DOI https://doi.org/10.30525/978-9934-26-446-7-47

COMPARATIVE ANALYSIS OF STRATEGIES AND POLICIES OF THE EU AND OTHER COUNTRIES IN THE SPHERE OF PUBLIC MANAGEMENT OF CRITICAL INFRASTRUCTURE FACILITIES

ПОРІВНЯЛЬНИЙ АНАЛІЗ СТРАТЕГІЙ ТА ПОЛІТИК ЄС ТА ІНШИХ КРАЇН У СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ ОБ'ЄКТАМИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Magomedov A. O.
Ph.D. in History,
Applicant of the Department of History and Culture of Ukraine
Hryhorii Skovoroda University in Pereiaslav
Pereiaslav, Ukraine

Магомедов А. О.
кандидат історичних наук,
здобувач кафедри історії та культури України
Університет Григорія Сковороди в Переяславі
м. Переяслав, Україна

У контексті Європейського Союзу (ЄС), де існує велика різноманітність систем управління держав-членів з різними рівнями розвитку та управлінських практик, питання ефективного управління об'єктами критичної інфраструктури набуває особливої актуальності. Водночас, з огляду на геополітичні виклики та загрози, які стають все більш складними і глобальними, міжнародна співпраця та порівняльний аналіз стратегій та політик стає необхідним елементом забезпечення стабільності та безпеки. Незважаючи на існуючі дослідження у сфері управління критичною інфраструктурою, важливим завданням є вивчення та аналіз досвіду різних країн з метою виявлення кращих практик та можливостей для вдосконалення стратегій управління. Такий порівняльний аналіз дозволить ідентифікувати ключові виклики, з якими стикаються різні країни, а також визначити можливості для впровадження ефективних інструментів та підходів [1–2].

У цьому контексті, дослідження має на меті провести порівняльний аналіз стратегій та політик ЄС та інших країн у сфері публічного управління об'єктами критичної інфраструктури, спрямоване на виявлення сучасних тенденцій, проблем та можливостей для подальшого розвитку та вдосконалення управління критичною інфраструктурою з метою забезпечення стійкості та безпеки як в межах окремих країн, так і на міжнародному рівні [3].

Загальний аналіз підходів до стратегій та політик Європейського Союзу та інших країн у сфері публічного управління об'єктами

критичної інфраструктури відображає різноманітність та специфічність підходів, які використовуються для забезпечення стійкості та безпеки, зокрема [4–5]:

1. Інтегрований підхід до управління критичною інфраструктурою, що передбачає координацію зусиль між різними секторами та рівнями уряду, а також партнерство з приватним сектором та громадськістю.

2. Стандартизація та регулювання для забезпечення безпеки критичної інфраструктури, включаючи вимоги щодо кібербезпеки, захисту від терористичних загроз, та інші вимоги.

3. Ризик-орієнтований підхід, що зосереджується на оцінці ризиків та розробці стратегій з управління ризиками, щоб ідентифікувати, оцінювати та зменшувати загрози критичній інфраструктурі.

4. Міжнародне співробітництво у рамках міжнародних організацій та платформ для обміну інформацією та кращих практик.

5. Інновації та технології, такі як штучний інтелект, блокчейн-платформ, за рахунок яких країни намагаються покращити ефективність та надійність своїх систем управління критичною інфраструктурою.

6. Гнучкість та адаптивність стратегії та політики для ефективності в умовах трансформаційного суспільства.

У таблиці 1 представлено аналіз стратегій та політик ЄС та інших країн у сфері публічного управління об'єктами критичної інфраструктури.

Таблиця 1

Аналіз міжнародного досвіду публічного управління об'єктами критичної інфраструктури

Країна	Стратегії	Переваги стратегії	Недоліки стратегії
1	2	3	4
США	Національна стратегія кібербезпеки National Cybersecurity Strategy https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf	- Широке охоплення різних секторів критичної інфраструктури. - Зосередження на кібербезпеці та кібернетичних загрозах.	- Нерівномірність заходів захисту між різними секторами. - Потреба в постійному оновленні стратегії відповідно до нових загроз.
Канада	Національна стратегія кібербезпеки National Cybersecurity Strategy https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx	- Інтегрований підхід до управління різними секторами. - Співпраця між урядом, приватним сектором та громадськістю.	- Відсутність однозначного визначення критичної інфраструктури. - Необхідність удосконалення координації між різними секторами.

Продовження таблиці 1

1	2	3	4
Японія	Стратегія кібербезпеки Cybersecurity Strategy https://www.nisc.go.jp/eng/pdf/cs-strategy-en-pamphlet.pdf	- Висока рівень технологічного розвитку та інновацій. - Зосередження на попередженні та мінімізації наслідків кризових ситуацій.	- Високі витрати на реалізацію заходів захисту. - Потреба в постійному оновленні стратегії відповідно до нових технологій.
Південна Корея	Національна стратегія кібербезпеки National Cybersecurity Strategy https://www.nknews.org/2023/06/seouls-new-national-security-strategy-spotlights-main-enemy-north-korea/	- Широке використання технологій та інновацій у сфері кібербезпеки. - Співпраця з іншими країнами та міжнародними організаціями.	- Недостатня увага до питань кібербезпеки у некритичних секторах. - Відсутність чіткої стратегії з врахуванням геополітичних аспектів.
Німеччина	Національна стратегія кібербезпеки National Cybersecurity Strategy https://www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-node.html	- Великий обсяг інвестицій у кібербезпеку та захист критичної інфраструктури. - Ефективне співробітництво з приватним сектором та активна участь громадськості.	- Потреба удосконалення законодавства та регулювання в сфері кібербезпеки. - Недостатня координація між різними органами влади та секторами.
Франція	Національна стратегія кібербезпеки National Cybersecurity Strategy, https://cyberwiser.eu/france-fr	- Акцент на протидію кібератакам та терористичним загрозам. - Розробка та впровадження інноваційних технологій у сфері кібербезпеки.	- Потреба в підвищенні свідомості та підтримці з боку громадськості. - Необхідність удосконалення міжсекторного співробітництва.
Італія	Національна стратегія кібербезпеки, National Cybersecurity Strategy 2022–2026 https://www.acn.gov.it/portale/en/strategia-nazionale-di-cybersicurezza	- Співпраця з іншими країнами ЄС та міжнародними організаціями. - Зосередження на реалізації конкретних заходів захисту.	- Недостатня фінансова підтримка програм кібербезпеки. - Відсутність єдиної координуючої структури з управління кризовими ситуаціями.

