УДК *65.012.5:351.74* **DOI***: https://doi.org/10.31521/modecon.V46(2024)-10*

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

ORCID ID: *0000-0001-5919-2340*
e-mail: *magomedovandriy@gmail.com*

Стійкість об'єктів критичної інфраструктури в контексті публічного управління

Анотація. *Захист критично важливих функцій та функціонування критичної інфраструктури в Україні є одним з найважливіших пріоритетів безпеки для держави. Досвід України у забезпеченні енергопостачання споживачів під час війни та руйнування об'єктів критичної інфраструктури свідчить про різні виклики, з якими стикаються в умовах повномасштабного військового вторгнення та ракетних атак. Для забезпечення стійкості критичної інфраструктури та подальшого розвитку необхідні узгоджені цілі та скоординовані зусилля всіх зацікавлених сторін. Розуміння організаційно-управлінських аспектів цієї проблематики важливо для розвитку ефективних стратегій управління та запобігання можливим загрозам.*

Метою даного дослідження є аналіз організаційно-управлінських аспектів, які впливають на стійкість об'єктів критичної інфраструктури в контексті публічного управління, з метою виявлення можливих шляхів покращення систем управління та забезпечення безпеки. Методи дослідження включають аналіз літератури, вивчення вітчизняного та зарубіжного досвіду, моделювання рекомендацій щодо захисту критичної інфраструктури в умовах повномасштабної військової агресії. Проведено аналіз основних принципів публічного управління в контексті забезпечення стійкості критичної інфраструктури, ідентифікацію загроз та вразливостей, а також розроблено пропозиції щодо вдосконалення систем управління ризиками та стратегій забезпечення безпеки.

На основі результатів дослідження були сформульовані висновки та рекомендації щодо практичного впровадження поліпшених стратегій управління критичною інфраструктурою. Рекомендації включають розробку і впровадження ефективних механізмів моніторингу та реагування на потенційні загрози, сприяння співпраці між сектором державного управління та приватним сектором, а також підвищення обізнаності та підготовки персоналу, що відповідає за управління критичною інфраструктурою.

Ключові слова: *організаційно-управлінські аспекти; стійкість; об'єкти критичної інфраструктури; публічне управління; загрози; вразливості; управління ризиками; стратегії; ефективність; безпека.*

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

Sustainability of Critical Infrastructure Facilities in the Context of Public Administration

Introduction. *Protection of critical functions and functioning of critical infrastructure in Ukraine is one of the most important security priorities for the state. Ukraine's experience in ensuring energy supply to consumers during wartime and the destruction of critical infrastructure facilities testifies to the various challenges faced in conditions of full-scale military invasion and missile attacks. To ensure the sustainability of critical infrastructure and its continued development, agreed goals and coordinated efforts of all stakeholders are necessary. Understanding the organizational and management aspects of this problem is important for the development of effective management strategies and prevention of possible threats.*

Purpose. *The purpose of this study is to analyze the organizational and management aspects that affect the stability of critical infrastructure objects in the context of public administration, with the aim of identifying possible ways to improve management systems and ensure security. The object of research is the management system of critical infrastructure objects, and the subject is the organizational and management aspects of ensuring their stability. Research methods include literature analysis, study of domestic and foreign experience, modeling of recommendations for the protection of critical infrastructure in conditions of full-scale military aggression. The author analyzed the main principles of public management in the context of ensuring the stability of critical infrastructure, identified threats and vulnerabilities, and also developed proposals for improving risk management systems and security strategies.*

Results. *Based on the results of the study, conclusions and recommendations regarding the practical implementation of improved critical infrastructure management strategies were formulated. Recommendations include the development and implementation of effective mechanisms for monitoring and responding to potential threats, promoting cooperation between the public administration sector and the private sector, and increasing awareness and training of personnel responsible for managing critical infrastructure.*

Conclusions. *It was concluded that critical infrastructure plays a key role in ensuring the functioning of the state and the economy. Analysis of risk management tools and methods aimed at ensuring the stability of critical infrastructure objects indicates the need for constant improvement of security systems and response to crisis situations.*

[1]**Стаття надійшла до редакції***: 06.07.2024*
Received*: 06 July 2024*

Keywords: *organizational and management aspects; sustainability; critical infrastructure objects; public administration; threats; vulnerabilities; risk management; strategies; efficiency; security.*

JEL Classification: *E 69; Q20; Q30.*

Постановка проблеми. Відповідно Закону України «Про критичну інфраструктуру», критичні послуги – це послуги, що надаються органами державної влади, місцевого самоврядування, установами, підприємствами та організаціями незалежно від форми власності, невиконання, відмова в наданні, переривання або зупинення яких має значний негативний вплив на національну безпеку [1]. Відповідно до законодавства «безпека критичної інфраструктури – стан захищеності критичної інфраструктури, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури» [1]. Для України викликом стали ракетні атаки на об'єкти критичної інфраструктури, що завдали суттєвих руйнувань та викликів для економіки як наслідок повномасштабної російської агресії проти України. Однак, проблема не обмежується самими інцидентами, але й залежить від ефективності системи управління, що контролює та реагує на ці загрози.

