодії, що передбачає створення механізмів постійної кооперації, обміну інформацією та спільного управління ризиками між органами публічної влади на різних рівнях;

– контроль за використанням і розподілом стратегічно важливих ресурсів, які є критичними для стабільного функціонування об'єктів, у тому числі резервного забезпечення, логістичної інфраструктури та енергопостачання;

– впровадження систем управління якістю процесів експлуатації та обслуговування об'єктів, з акцентом на екологічну, технологічну та соціальну

безпеку, із застосуванням інструментів функціонального аудиту, державно-громадського моніторингу та адаптивного регулювання;

– здатність до трансформації механізмів управління в умовах кризової ситуації або невизначеності зовнішнього середовища, що передбачає сценарне планування, резервне моделювання рішень та адаптивне бюджетування;

– побудова гнучких організаційно-управлінських структур, які забезпечують безперервність функціонування об'єктів у випадку порушення системи центрального управління або обмеженого доступу до ресурсів;

– формування як формалізованих, так і неформальних зв'язків між учасниками процесу управління, що посилює ефективність координації дій у разі надзвичайних ситуацій та підвищує рівень міжвідомчої комунікації;

– управління обсягом, якістю та актуальністю інформаційної бази щодо технічного стану об'єктів, можливих загроз, очікуваних сценаріїв розвитку подій, що забезпечує оперативність і достовірність управлінських рішень;

– узгодженість стратегічного та оперативного планування, що вимагає чіткої інтеграції довгострокових програм розвитку інфраструктурних секторів з інструментами щорічного програмно-цільового бюджетування, заснованого на достовірних даних та сучасних цифрових платформах.

Голова правління Мирослав БУРИК

ГРОМАДСЬКА ОРГАНІЗАЦІЯ "СХІДНО-ЄВРОПЕЙСЬКА СПІЛКА НАУКОВЦІВ" 45512518 УКРАЇНА

Міністерство освіти і науки України
УНІВЕРСИТЕТ ГРИГОРІЯ СКОВОРОДИ В ПЕРЕЯСЛАВІ
вул. Сухомлинського, 30,
м. Переяслав,
Київська обл., 08401
тел.: (044) 293-11-11
ел. пошта: uhsp.edu@gmail.com
код ЄДРПОУ 04543387
№

Ministry of Education and Science of Ukraine
HRYHORII SKOVORODA UNIVERSITY IN PEREIASLAV
30, Sukhomlynskoho Str.,
Pereiaslav,
Kyiv reg., 08401
tel.: (044) 293-11-11
e-mail: uhsp.edu@gmail.com

ДОВІДКА

про впровадження результатів дисертаційного дослідження
Магомедова Андрія Омаровича
на тему: «Концептуальні засади публічного управління у сфері трансформації об'єктів критичної інфраструктури»
на здобуття ступеня доктора наук з державного управління
за спеціальністю 25.00.02 Механізми державного управління

Результати дисертаційного дослідження Магомедова Андрія Омаровича «Концептуальні засади публічного управління у сфері трансформації об'єктів критичної інфраструктури» впроваджені в освітній процес та науково-методичну діяльність кафедри публічного управління та адміністрування Університету Григорія Сковороди в Переяславі.

Теоретико-методологічні положення та практичні рекомендації, розроблені дисертантом, використовуються при викладанні навчальних дисциплін кафедри публічного управління адміністрування. Зокрема, вони інтегровані в програми таких курсів: «Теорія і практика реформ», «Управлінський контроль в публічній сфері».

Особливу цінність для освітнього процесу становлять запропоновані дисертантом:

– система управлінських заходів відновлення об'єктів критичної інфраструктури у поствоєнний період;
– науково-методичний підхід до формування стратегічних документів відбудови об'єктів критичної інфраструктури України після війни;
– інноваційний інструментарій публічного управління трансформацією об'єктів критичної інфраструктури.

Матеріали та напрацювання, що викладені в дисертації, використовуються при оновленні робочих програм навчальних дисциплін та навчально-методичних комплексів.