** Джерело: розроблено автором на основі аналізу [4–6].*

Доцільно представити результати опитування жителів країн ЄС, яке проводилося у рамках дослідження [5] стосовно запитів до надання послуг та функціонування об'єктів критичної інфраструктури. Результати представлені на рис. 1.

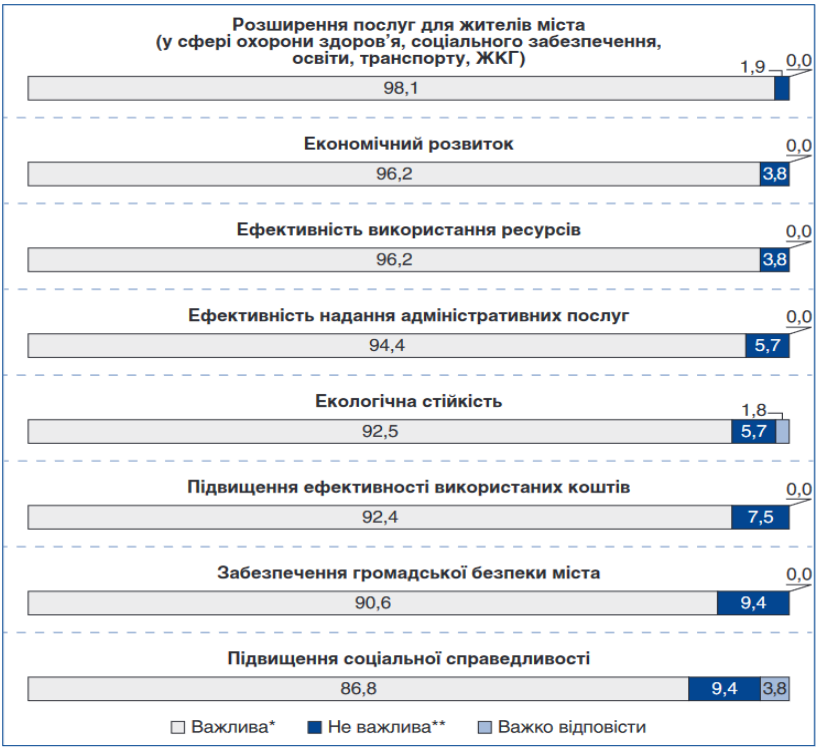

Рис. 1. Результати опитування жителів країн ЄС стосовно запитів до надання послуг та функціонування об'єктів критичної інфраструктури [5]

За результатами дослідження виявлено, що найбільшу вагу жителі країн ЄС віддають розширенню послуг саме критичної інфраструктури (98,1%), а такі параметри як екологічна стійкість, ефективність використання ресурсів та економічний розвиток безпосередньо пов'язані із діяльністю та інноваційним розвитком критичної інфраструктури, що визначає провідну роль розвитку сталості та підвищення ефективності реалізації стратегічної політики ЄС в сфері публічного управління критичною інфраструктурою.

Загальний аналіз показує, що розвинені країни використовують різноманітні підходи та стратегії для управління критичною інфраструктурою, проте існує потреба у подальшому обміні досвідом та співпраці для досягнення більшої ефективності та стійкості національних та міжнародних систем управління.

Література:

1. Богдан Б. В. Актуальні питання нормативно-правового регулювання захисту критичної інфраструктури в умовах воєнного стану в Україні. *Проблеми сучасних трансформацій. Серія : Право, публічне управління та адміністрування*. 2022. № 6. URL: https://doi.org/10.54929/2786-5746-2022-6-01-09

2. Кузьменко О. В., Доценко Т. В., Боженко В. В., Світлична А. О. Закономірності здійснення кібератак в країнах ЄС на основі використання асоціативних правил. *Вісник Сумського державного університету. Серія : Економіка*. 2021. № 1. С. 95–103.

3. Дрейс Ю.О. Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави. *Захист інформації*. 2017. Т. 19, № 3. С. 214–222.

4. A Short Guide to the EU. Luxembourg: Publications Office of the European Union, 2023. 32 p. URL: https://op.europa.eu/en/publication-detail/-/publication/9bee2406-dff5-11ed-a05c-01aa75ed71a1/language-en

5. Garcia-Perez A., Sallos M. P. and Tiwasing P. Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective. *Journal of Intellectual Capital*. 2023. Vol. 24 No. 2. Pp. 465–486. https://doi.org/10.1108/JIC-06-2021-0166

6. Espada R., Apan A. and McDougall K. Vulnerability assessment of urban community and critical infrastructures for integrated flood risk management and climate adaptation strategies. *International Journal of Disaster Resilience in the Built Environment*. 2017. Vol. 8. No. 4. Pp. 375–411. https://doi.org/10.1108/IJDRBE-03-2015-0010