У результаті військових дій та ракетних обстрілів критичної інфраструктури України російськими агресорами загальні збитки станом на початок 2024 року скали 143,8 млрд дол. США житловій та нежитловій нерухомості (за вартістю заміщення). Найбільша частка у загальному обсязі прямих втрат припадає на житлові будівлі, що складає 37,3% або 53,6 млрд дол. США, та на інфраструктуру, яка становить 25,2% або 36,2 млрд дол. США. Втрати активів бізнесу наразі досягли рівня у 11,3 млрд дол. США і продовжують зростати. Додатково, ще 8,7 млрд дол. США припадають на прямі втрати у сільському господарстві через наслідки війни [2]. Описані проблеми підкреслюють необхідність удосконалення стратегій захисту критичної інфраструктури від сучасних загроз та пошуку шляхів захисту від ракетних обстрілів з боку країни-агресорки, що використовує руйнування критичної інфраструктури як акти тероризму та засоби економічного та політичного впливу. Гіпотеза дослідження полягає у припущенні, що ефективне управління та координація між різними секторами, включаючи державний та приватний, може значно зменшити вразливість критичної інфраструктури перед сучасними загрозами. Враховуючи велику кількість зацікавлених сторін та складність інфраструктурних систем, доцільно дослідити організаційно-управлінські аспекти забезпечення стійкості об'єктів критичної інфраструктури в контексті публічного управління.

Аналіз останніх досліджень і публікацій. Актуальність теми дослідження визначається увагою авторів до розробки проблематики, зокрема: А. Невольніченко, С. Чумаченко, А. Михайлова, О. Пиріков, Р. Мурасов, S. Onyshchenko, A. Hlushko, D. Melnyk, D. Lallemant, R. Bicksler, K. Barns, P. Hamel, R .Soden, S. Bannister, G. Ampratwum, V. Tam, R. Osei-Kyei, L. Almeida, R. Nyqvist, A. Peltokorpi, O. Seppänen, T. Andersen, J. Sax, A. Wasgen M. T. Adu Gyamfi, C. Aigbavboa, W. Thwala, M. Fitz-Oliveira [3-12] та інші автори.

Формулювання цілей дослідження. Метою статті є вивчення організаційно-управлінських аспектів, що впливають на стійкість об'єктів критичної інфраструктури в контексті публічного управління.

Завдання дослідження:

1. Аналізувати концепції критичної інфраструктури та її роль у сучасному суспільстві.
2. Вивчити основні загрози та вразливості, що ставлять під загрозу стійкість об'єктів критичної інфраструктури.
3. Розглянути принципи публічного управління в контексті забезпечення стійкості критичної інфраструктури.
4. Проаналізувати інструменти та методи управління ризиками, які можуть бути застосовані для забезпечення стійкості об'єктів критичної інфраструктури.
5. Висвітлити передовий досвід та кращі практики з публічного управління критичною інфраструктурою в різних країнах.
6. Сформулювати рекомендації щодо поліпшення систем управління та забезпечення безпеки об'єктів критичної інфраструктури в умовах сучасних загроз та викликів.

Виклад основного матеріалу дослідження. Критична інфраструктура стала ключовою у контексті забезпечення економічної, фінансової безпеки та стійкості. Підвищення стійкості безпеки до загроз для критичної інфраструктури регулюються низкою механізмів та заходів із забезпечення безпеки, зокрема планами захисту функціонування, операційних процесів, інформації та планами взаємодії суб'єктів, що задіяні при провадженні операцій із забезпечення безпеки в умовах повномасштабного військового вторгнення. Такі плани в першу чергу спрямовані на забезпечення безпеки конкретних об'єктів критичної інфраструктури, зокрема, енергетичної, що зазнає суттєвих руйнувань та є основним об'єктом російського терору. Питання стійкості функцій критичної інфраструктури виходить за межі відповідальності та компетенції окремих її операторів і потребує залучення ширшого кола стейкхолдерів: органи публічної влади, місцева влада, генеральний штаб, профільні експерти. Законодавство України

встановлює низку конкретних завдань для забезпечення сталості таких функцій, зокрема, галузеві органи влади розробляють і затверджують плани взаємодії та підтримання критично важливих функцій у разі порушення роботи об'єктів критичної інфраструктури [1-2]. Проте, варто зазначити, що органи публічного управління як в Україні, так і в європейських країнах не стикалися з викликами до функціонування критичної інфраструктури у таких масштабах з часів Другої світової війни [2].