Довідка видана для пред'явлення за місцем захисту дисертації.

Проректор
з навчально-методичної роботи Володимир НОСАЧЕНКО

Університет Григорія Сковороди в Переяславі
№ 647 від 08.06.2026

ДОДАТОК Б

Оцінка пошкодження об’єктів критичної інфраструктури України у період воєнного впливу

№	Сектор	Об’єкт / група об’єктів	Зафіксований стан	Кількісний / аналітичний показник	Значення	Одиниця	Характер впливу	Територіальна локалізація	Аналітичний висновок
1	Енергетика	Об’єкти енергетичної інфраструктури	пошкоджені / уражені	Загальні збитки	понад 12	млрд дол. США	критичний	прифронтові та тилові регіони	енергетика є найбільш вразливим сектором
2	Енергетика	ТЕС	уражені	Частка уражених ТЕС	усі	повне охоплення	системний	вся територія під контролем України	атаки мали не вибірковий, а системний характер
3	Енергетика	ГЕС	уражені	Частка уражених ГЕС	усі	повне охоплення	системний	державний рівень	пошкодження торкнулися всіх гідрооб’єктів
4	Енергетика	ТЕЦ	уражені	Кількість уражених ТЕЦ	20	од.	критичний	державний рівень	зафіксовано масштабне ураження теплоенергетики
5	Енергетика	Блоки ТЕС	пошкоджені	Кількість пошкоджених блоків під час одного масованого удару	9	од.	високий	опалювальний сезон 2022–2023 рр.	одиничний удар призвів до значного скорочення потужностей
6	Енергетика	Блоки ТЕС	знищені	Кількість повністю знищених блоків у межах згаданого удару	1	од.	критичний	опалювальний сезон 2022–2023 рр.	окремі елементи генерації втрачено безповоротно
7	Енергетика	Каховська ГЕС	повністю зруйнована	Прямі збитки	586	млн дол. США	катастрофічний	Херсонська область	руйнування мало національний і міжсекторальний ефект
8	Енергетика	Енергоблоки Ладижинської та	виведені з ладу	Втрачені потужності	понад 4	ГВт	критичний	Вінницька, Івано-	втрати суттєво вплинули на баланс генерації

№	Сектор	Об’єкт / група об’єктів	Зафіксований стан	Кількісний / аналітичний показник	Значення	Одиниця	Характер впливу	Територіальна локалізація	Аналітичний висновок
		Бурштинської ТЕС						Франківська обл.	
9	Енергетика	Харківська ТЕЦ-5	майже повністю знищена	Ступінь руйнування	майже повний	якісна оцінка	критичний	Харківська область	об’єкт втратив базову функціональність
10	Енергетика	Зміївська ТЕС	майже повністю знищена	Ступінь руйнування	майже повний	якісна оцінка	критичний	Харківська область	відновлення потребує не ремонту, а фактично реконструкції
11	Енергетика	Трипільська ТЕС	фактично перестала існувати	Статус об’єкта	функціонально втрачена	якісна оцінка	критичний	Київська область	об’єкт вибув із діючої енергосистеми
12	Транспорт	Автомобільні дороги	суттєво пошкоджені	Рівень пошкодження	високий	якісна оцінка	високий	різні області	порушено транспортну зв’язність територій
13	Транспорт	Мости	суттєво пошкоджені	Рівень пошкодження	високий	якісна оцінка	високий	різні області	транспортна система втратила частину вузлових елементів
14	Транспорт	Портова інфраструктура	суттєво пошкоджена	Рівень пошкодження	високий	якісна оцінка	високий	портові регіони	порушено зовнішньоторговельні та логістичні потоки
15	Телекомунікації	Телекомунікаційна інфраструктура	пошкоджена	Факт ураження	зафіксовано	бінарний індикатор	значний	державний рівень	цифрова стійкість знижена
16	Комунальне господарство	Об’єкти ЖКГ	пошкоджені	Факт ураження	зафіксовано	бінарний індикатор	значний	державний рівень	ураження впливають на базові послуги населенню
17	Охорона здоров’я	Об’єкти медичної інфраструктури	пошкоджені	Факт ураження	зафіксовано	бінарний індикатор	значний	державний рівень	ураження підвищують гуманітарні ризики

