УДК 342.85:658.5.5

Магомедов Андрій Омарович
кандидат історичних наук,
здобувач кафедри історії та культури України
Університет Григорія Сковороди в Переяславі
Magomedov Andrii
PhD in History,
Applicant of the Department of History and Culture of Ukraine
Hryhorii Skovoroda University in Pereiaslav
ORCID: 0000-0001-5919-2340

DOI: 10.25313/2617-572X-2024-7-10106

ІННОВАЦІЇ В ПУБЛІЧНОМУ УПРАВЛІННІ СФЕРОЮ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

INNOVATIONS IN PUBLIC MANAGEMENT OF CRITICAL INFRASTRUCTURE

Анотація. *Вступ. В контексті сучасних глобальних викликів та загроз, ефективне управління критичною інфраструктурою є вирішальною проблемою для національної безпеки та стабільності. Україна, яка стикається зі складнощами управління критичною інфраструктурою через наслідки повномасштабної військової агресії. Досягнення стійкої та ефективної безпеки об'єктів критичної інфраструктури в умовах воєнного стану в Україні є пріоритетом для забезпечення стабільності та безпеки суспільства.*

Мета. Метою дослідження є аналіз особливостей впровадження інноваційних підходів у публічне управління для трансформації об'єктів критичної інфраструктури, ідентифікація ключових проблем та викликів у цій сфері та розробка рекомендацій щодо практичного впровадження отриманих результатів. Об'єктом дослідження є процес впровадження інноваційних підходів у публічне управління, а предметом – трансформація об'єктів критичної інфраструктури. Особлива увага зосереджена на ідентифікації проблем управління критичною інфраструктурою, пов'язаних із повномасштабним військовим вторгненням російської федерації, та шляхів їх подолання.

Матеріали і методи. У дослідженні були використані методи аналізу та синтезу наукових джерел, включаючи вітчизняну та зарубіжну літературу, результати конференцій, а також досвід провідних науковців у галузі. Крім того, були використані методи аналізу та порівняльного аналізу для оцінки ефективності різних підходів.

Результати. У дослідженні було проведено аналіз теоретичних підходів до поняття «інновації» у сфері управління критичною інфраструктурою, виявлено ключові проблеми та виклики, з якими стикаються органи державної влади у процесі трансформації, та розроблені рекомендації щодо їх подолання. На підставі отриманих результатів дослідження були сформульовані рекомендації щодо практичного впровадження інноваційних підходів у публічне управління для трансформації об'єктів критичної інфраструктури в умовах воєнного стану та післявоєнної відбудови. Вони включають у себе необхідність залучення всіх зацікавлених сторін, створення механізмів підтримки та фінансування, а також посилення співпраці між публічним та приватним сектором.

Перспективи. Перспективами подальших досліджень є інновацій в публічному управлінні сферою критичної інфраструктури є дослідження ефективності цифрових рішень у критичній інфраструктурі, зокрема, використання штучного інтелекту та великих даних, інноваційних підходів до кібербезпеки в критичній інфраструктурі та оцінка економічної доцільності інноваційних проектів у сфері критичної інфраструктури.

Ключові слова: *інноваційні підходи, публічне управління, критична інфраструктура, безпека, ризики, управління ризиками, громадська безпека.*

Summary. *Introduction. In the context of today's global challenges and threats, the effective management of critical infrastructure is a critical issue for national security and stability. Ukraine, which faces the complexities of managing critical infrastructure due to the consequences of full-scale military aggression. Achieving sustainable and effective security of critical infrastructure facilities in the conditions of martial law in Ukraine is a priority for ensuring the stability and security of society.*

Purpose. The purpose of the study is to analyze the features of the implementation of innovative approaches in public administration for the transformation of critical infrastructure objects, to identify key problems and challenges in this area, and to develop recommendations for the practical implementation of the obtained results. The object of research is the process of introducing innovative approaches in public administration, and the subject is the transformation of critical infrastructure objects. Particular attention is focused on the identification of critical infrastructure management problems associated with a full-scale military invasion of the Russian Federation and ways to overcome them.

Materials and methods. The research used methods of analysis and synthesis of scientific sources, including domestic and foreign literature, results of conferences, as well as the experience of leading scientists in the field. In addition, analytical and comparative analysis methods were used to evaluate the effectiveness of different approaches.

Results. The study analyzed theoretical approaches to the concept of "innovation" in the field of critical infrastructure management, identified key problems and challenges faced by state authorities in the process of transformation, and developed recommendations for overcoming them. Based on the results of the study, recommendations were formulated for the practical implementation of innovative approaches in public administration for the transformation of critical infrastructure objects in the conditions of martial law and post-war reconstruction. They include the need to involve all stakeholders, create support and financing mechanisms, and strengthen cooperation between the public and private sectors.