Організаційно процеси управління ризиками для критичної інфраструктури сформовані шляхом розробки обласними (військовими) адміністраціями програм підвищення стійкості громад до кризових ситуацій, та забезпечення виконання критично важливих функцій об'єктами критичної інфраструктури. Програми відновлення є формальними рамковими угодами між усіма зацікавленими сторонами, залученими до процесу [1] забезпечення функціонування критичної інфраструктури.

Стійкість критичної інфраструктури – це такий її стан, за якого забезпечується її функціонування у штатному режимі, адаптація до мінливих умов зовнішнього середовища, протистояння та швидке відновлення роботи після негативного різного виду загроз [13].

Стійкість об'єктів критичної інфраструктури залежить від їх здатності відновлюватися після негативного впливу або руйнування, тому вивчення основних небезпек та вразливостей критичної інфраструктури дозволяє розробляти ефективні заходи захисту та плани надзвичайних ситуацій, спрямовані на зменшення ризиків та забезпечення стійкості об'єктів у випадку негативних подій (див. табл. 1.).

За даними ДСНС у 2023 році в Україні відбулося 109 надзвичайних ситуацій (для порівняння 66 у 2022 році), з яких – 60 природного та 48 техногенного характеру, зокрема за масштабами: 4 державного рівня, 5 – регіонального рівня, 54 місцевого та 46 об'єктового рівня. Серед надзвичайних ситуацій державного рівня воєнного характеру власне саме руйнування та пошкодження критичної інфраструктури: з початку 2022 року пошкоджено, зруйновано понад 214 тисяч її об'єктів (8 тис. 642 – це об'єкти життєзабезпечення, 1 тис. 592 об'єктів транспортної інфраструктури, 3 тис. 679 освітніх закладів та 1 тис. 569 медичних закладів тощо) [17].

Таблиця 1 **Основні загрози для критичної інфраструктури, їх наслідки та можливі заходи захисту у випадку настання негативних подій**

Основні загрози	Наслідки	Заходи захисту
Ракетні атаки	Руйнування інфраструктури зі значними збитками та неможливістю швидкого відновлення	Розробка програм та стратегій безпеки об'єктів критичної інфраструктури як елементу системи державної безпеки, розробка управлінських механізмів швидкого реагування на наслідки пошкоджень та їх оперативного усунення
Природні катастрофи [2]	Пошкодження інфраструктури, перебої в енергопостачанні, затоплення	Розробка планів евакуації, підвищення стандартів будівельного проєктування, створення систем моніторингу небезпек
Терористичні акти [3]	Фізичне знищення або пошкодження інфраструктури, застосування зброї масового знищення	Запровадження підвищених заходів безпеки, контроль над доступом до об'єктів, співпраця з правоохоронними органами
Техногенні аварії [4]	Викиди небезпечних речовин, пожежі, вибухи	Проведення аудитів безпеки, розробка планів екстреного реагування, вдосконалення систем виявлення та попередження аварій
Соціальні конфлікти [5]	Блокування доступу до об'єктів, вандалізм, загрози для персоналу	Забезпечення безпеки працівників, встановлення систем внутрішньої безпеки, спілкування з громадськістю та консультування
Економічні кризи [6]	Обмеження фінансування проєктів, зниження рівня безпеки інфраструктури	Розробка програм підтримки для забезпечення фінансової стійкості, перегляд бюджетних пріоритетів, посилення моніторингу витрат
Технологічні вади [7]	Відмови обладнання, витоки даних, порушення послуг	Проведення технічного обслуговування та аудитів, створення резервних каналів зв'язку, розробка планів відновлення після вади

Джерело: сформовано автором на основі [1, 2, 3, 4, 5, 6, 7]

В Україні розроблені практичні рекомендації щодо забезпечення стійкості критичної інфраструктури для забезпечення безперебійного надання населенню критично важливих функцій за участі територіальних

громад. Рекомендації, розроблені з врахуванням досвіду ЄС за такими напрямками: підвищення її готовності до кризових ситуацій, підвищення спроможності громад та операторів інфраструктури до реагування на загрози. У громадах активно впроваджуються надані ЄС рекомендації [13]. Зважаючи на наявність досвіду європейських держав в управлінні критичною інфраструктурою, варто оглянути їх досвід до підтримки стійкості та стабільності.