№	Сектор	Об’єкт / група об’єктів	Зафіксований стан	Кількісний / аналітичний показник	Значення	Одиниця	Характер впливу	Територіальна локалізація	Аналітичний висновок
18	Просторовий вимір	Прифронтові області	найбільші руйнування	Просторовий патерн	максимальна концентрація	якісна оцінка	критичний	прифронтові регіони	ступінь руйнування залежить від близькості до бойових дій
19	Просторовий вимір	Тилові регіони	об’єкти також уражалися	Просторовий патерн	наявні атаки	якісна оцінка	високий	тилові регіони	безпекова загроза має загальнодержавний характер
20	Управлінський вимір	Уся система КІ	потребує відновлення	Тип необхідних дій	термінове відновлення і модернізація	якісна оцінка	системний	державний рівень	відбудова має поєднувати ремонт і технологічне оновлення

ДОДАТОК В

Аналітичні дані міжнародних моделей забезпечення стійкості та кібербезпеки критичної інфраструктури

№	Країна / група країн	Тип управлінської моделі	Координація державної політики	Оцінка ризиків	Інтегрована платформа обміну інформацією	Роль приватного сектору	Ключовий акцент моделі	Практична цінність для України
1	Франція	централізовано-координаційна	висока	багаторівнева	наявна	висока	стратегічна координація та стандартизація	придатна для посилення центральної координації
2	Нідерланди	мережева	висока	трирівнева	наявна	висока	узгодження держави й операторів	придатна для платформенного обміну даними
3	Велика Британія	інтегрована	висока	системна	наявна	висока	підзвітність і міжсекторальна взаємодія	придатна для побудови системи відповідальності
4	Держави ЄС загалом	наднаціонально-узгоджена	висока	гармонізована	розвинена	значна	класифікація КІ та спільні підходи	придатна для нормативної гармонізації
5	ЄС	міждержавна	висока	стандартизована	наявна	значна	стійкість внутрішнього ринку	корисна для синхронізації секторних правил
6	США	нормативно деталізована	дуже висока	системна	розвинена	дуже висока	захист фізичних і цифрових об’єктів	придатна для секторального розподілу відповідальності
7	США	міжвідомча	висока	формалізо-вана	наявна	дуже висока	довіра між державою і приватними операторами	придатна для моделі довіреного обміну даними
8	Канада	партнерська	висока	системна	наявна	дуже висока	кіберстійкість та міжнародна співпраця	придатна для моделі державно-приватного партнерства

№	Країна / група країн	Тип управлінської моделі	Координація державної політики	Оцінка ризиків	Інтегрована платформа обміну інформацією	Роль приватного сектору	Ключовий акцент моделі	Практична цінність для України
9	Ізраїль	централізована кібермодель	дуже висока	оперативна	наявна	висока	швидке реагування на кіберзагрози	придатна для створення центру кіберкоординації
10	Австралія	регуляторно-партнерська	висока	системна	наявна	дуже висока	нормативна база і участь бізнесу	придатна для регулювання участі приватного сектору
11	ЄС, США, Канада	порівняльний підсумок	висока	трирівнева / системна	інтегрована	висока	стійкість через координацію та дані	придатна для створення національної інтегрованої системи
12	Ізраїль, Австралія	порівняльний підсумок	висока	кіберорієнтована	наявна	висока	кіберзахист і швидка адаптація	придатна для кіберкомпонента української моделі

ДОДАТОК Г

Документальнео та проєктне забезпечення відбудови критичної інфраструктури України