Discussion. Prospects for further research into innovations in the public management of critical infrastructure are the study of the effectiveness of digital solutions in critical infrastructure, in particular, the use of artificial intelligence and big data, innovative approaches to cyber security in critical infrastructure and the assessment of the economic feasibility of innovative projects in the field of critical infrastructure.

Key words: *innovative approaches, public management, critical infrastructure, security, risks, risk management, public safety.*

Постановка проблеми. Проблема впровадження інновацій в публічному управлінні сферою критичної інфраструктури в Україні стає особливо актуальною через ведення воєнних дій на території країни. З урахуванням сучасних геополітичних загроз та повномасштабного військового вторгнення російської федерації, критична інфраструктура України, така як енергетика, транспорт, телекомунікації та інші, стає об'єктом особливої уваги. Оскільки ці об'єкти є стратегічно важливими для функціонування держави та забезпечення її національної безпеки, ефективне управління ними є критично важливим завданням. Основним викликом в публічному управлінні сферою критичної інфраструктури в Україні є необхідність забезпечення безпеки та стійкості цих об'єктів в умовах воєнного стану.

Аналіз останніх досліджень та публікацій. Актуальність теми дослідження визначається увагою авторів до розробки проблематики, зокрема, Страхніцький Я.О. [1], Домарацький М.Б. [3], Богдан Б.В. [4], Плахотнюк Р.В.[6, 12] та інші досліджують різні аспекти управління критичною інфраструктурою. Крім того, Аль-Мхдаві М.К.С., О'Коннор А., Казі А., Рахіміан Ф. та Дакре Н. [5], Еспада Р., Апан А. і Макдугал К. [7], Сун Дж., Балакрішнан С. і Чжан З. [8], Гарсіа-Перес А., Саллос М.П. і Тівасінг П. [11] присвячують свої роботи вивченню міжнародного досвіду та кращих практик у сфері управління критичною інфраструктурою, що можуть слугувати цінним джерелом інформації для країн зі схожими викликами та завданнями.

Усі ці джерела доповнюють одне одного, надаючи широкий обсяг знань та різноманітні підходи до впровадження інновацій у публічне управління для трансформації об'єктів критичної інфраструктури.

Мета статті. Метою дослідження є огляд особливостей впровадження інноваційних підходів у сфері публічного управління з метою трансформації об'єктів критичної інфраструктури. Головна увага зосереджена на аналізі сучасних тенденцій та проблем, що виникають у цій галузі, а також на розробці практичних рекомендацій для вдосконалення управління об'єктами критичної інфраструктури за допомогою інноваційних методів.

Матеріали і методи. У дослідженні були використані методи аналізу та синтезу наукових джерел, включаючи вітчизняну та зарубіжну літературу, результати конференцій, а також досвід провідних науковців у галузі. Крім того, були використані методи аналізу та порівняльного аналізу для оцінки ефективності різних підходів.

Виклад основного матеріалу. На міжнародному та національному рівнях управління критичною інфраструктурою існують деякі серйозні проблеми та виклики. Однією з головних проблем є висока залежність процесів життєдіяльності населення від цієї інфраструктури, яка забезпечує життєво важливі послуги, такі як електроенергія, транспорт, телекомунікації та водопостачання. Додатковою проблемою є недостатність координації між різними відомствами та органами управління, що відповідають за безпеку критичної інфраструктури, що може призвести до дублювання повноважень, недоліків у взаємодії та зниження ефективності вирішення проблем у кризових ситуаціях [1]. Ще однією проблемою є недостатнє фінансування та ресурси, необхідні для впровадження сучасних технологій та заходів безпеки [2].

Усі ці проблеми та виклики потребують комплексного підходу та співпраці всіх зацікавлених сторін для забезпечення ефективного управління критичною інфраструктурою та збереження безпеки

суспільства. Впровадження інновацій у сферу управління критичною інфраструктурою стає все більш важливим у зв'язку зі зростанням загроз та викликів, що ставляться перед цією галуззю (див. табл. 1).

Різні методи та підходи до впровадження інновацій у сферу управління критичною інфраструктурою мають свої переваги та недоліки. Технологічні інновації можуть забезпечити покращення ефективності та безпеки, але вимагають великих фінансових витрат та постійного оновлення. Стратегічне планування дозволяє визначити довгострокові цілі та узгодити дії між зацікавленими сторонами, але може вимагати високого рівня гнучкості. Кризове управління забезпечує швидку реакцію на надзвичайні ситуації, але потребує вправності управлінців та ефективної комунікації. Враховуючи ці особливості, необхідно збалансувати різні підходи для досягнення оптимальних результатів у сфері управління критичною інфраструктурою [3].