У середині 2000-х років в країнах ОЕСР почали розроблятися та впроваджуватися комплексні багатогалузеві державні політики для підтримки стійкості або захисту критичної інфраструктури. За опитуванням ОЕСР з 37 країн 90% зазначили, що визначили певні сектори інфраструктури критичними для управління ризиками у 2018 році. У більшості країн використано секторальний підхід в управлінні критичною інфраструктурою, створено національну систему інвентаризації активів за методикою оцінки критичності та наявних ризиків, створені національні програми посилення їх стійкості до потрясінь. Програми побудовані на механізмі управлінні, що передбачає обмін даними та інформацією між урядовими структурами та операторами критичної інфраструктури. Такий механізм також містить комбінацію політичних інструментів регулювання та стимулювання в цілях підтримки досягнення цілей стійкості критичної інфраструктури [14].

За результатами дослідження ОЕСР 2020 року у 2019 році 8 країн здійснювали секторальне регулювання в цілях стимулювання операторів критичної інфраструктури до підвищення та забезпечення її стійкості (серед країн Європи – це Швеція, Норвегія, Фінляндія, Естонія, Німеччина). У деяких країн законодавчо передбачені фінансові штрафи за збої в обслуговуванні критичної інфраструктури (серед європейських країн такі стимули закріплені у Норвегії, Швеції, Фінляндії, Естонії) [16].

У США передбачено надання грантів в межах чинних грантових програм підтримки стійкості критичної інфраструктури. У 2024 році адміністрація Дж. Байдена оголосила про надання грантів за програмою «Відновлення американської інфраструктури за допомогою сталого розвитку та справедливості» (RAISE) саме на підтримку стійкості інфраструктури на суму 1,8 млрд дол. США, які будуть спрямовані на посилення безпеки її секторів в межах всієї країни: від безпеки дорожнього руху до оновлення транспорту, будівництва доріг. За програмою передбачено реалізація 148 проєктів в громадах різного розміру. Водночас у більшості країн ОЕСР не передбачено жодних стимулів підтримки стійкості критичної інфраструктури, серед яких Словаччина, Польща, Люксембург, Франція, Іспанія, Австрія, Австралія та інші [15].

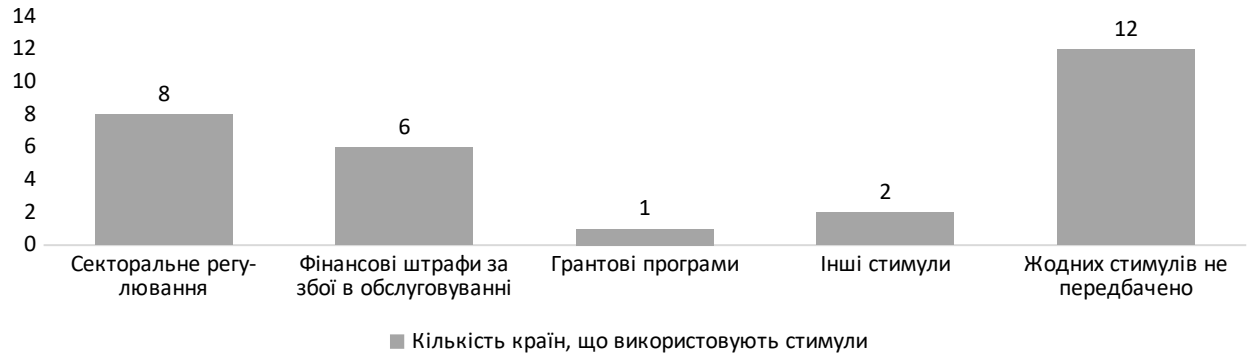

Рисунок 1 – **Державні стимули для операторів критичної інфраструктури для заохочення інвестицій в стійкість критичної інфраструктури, 2019 рік**

Джерело: сформовано автором на основі [16]

Розгляд принципів публічного управління в контексті забезпечення стійкості критичної інфраструктури є важливим аспектом ефективного функціонування держави. Публічне управління визначається як система управлінських методів, процедур та інструментів, які використовуються урядом або іншими органами влади для досягнення стратегічних цілей та забезпечення інтересів громадян. У контексті критичної інфраструктури, публічне управління спрямоване на забезпечення безпеки, стійкості та надійності цих систем [8].

Терористичні акти, що супроводжують повномасштабну агресію російської федерації проти України шляхом ракетних атак на критичну інфраструктуру є не лише актом воєнних злочинів, а також спробою економічного та соціального тиску на Україну з метою спонукання до виконання умов, що сприяли б інтересам країни-агресорки. Після втрат тимчасово окупованих територій в боях за Київську, Сумську, Чернігівську, Харківську, Запорізьку та Херсонську області, російська федерація звернулася до стратегії терористичних дій: з 10 жовтня 2022 року

російські сили систематично наносили масштабні та скоординовані ракетні удари по об'єктах критичної інфраструктури України. На кінець листопада 2022 року російські війська зруйнували чи пошкодили понад 700 важливих об'єктів, включаючи аеропорти, мости, нафтобази, трансформаторні підстанції та електростанції, що мало на меті розгойдати енергетичну систему України, знищуючи ключові трансформаторні підстанції та перешкоджаючи перетоку електроенергії між регіонами. Станом на 26 січня 2023 року від цих ударів загинули принаймні 134 цивільних особи, близько 380 були поранені. Масштаби ракетних атак та їх наслідки наведені у таблиці 2.