№	Група показників	Конкретний індикатор	Кількісне значення	Одиниця виміру	Тип показника	Джерело формування	Рівень застосування	Управлінське призначення	Аналітична інтерпретація
1	Документальне забезпечення	Кількість звітів RDNA	4	од.	фактичний	міжнародні партнери, уряд України	національний	оцінка втрат і потреб	сформовано базову систему аналітичного моніторингу
2	Документальне забезпечення	Останній звіт	RDNA4	назва	факт	міжнародні організації	національний	оновлення даних	забезпечено актуалізацію оцінок
3	Документальне забезпечення	Періодичність оновлення	регулярна	якісна оцінка	процесний	міжнародні партнери	національний	відстеження динаміки	оцінювання має безперервний характер
4	Документальне забезпечення	Тип оцінки	швидка оцінка збитків	тип	класифікаційний	Світовий банк, ЄС	національний	формування бази даних	застосовується прискорена методологія
5	Документальне забезпечення	Структура оцінки	багатосекторна	тип	структурний	міжнародні партнери	національний	комплексний аналіз	охоплює всі сектори КІ
6	Фінансове планування	Оцінка потреб у фінансуванні	визначена	якісна оцінка	фінансовий	RDNA	національний	бюджетне планування	сформовано орієнтири фінансування
7	Фінансове планування	Облік інвестиційних проєктів	наявний	бінарний	фінансовий	RDNA	національний	контроль ресурсів	фіксуються проєкти відбудови
8	Фінансове планування	Облік неінвестиційних програм	наявний	бінарний	фінансовий	RDNA	національний	оцінка програм підтримки	включено гуманітарні та інституційні програми

№	Група показників	Конкретний індикатор	Кількісне значення	Одиниця виміру	Тип показника	Джерело формування	Рівень застосування	Управлінське призначення	Аналітична інтерпретація
9	Фінансове планування	Рівень деталізації витрат	середній	якісна оцінка	аналітичний	RDNA	національний	планування бюджету	деталізація недостатня для реалізації
10	Фінансове планування	Рівень точності оцінок	високий	якісна оцінка	аналітичний	міжнародні оцінки	національний	прогнозування	оцінки вважаються достовірними
11	Проєктне управління	Наявність дорожніх карт	відсутні	бінарний	управлінський	державна система	національний	координація відбудови	бракує чіткої реалізаційної логіки
12	Проєктне управління	Системність управління	низька	якісна оцінка	управлінський	національна практика	національний	організація процесу	відсутня інтегрована модель
13	Проєктне управління	Використання PMBoK	рекомендовано	бінарний	методичний	наукове обґрунтування	національний	структуризація проєктів	запропоновано класичну проєктну модель
14	Проєктне управління	Використання Agile	рекомендовано	бінарний	методичний	наукове обґрунтування	національний	адаптивність управління	передбачає гнучке коригування
15	Проєктне управління	Етапність проєктів	чітко визначена	якісна оцінка	структурний	PMBoK	національний	управління життєвим циклом	формалізовано стадії реалізації
16	Проєктне управління	Розподіл відповідальності	структуро-ваний	якісна оцінка	організаційний	PMBoK	національний	координація суб’єктів	забезпечується прозорість ролей
17	Проєктне управління	Прозорість бюджету	висока	якісна оцінка	фінансовий	PMBoK	національний	контроль витрат	передбачено чіткий бюджетний контроль
18	Інституційна взаємодія	Участь держави	домінуюча	якісна оцінка	інституційний	уряд	національний	стратегічне управління	держава визначає пріоритети
19	Інституційна взаємодія	Участь громад	наявна	якісна оцінка	інституційний	місцеві органи	регіональний	локальне управління	громади включені в процес
20	Інституційна взаємодія	Участь бізнесу	обмежена	якісна оцінка	інституційний	приватний сектор	національний	інвестування	потребує розширення