Інновації забезпечують трансформацію систем та активів інфраструктури, як наслідок — скорочується ступінь ризиків та загроз негативного впливу на її функціонування, що є складовою політики стійкості та безпеки критичної інфраструктури.

Трансформації відбуваються в різних секторах: енергетичному, транспортному, інформаційному та інших. Інновації впроваджуються в енергетичному секторі завдяки зростанню частки відновлювальних ресурсів, розвитку інтелектуальних мереж, децентралізованому та локалізованому підходах до виробництва, споживання енергії.

Динамічність у розвитку автономних транспортних засобів та використання штучного інтелекту трансформує транспортний сектор, виникають нові вразливості його інфраструктури, що потребує пошуку нових інноваційних методів публічного управління в роботі повноважних органів та суб'єктів.

Інформаційно-комунікаційні технології змінили способи обміну даними. Розумні міста, керований вплив на які здійснюється на основі підходу, орієнтованого на дані, поєднують інформаційну революцію та інновації, міські послуги населенню, особливо у мегаполісах.

Все вище вказане вплинуло на прискорення інноваційного розвитку публічного управління, де більш децентралізовані системи, автономні механізми керованого впливу поступово замінюють централізовані управлінські мережі з автоматизацією та контролем. Такі характеристики нового публічного менеджменту посилюють стійкість за рахунок гнучкості та адаптивності.

У таблиці 2 представлено інноваційні інструменти політики для підвищення стійкості критичної інфраструктури, які активно використовуються в різних країнах.

Надання інформації про загрози, небезпеки в Австралії відбувається завдяки створенню довіреної мережі обміну інформацією (TISN) для стійкості критичної інфраструктури, що створена урядом країни 2003 року. Мережа надає допомогу операторам для кращого запобігання, протидії, підготовки, реагування та відновлення роботи об'єктів після збоїв і несприятливих подій. TISN охоплює різні зацікавлені сторони: Департамент генерального прокурора, ряд австралійських урядових установ, представників

Таблиця 1

Методи та підходи до впровадження інновацій у сферу управління критичною інфраструктурою

Метод/ Підхід	Переваги	Недоліки	Особливості
Технологічні інновації	– покращення ефективності інфраструктури; – збільшення безпеки та стійкості системи; – покращення якості обслуговування	– високі витрати на впровадження і підтримку; – ризик технологічного застаріння	– потреба в постійному оновленні та моніторингу; – необхідність висококваліфікованих кадрів та підготовки персоналу
Стратегічне планування	– визначення довгострокових цілей та завдань; – узгодженість дій між різними зацікавленими сторонами; – можливість адаптації до змін у середовищі	– може бути довготривалим та ресурсоємким; – ризик втрати актуальності стратегічних планів	– потреба у визначенні стратегічних пріоритетів та підвищенні гнучкості управління; – важливість постійного моніторингу та оновлення стратегій
Кризове управління	– швидка реакція на надзвичайні ситуації; – можливість мінімізації збитків та загроз	– ризик непропорційності реакції; – неможливість передбачення всіх можливих ризиків	– необхідність тренування та вправності управлінців у кризових ситуаціях; – потреба в швидкій та ефективній комунікації з усіма зацікавленими сторонами

Джерело: авторська розробка

Таблиця 2

Перелік інноваційних інструментів політики для підвищення стійкості критичної інфраструктури в країнах ОЕСР