Таблиця 2 **Масштаби ракетних атак російської федерації проти України**

Дата	Кількість ракет	перехоплено	Кількість дронів	перехоплено	Кількість загиблих / поранених	Наслідки обстрілів
11 вересня 2022	12	9			4	Військова та цивільна інфраструктура, пункти управління, аеропорти
10 жовтня 2022	84	43	24		23/ 105	пошкоджено 11 важливих об'єктів інфраструктури у 8 регіонах та місті Києві
11 жовтня 2022	28	20	10		5/-	Військова та цивільна інфраструктура
22 жовтня 2022	33	18			0/0	Енергетична інфраструктура
31 жовтня 2022	56	45	5		1/13	вразили 18 об'єктів критичної інфраструктури, розташованих у 10 регіонах України.
15 листопада 2022	96	75		10	3/17	Руйнування енергетичної інфраструктури Харківської та Запорізької областей
17 листопада 2022	18	6				Руйнування енергетичної інфраструктури Харківської та Запорізької областей
23 листопада 2022	70	51			10/36	Руйнування об'єктів енергетичної інфраструктури
5 грудня 2022	70	60			4/5	Руйнування енергетичної інфраструктури Сумської, Одеської, Житомирської області, міста Кропивницький
16 грудня 2022	76	60			0/0	Руйнування енергетичної інфраструктури Київської, Одеської, Херсонської, Харківської області
29 грудня 2022	70	58		11	3/6	було обстріляно 10 областей і пошкоджено 28 об'єктів, із яких 18 – приватні будинки, а решта – об'єкти критичної інфраструктури
31 грудня 2022	20	12	13	13	1/39	Руйнування енергетичної інфраструктури Хмельницька, Запорізька, Миколаївська, Херсонська області
14 січня 2023	38	25			45/80	Ракетний удар по житловому будинку в Дніпрі
26 січня 2023	55	47	17	17	11/11	у деяких областях запроваджено аварійні відключення світла
10 лютого 2023	71	61	28	22	0/8	у деяких областях запроваджено аварійні відключення світла затримки потягів

16 лютого 2023	36	16			1/8	Влучання в об'єкти критичної інфраструктури на півночі, заході України, у Дніпропетровській і Кіровоградській областях
9 березня 2023	75	42	8	4	6/-	Пошкоджено об'єкти генерації та розподілу електричної енергії у 8 регіонах, зокрема – три електростанції компанії ДТЕК
Загалом	**949**	**684**		**687**	**117 / 328**	

Джерело: сформовано автором на основі [9]

Першим принципом публічного управління в цьому контексті є принцип передбачення. Це означає, що органи влади повинні передбачати потенційні загрози та ризики для критичної інфраструктури та розробляти відповідні стратегії захисту і реагування на них. Другий принцип – це принцип превентивного управління, що передбачає прийняття заходів ще до виникнення загрози для запобігання можливим аваріям або кризовим ситуаціям. Він включає планування та підготовку до надзвичайних ситуацій, вдосконалення інфраструктури та запровадження технологій безпеки. Третім принципом є принцип відкритості та прозорості в урядових структурах, які мають забезпечувати доступність інформації щодо стану критичної інфраструктури, планів захисту та реагування на негативні події для громадськості та інших зацікавлених сторін. Четвертий принцип – це принцип координації та співпраці щодо управління критичною інфраструктурою, яка вимагає взаємодії між різними секторами суспільства, включаючи урядові структури, приватний сектор, місцеву владу та громадські організації, для ефективного реагування на загрози та забезпечення стійкості інфраструктури. П'ятий принцип – це принцип постійного вдосконалення в урядових структурах, які повинні постійно аналізувати та вдосконалювати свої підходи до управління критичною інфраструктурою, враховуючи нові технології, загрози та навчальний досвід [9].

Важливо постійно вивчати нові технології та адаптувати їх до потреб інфраструктурних об'єктів для забезпечення максимальної безпеки та стійкості коштом запровадження інноваційних технологій, які відіграють важливу роль у покращенні управління критичною інфраструктурою, забезпечуючи більш ефективну та безпечну роботу об'єктів інфраструктури (рис. 2).