№	Група показників	Конкретний індикатор	Кількісне значення	Одиниця виміру	Тип показника	Джерело формування	Рівень застосування	Управлінське призначення	Аналітична інтерпретація
21	Інституційна взаємодія	Механізм ДПП	запропоно-ваний	бінарний	інституційний	наукова модель	національний	фінансування проєктів	визначено потенціал партнерства
22	Інституційна взаємодія	Рівень інтеграції	середній	якісна оцінка	системний	національна практика	національний	узгодження дій	інтеграція недостатньо розвинена
23	Аналітичне забезпечення	Наявність аналітичних моделей	часткова	якісна оцінка	аналітичний	RDNA	національний	підтримка рішень	відсутня повна інтеграція
24	Аналітичне забезпечення	Використання сценарного аналізу	обмежене	якісна оцінка	аналітичний	наукові підходи	національний	прогнозування	потребує розширення
25	Аналітичне забезпечення	Оцінка ризиків	часткова	якісна оцінка	аналітичний	національна практика	національний	управління ризиками	не має системного характеру
26	Цифрове забезпечення	Єдина цифрова платформа	відсутня	бінарний	цифровий	національна система	національний	координація	необхідна інтеграція даних
27	Цифрове забезпечення	Інтеграція даних	фрагментована	якісна оцінка	цифровий	державні системи	національний	аналітика	дані не об’єднані
28	Цифрове забезпечення	Моніторинг у реальному часі	відсутній	бінарний	цифровий	національна система	національний	оперативне управління	потрібне впровадження
29	Стратегічне планування	Наявність стратегій відбудови	обмежена	якісна оцінка	стратегічний	уряд	національний	планування	стратегічні документи не систематизовані
30	Стратегічне планування	Узгодженість стратегій	низька	якісна оцінка	стратегічний	державні органи	національний	координація	відсутня єдина логіка
31	Стратегічне планування	Пріоритизація відбудови	часткова	якісна оцінка	стратегічний	державна практика	національний	розподіл ресурсів	критерії не формалізовані
32	Стратегічне планування	Орієнтація на стійкість	декларована	якісна оцінка	стратегічний	політичні документи	національний	довгостроковий розвиток	потребує конкретизації

№	Група показників	Конкретний індикатор	Кількісне значення	Одиниця виміру	Тип показника	Джерело формування	Рівень застосування	Управлінське призначення	Аналітична інтерпретація
33	Міжнародна підтримка	Участь міжнародних організацій	висока	якісна оцінка	інституційний	Світовий банк, ЄС	міжнародний	фінансування і експертиза	критично важлива для відбудови
34	Міжнародна підтримка	Координація донорів	середня	якісна оцінка	інституційний	міжнародні партнери	міжнародний	узгодження ресурсів	потребує централізації
35	Міжнародна підтримка	Обсяг експертної підтримки	значний	якісна оцінка	інституційний	міжнародні організації	міжнародний	аналітика	забезпечує методологічну основу
36	Загальна оцінка	Рівень готовності системи відбудови	середній	якісна оцінка	інтегральний	узагальнення	національний	оцінка спроможності	система потребує структурної модернізації

ДОДАТОК Д

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у фахових виданнях індексованих у міжнародній науково-метричній базі Scopus/Web of science:

1. Magomedov A., Ivanov A., Pron L., Trostianska K., Forkun I. Administrative oversight of critical infrastructure and social security protection. AD ALTA: Journal Of Interdisciplinary Research (14/01-XLII.) 2024, p. 16-20. URL: https://doi.org/10.5281/zenodo.11816980.

(Особистий внесок здобувача: обґрунтовано концептуальні засади публічного управління у сфері захисту критичної інфраструктури та соціальної безпеки).

2. Bohun V., Magomedov A., Hromyka O., Kovshun N., Fedorchuk Y. Assessing the Impact of Infrastructure Damage on National Investment Attractiveness During Martial Law. Pakistan Journal of Life and Social Sciences, 2024, 22(2), p.100379-100385. DOI: 10.57239/PJLSS-2024-22.2.00784.