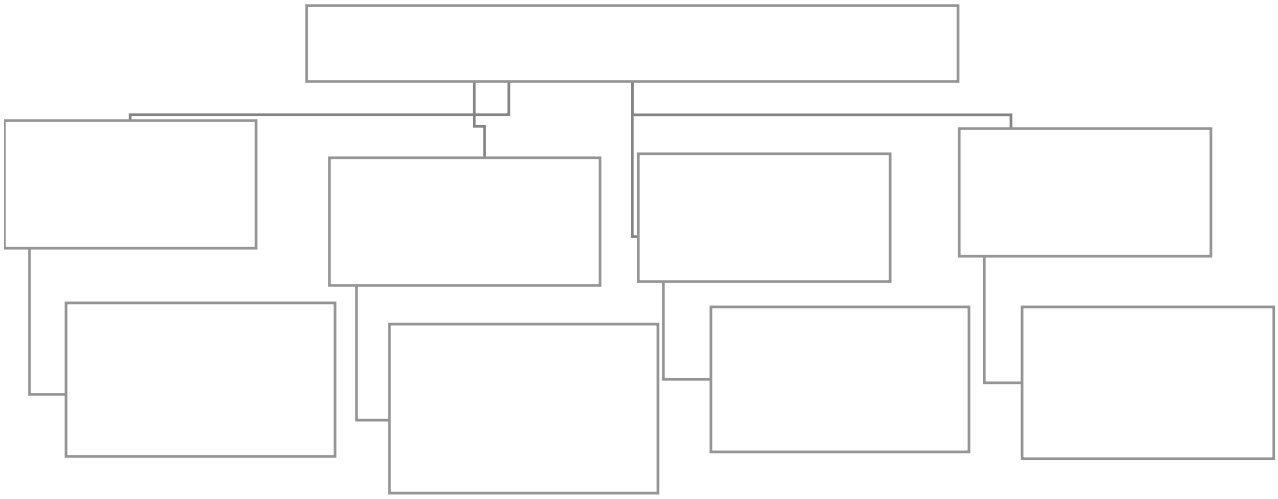

Рисунок 2 – **Інноваційні технології, як допоміжний сегмент управління критичною інфраструктурою**

Джерело: сформовано автором на основі [10, 11]

Отже, дослідивши основні загрози та вразливості стійкості об'єктів критичної інфраструктури, інструменти та методи управління ризиками, можна сформулювати конкретні рекомендації, щодо підвищення ефективності систем управління та забезпечення безпеки об'єктів критичної інфраструктури в умовах сучасних загроз та викликів:

- планування умов функціонування критичної інфраструктури та заходів реагування відповідно до аналізу виявлених, рівня їх наслідків;

- застосування заходів для уникнення загрози або пом'якшення наслідків її впливу шляхом оптимізації процесів військового захисту та розосередження;

- заходи, що вживаються у відповідь на подію (загрозу) для повернення до проєктних параметрів функціонування критичної інфраструктури;

- першочергове реагування з метою локалізації негативного впливу загрози;

- зменшення потреб у послугах, збільшення обсягів надання послуг коштом використання резервних функцій.

Варто зазначити, що планування стійкості критичної інфраструктури повинно відповідати викликам повномасштабного військового вторгнення та враховувати перспективи розвитку інфраструктури з урахуванням нових технологій, що дасть змогу адаптуватись до нових умов експлуатації об'єктів критичної інфраструктури та досягти кращого рівня відновлення, що є одним з головних викликів для забезпечення сталості.

Висновки. Аналізуючи концепції критичної інфраструктури та її роль у сучасному суспільстві, можна зробити висновок, що ця інфраструктура відіграє ключову роль у забезпеченні функціонування держави та економіки. Як показали наслідки російської агресії проти України та тактики масованих ракетних обстрілів критичної інфраструктури, доцільно розробити шляхи забезпечення захисту інфраструктури як елемент національної та економічної безпеки. Розглядаючи принципи публічного управління в контексті забезпечення стійкості критичної інфраструктури, можна побачити, що співпраця між урядовими органами, приватним сектором та громадськістю є важливою складовою успішного управління кризовими ситуаціями. Аналіз інструментів та методів управління ризиками, спрямованих на забезпечення стійкості об'єктів критичної інфраструктури, вказує на необхідність постійного вдосконалення систем безпеки та реагування на кризові ситуації. Сформульовані рекомендації щодо поліпшення систем управління та забезпечення безпеки об'єктів критичної інфраструктури в умовах сучасних загроз та викликів підкреслюють необхідність постійного вдосконалення та адаптації до нових технологічних та соціальних викликів.

Література:

1. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX (зі змінами). Вебсайт Верховної Ради України. 2023. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.
2. Звіт про прямі збитки інфраструктури від руйнувань внаслідок військової агресії росії проти України. Вебсайт Київської школи економіки. 2023. URL: https://kse.ua/wp-content/uploads/2023/03/UKR_Feb23_FINAL_Damages-Report-1.pdf.
3. Невольніченко А.І., Чумаченко С.М., Михайлова А.В., Пиріков О.В., Мурасов Р.К. Моделювання загроз виникнення надзвичайних ситуацій на об'єктах критичної інфраструктури з використанням методу системної динаміки. *Таврійський науковий вісник. Серія: Технічні науки*. 2022. Вип. 3. С. 88–99. DOI: https://doi.org/10.32851/tnv-tech.2022.3.10.
4. Lallemant D., Bicksler R., Barns K., Hamel P., Soden R., Bannister S. Toward a critical technical practice in disaster risk management: lessons from designing collaboration initiatives. *Disaster Prevention and Management*. 2023. Vol. 32 No. 1, pp. 100–116. DOI: https://doi.org/10.1108/DPM-08-2022-0160.
5. Onyshchenko S., Hlushko A. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. *Науковий журнал «Економіка і регіон»*. 2022. № 184. С. 13–20. DOI: https://doi.org/10.26906/EiR.2022.1(84).2540.
6. Ampratwum G., Tam V.W.Y., Osei-Kyei R. Critical analysis of risks factors in using public-private partnership in building critical infrastructure resilience: a systematic review. *Construction Innovation*. 2023. Vol. 23 No. 2. P. 360–382. DOI: https://doi.org/10.1108/CI-10-2021-0182.
7. Melnyk D. Protection of national critical information infrastructure: issues of the day and solutions. *Administrative law and process.* 2022. Vol. 3(38). P. 5–16. DOI: https://doi.org/10.17721/2227-796X.2022.3.01.
8. Osei-Kyei R., Almeida L.M., Ampratwum G. and Tam V. "Systematic review of critical infrastructure resilience indicators". *Construction Innovation.* 2023. Vol. 23. No. 5. P. 1210–1231. DOI: https://doi.org/10.1108/CI-03-2021-0047.
9. Nyqvist R., Peltokorpi A. and Seppänen O. "Can ChatGPT exceed humans in construction project risk management?". *Engineering, Construction and Architectural Management.* 2024. Vol. 31. No. 13. P. 223 – 243. DOI: https://doi.org/10.1108/ECAM-08-2023-0819.
10. Ракетні удари по Україні. Вебсайт uk.wikipedia.org. URL: https://uk.wikipedia.org/wiki/%D0%A0%D0%B0%D0%BA%D0%B5%D1%82%D0%BD%D1%96_%D1%83%D0%B4%D0%B0%D1%80%D0%B8_%D0%BF%D0%BE_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96.
11. Andersen T.J. and Sax J. Responding to Advance Upside Potential Through Interactive Strategic Control Processes. *Responding to Uncertain Conditions: New Research on Strategic Adaptation (Emerald Studies in Global Strategic Responsiveness*). Leeds : Emerald Publishing Limited, 2023. P. 65–89. DOI: https://doi.org/10.1108/978-1-80455-964-220231004.
12. Adu Gyamfi T., Aigbavboa C.O. and Thwala W.D. Risk resources management influence on public-private partnership risk management in construction industry. Confirmatory factor analysis approach. *Journal of Engineering, Design and Technology*. 2022. DOI: https://doi.org/10.1108/JEDT-12-2021-0699.
13. Практичні рекомендації щодо забезпечення стійкості об'єктів критичної інфраструктури, недопущення припинення або погіршення надання важливих функцій для життєдіяльності населення. Вебсайт Затурцівської сільської ради. 2023. URL: https://zaturcivska-gromada.gov.ua/news/1687855421/

14. Good Governance for Critical Infrastructure Resilience, OECD Reviews of Risk Management Policies. Paris : OECD Publishing, 2019. p. 118. DOI: https://doi.org/10.1787/02f0e5a0-en.
15. Biden-Harris Administration Announces $1.8 Billion in Infrastructure Grants Across the Country, Putting More Projects into the Pipeline as Part of Our Infrastructure Decade. Website U.S. Department of Transportation. 2024. URL: https://www.transportation.gov/briefing-room/investing-america-biden-harris-administration-announces-18-billion-infrastructure
16. Government at a Glance 2021. Paris : OECD Publishing, 2021. p. 280. DOI: https://doi.org/10.1787/1c258f55-en.
17. Інформаційно-аналітична довідка про надзвичайні ситуації в Україні у 2023 році. Вебсайт ДСНС України. URL: https://dsns.gov.ua/upload/2/0/2/2/3/2/1/2023-rik.pdf