(Особистий внесок здобувача: здійснено концептуалізацію дослідження впливу руйнування інфраструктури на інвестиційну привабливість України в умовах воєнного стану; сформовано методологічні підходи до оцінювання наслідків пошкодження критичної інфраструктури; проведено систематизацію та опрацювання даних, а також підготовлено й доопрацьовано текст статті).

3. Polovenko V., Magomedov A., Kravtsev O., Krasnostanova N., Kryzhanovskyi S. Regulatory and Institutional Frameworks for Ensuring Financial Security in Ukraine's Energy Sector: Challenges and Future Outlook. Grassroots Journal of Natural Resources, 2024, 7(3): s313-s330. DOI: https://doi.org/10.33002/nr2581.6853.0703ukr16.

(Особистий внесок здобувача: сформовано методологічний підхід дослідження, проведено порівняльний аналіз регуляторних та інституційних засад енергетичної безпеки).

Статті у фахових виданнях України категорії Б:

4. Магомедов А. Стратегічні документи і заходи повоєнної відбудови України. Публічне управління: концепції, парадигма, розвиток, удосконалення. 2023. № 4. С. 61–75. DOI: https://doi.org/10.31470/2786-6246-2023-4-61-75.

5. Магомедов А.О. Зарубіжний досвід економічного відновлення після війни. Наукові перспективи, 2023, №11(41). С.252-263. DOI: https://doi.org/10.52058/2708-7530-2023-11(41)-252-265.

6. Магомедов А. О. Державне регулювання повоєнного відновлення економіки. Електронне наукове видання "Публічне адміністрування та національна безпека". 2023. №10. DOI: https://doi.org/10.25313/2617-572X-2023-10-9397.

7. Магомедов А. О. Фінансове забезпечення повоєнної відбудови та відновлення економіки: теоретичні засади. Публічне управління: концепції, парадигма, розвиток, удосконалення, 2023, №5. С.60-76. DOI: https://doi.org/10.31470/2786-6246-2023-5-60-76.

8. Магомедов А. О. Аналіз втрат та руйнувань інфраструктури України, що підлягає відновленню. Таврійський науковий вісник. Серія: Публічне управління та адміністрування. 2023. № 6. С. 62-72. DOI: https://doi.org/10.32782/tnv-pub.2023.6.9.

9. Магомедов А. О. Оцінка економічних наслідків війни та втрат економіки України. Актуальні питання у сучасній науці. 2024. №1(19). С. 191-206. DOI: https://doi.org/10.52058/2786-6300-2024-1(19)-191-206.

10. Магомедов А. О. Механізм публічного управління розвитком об’єктів критичної інфраструктури: законодавчі, організаційні та управлінські виміри. Державне управління: удосконалення та розвиток. 2024. № 5. DOI: http://doi.org/10.32702/2307-2156.2024.5.12.

11. Магомедов А. О. Відбудова об’єктів критичної інфраструктури України після війни: стратегія та перспективи. Економіка, фінанси, управління: Актуальні питання науки та практичної діяльності. 2024. № 1. С. 100-116. DOI: 10.37128/2411-4413-2024-1-7.

12. Магомедов А. О. Публічне управління процесами трансформації критичної інфраструктури в країнах ЄС. Успіхи і досягнення. 2024. № 6. С. 520-537. DOI: https://doi.org/10.52058/3041-1254-2024-6(6)-520-537.

13. Магомедов А. О. Особливості публічного управління об’єктами критичної інфраструктури. Наукові перспективи. 2024. No 7(49). С. 412-427. DOI: https://doi.org/10.52058/2708-7530-2024-7(49)-412-427.

14. Магомедов А. О. Інновації в публічному управлінні сферою критичної інфраструктури. Публічне адміністрування та національна безпека. 2024. № 7. DOI: https://doi.org/10.25313/2617-572X-2024-7-10106.

15. Магомедов А. О. Ризики та загрози для об'єктів критичної інфраструктури та шляхи їх подолання. Інвестиції: практика та досвід. 2024. № 15. С. 216-221. DOI: 10.32702/2306-6814.2024.15.216.