References:

1. Verkhovna Rada of Ukraine (2021). *On critical infrastructure. No. 1882-IX*. https://zakon.rada.gov.ua/laws/show/1882-20#Text.
2. Kyiv School of Economics (2023). *Report on direct damage to infrastructure from the destruction caused by Russia's military aggression against Ukraine.* https://kse.ua/wp-content/uploads/2023/03/UKR_Feb23_FINAL_Damages-Report-1.pdf.
3. Nevolnichenko, A.I., Chumachenko, S.M., Mykhailova, A.V., Pyrikov, O.V., & Murasov, R.K. (2022). Modeling the threat of emergency situations at critical infrastructure facilities using the system dynamics method. *Taurian Scientific Bulletin. Series: Technical sciences*, 3, 88–99. https://doi.org/10.32851/tnv-tech.2022.3.10.
4. Lallemant, D., Bicksler, R., Barns, K., Hamel, P., Soden, R. & Bannister, S. (2023). Toward a critical technical practice in disaster risk management: lessons from designing collaboration initiatives. *Disaster Prevention and Management,* 32 (1), 100–116. https://doi.org/10.1108/DPM-08-2022-0160.
5. Onyshchenko, S. & Hlushko, A. (2022). Analytical measurement of Ukraine's cyber security in the face of growing challenges and threats. *Scientific journal "Economy and Region"*, 1(84), 13–20. https://doi.org/10.26906/EiR.2022.1(84).2540.
6. Ampratwum, G., Tam, V.W.Y. & Osei-Kyei, R. (2023). Critical analysis of risks factors in using public-private partnership in building critical infrastructure resilience: a systematic review. *Construction Innovation,* 23 (2), 360–382. https://doi.org/10.1108/CI-10-2021-0182.
7. Melnyk, D. (2022). Protection of national critical information infrastructure: issues of the day and solutions. *Administrative law and process,* 3(38), 5–16. https://doi.org/10.17721/2227-796X.2022.3.01.
8. Osei-Kyei, R., Almeida, L.M., Ampratwum, G. & Tam, V. (2023). Systematic review of critical infrastructure resilience indicators. *Construction Innovation*, 23 (5), 1210–1231. https://doi.org/10.1108/CI-03-2021-0047.
9. Nyqvist, R., Peltokorpi, A. & Seppänen, O. (2024). Can ChatGPT exceed humans in construction project risk management? *Engineering, Construction and Architectural Management,* 31 (13), 223 – 243. https://doi.org/10.1108/ECAM-08-2023-0819.
10. Uk.wikipedia. (2024). *Missile strikes on Ukraine*. https://uk.wikipedia.org/wiki/%D0%A0%D0%B0%D0%BA%D0%B5%D1%82%D0%BD%D1%96_%D1%83%D0%B4%D0%B0%D1%80%D0%B8_%D0%BF%D0%BE_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96.
11. Andersen, T.J. & Sax, J. (2023). *Responding to Advance Upside Potential Through Interactive Strategic Control Processes. Responding to Uncertain Conditions: New Research on Strategic Adaptation (Emerald Studies in Global Strategic Responsiveness)*, Emerald Publishing Limited. https://doi.org/10.1108/978-1-80455-964-220231004.
12. Adu Gyamfi, T., Aigbavboa, C.O. & Thwala, W.D. (2022). Risk resources management influence on public–private partnership risk management in construction industry. Confirmatory factor analysis approach, *Journal of Engineering, Design and Technology*. https://doi.org/10.1108/JEDT-12-2021-0699.
13. Zaturtsivka village council (2023). *Practical recommendations on ensuring the stability of critical infrastructure objects, preventing the termination or deterioration of the provision of important functions for the population's daily life*. https://zaturcivska-gromada.gov.ua/news/1687855421/.
14. OECD Publishing. (2019). *Good Governance for Critical Infrastructure Resilience, OECD Reviews of Risk Management Policies*. https://doi.org/10.1787/02f0e5a0-en.
15. U.S. Department of Transportation (2024). *Biden-Harris Administration Announces $1.8 Billion in Infrastructure Grants Across the Country, Putting More Projects into the Pipeline as Part of Our Infrastructure Decade.* https://www.transportation.gov/briefing-room/investing-america-biden-harris-administration-announces-18-billion-infrastructure.
16. OECD Publishing. (2021). *Government at a Glance 2021*. https://doi.org/10.1787/1c258f55-en.
17. State Emergency Service of Ukraine. (2023). *Informational and analytical reference on emergency situations in Ukraine in 2023*. https://dsns.gov.ua/upload/2/0/2/2/3/2/1/2023-rik.pdf.