16. Магомедов А. О. Стійкість об'єктів критичної інфраструктури в контексті публічного управління. Modern Economics. 2024. № 46. С.69-76. DOI: https://doi.org/10.31521/modecon.V46(2024)-10.

17. Магомедов А. О. Стратегічне управління трансформацією об’єктів критичної інфраструктури: організаційні та управлінські виклики та можливості. Публічне управління і адміністрування в Україні. 2024. № 41. С. 84-89. DOI: https://doi.org/10.32782/ pma2663-5240-2024.41.11.

18. Магомедов А. О. Стратегічне планування повоєнної відбудови критичної інфраструкури України: еволюція підходів, фінансові розриви та цифрові інструменти. Філософія та управління, 2026, (3(19). DOI: https://doi.org/10.70651/3041-248X/2026.3.21.

19. Магомедов А. О. Стан, проблеми публічного управління та стратегічні пріоритети відновлення критичної інфраструктури України (2022–2025). Філософія та управління, 2026, (4(20). DOI: https://doi.org/10.70651/3041-248X/2026.4.07.

20. Магомедов А. О. Корпоратизація державних підприємств критичної інфраструктури України: інституційні проблеми та міжнародні уроки. Публічне

управління і політика, 2026, (4(20). DOI: https://doi.org/10.70651/3041-2498/2026.4.20.

21. Magomedov A. Legal and regulatory framework of public management of the security and transformation of critical infrastructure facilities in modern conditions. Public Management and Policy. 2026. № 6(22). DOI: https://doi.org/10.70651/3041-2498/2026.6.03.

22. Magomedov A. Innovative public management tools for ensuring the resilience and transformation of critical infrastructure facilities amidst modern challenges. Philosophy and Governance. 2026. № 6(22). DOI: https://doi.org/10.70651/3041-248X/2026.6.03.

Публікації, що засвідчують апробацію результатів дисертації:

23. Магомедов А. О. Вплив трансформації об'єктів критичної інфраструктури на економіку та соціальні процеси. II науково-практичній конференції "Комплексний підхід до модернізації міждисциплінарних наукових досліджень", м. Дніпро, 24–25 травня 2024 року. URL: https://molodyivchenyi.ua/omp/index.php/conference/catalog/view/86/1420/2954-1.

24. Магомедов А. О. Порівняльний аналіз стратегій та політик ЄС та інших країн у сфері публічного управління об’єктами критичної інфраструктури. Міжнародна наукова конференція «Сучасні тенденції наукових досліджень у світі» 30–31 травня 2024 року м. Рига, Латвійська Республіка. URL: http://www.baltijapublishing.lv/omp/index.php/bp/catalog/view/478/12795/26738-1.

25. Магомедов А. О. Трансформація об'єктів критичної інфраструктури у системі публічного управління. VI International Scientific and Theoretical Conference «Current issues of science, prospects and challenges» 17.05, Сідней, Австралія. 2024. URL: https://previous.scientia.report/index.php/archive/issue/view/17.05.2024.

26. Магомедов А. О. Роль інформаційних технологій у підвищенні ефективності публічного управління трансформацією об'єктів критичної інфраструктури. І Всеукраїнській науково-практичній конференції за

міжнародною участю “Публічне управління та адміністрування в Україні: євроінтеграційний поступ» 31 травня 2024. URL: https://nung.edu.ua/sites/default/files/2024-07/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA_%D1%82%D0%B5%D0%B7_%D0%86%D0%A4%D0%9D%D0%A2%D0%A3%D0%9D%D0%93_2024.pdf.

27. Магомедов А. О. Інноваційні підходи до забезпечення безпеки та стійкості об'єктів критичної інфраструктури. III Міжнародної наукової конференції Наукові орієнтири: теорія та практика досліджень, 17 травня 2024, Ужгород, Україна. 2024. С. 54-56. URL: https://archive.mcnd.org.ua/index.php/conference-proceeding/issue/view/17.05.2024/65.