Інструмент політики	Характеристика
Надання інформації про загрози, небезпеки	Уряди надають власникам, операторам об'єктів критичної інфраструктури результати оцінок загроз та небезпек на національному рівні або в інфраструктурі.
Механізми або платформи добровільного обміну інформацією	Уряди держав заохочують власників та операторів критичної інфраструктури до обміну інформацією в сфері безпеки та стійкості активів та систем, між операторами та урядами на добровільній основі.
Механізми або платформи обов'язкового обміну інформацією	Закони та нормативно-правові акти встановлюють вимоги до операторів критичної інфраструктури щодо обміну з урядом інформацією, яка стосується безпеки та стійкості активів і систем.
Заходи з підвищення обізнаності та тренінги	Заходи з підвищення обізнаності та тренінги сприяють розвитку культури оцінки та розуміння ризиків в критичній інфраструктурі. Тренінги та навчання сприяють перевірці системи управління критичною інфраструктурою в надзвичайних ситуаціях та надають інформацію про обов'язки під час криз.
Рекомендації щодо підтримки стійкості для операторів критичної інфраструктури	Рекомендації щодо стійкості окреслюють етапи та методи, які оператори критичної інфраструктури виконують для підвищення стійкості їх активів і систем. Такі керівні принципи можуть бути вузько спеціалізованими за обсягом, наприклад, керівні вказівки для оцінки небезпеки на рівні оператора, або широкими за обсягом, в яких перераховуються численні інструменти та заходи підвищення стійкості.
Сприяння розвитку/використанню професійних стандартів	Галузеві нормативні акти, присвячені стійкості критичної інфраструктури
Механізм стимулювання операторів критичної інфраструктури для оцінки ризиків і вразливостей	Правила забезпечення безперервності діяльності на основі показників ефективності, які заохочують операторів критичної інфраструктури проводити оцінку ризиків, небезпек та вразливості. Стимулами можуть бути технічна підтримка та керівні документи в цій сфері, або механізми винагороди, такі як оприлюднення оглядів з досягнення цілей стійкості або сертифікації.
Механізми стимулювання інвестування в стійкість	Уряди надають стимули, які заохочують операторів критичної інфраструктури інвестувати в стійкість критичної інфраструктури, зокрема: субсидії, аналіз витрат і вигод або участь уряду в схемах страхування.
Розробка професійних стандартів стійкості критичної інфраструктури, таких як контрольні показники можливостей, стандарти виконання операцій	Уряди розробляють нормативні акти, які визначають операторів критичної інфраструктури для виконання певних контрольних показників, стандартів. За допомогою цього інструменту встановлюються обов'язкові вимоги до операторів критичної інфраструктури, які необхідно виконати для забезпечення захисту та стійкості на основі галузевих особливостей. Також визначають норми для заохочення операторів критичної інфраструктури досягати цільового рівня продуктивності для підтримки послуг під час збоїв.
Обов'язкові плани безперервності діяльності	Уряди вимагають від операторів критичної інфраструктури розробки планів безперервності бізнесу. Такі плани включають заходи запобігання та готовності (включаючи плани на випадок надзвичайних ситуацій, аварій, збоїв тощо), які оператори можуть використовувати під час небезпечних ситуацій та загроз для продовження бізнес-операцій.
Перевірки та оцінка ефективності	Уповноважені інспектори перевіряють стан запровадження необхідних заходів стійкості операторами критичної інфраструктури
Штрафи за недотримання вимог стійкості	У випадках виявлення інспекторами недотримання вимог стійкості можуть бути накладені штрафні санкції
Інші види штрафів за невиконання вимог стійкості	Інші види покарань за невідповідність можуть включати: анулювання ліцензії на експлуатацію або тимчасове усунення з експлуатації до виконання вимог.
Ранжування на основі результатів перевірки/виконання	Уряд складає рейтинг та оголошує результати перевірки/виконання вимог операторами. Оператори зацікавлені в високих оцінках рейтингу для збереження іміджу та репутації як важливого фактору успіху бізнесу
Звітність операторів по стійкості	Оператори проводять оцінювання стійкості критичної інфраструктури та надають результати уряду та/або громадськості.
Державні інвестиції в стійкість інфраструктури	Державні інвестиції спрямовуються в проекти розвитку та розбудови нової інфраструктури, її стійкості поряд із забезпеченням усунення прогалин в регулюванні в разі потреби. В разі державного фінансування для створення стійких систем критичної інфраструктури можуть бути встановлені стандарти для підтвердження цінності інвестицій.

Продовження табл. 2

Керівництво для субнаціональних рівнів управління	Керівні принципи для субнаціональних рівнів управління для зростання ступеня обізнаності про об'єкти критичної інфраструктури у відповідних юрисдикціях, які можуть зумовлювати транскордонні ризики, для посилення стійкості систем на транскордонних територіях
Обов'язкове страхування критичної інфраструктури	Для власників і операторів критичної інфраструктури можуть бути застосовані зобов'язання зі страхування об'єктів на випадок шоку або зриву послуг.
Рецензування, моніторинг та оцінка	Експерти проводять оцінку та перегляд прогресу досягненні цілей стійкості на основі узгоджених критеріїв оцінки відповідно до вказівок щодо стійкості до окремих секторів. Результати можуть виявити потенційні прогалини та надати пропозиції щодо напрямків покращення.

Джерело: систематизовано автором за даними [14–15]

багатьох найбільших і найвідоміших компаній Австралії, уряди штатів і територій.

Уряди інших країн використовують такі інноваційні інструменти політики, як механізми або платформи добровільного, обов'язкового обміну інформацією; заходи з підвищення обізнаності та тренінги; рекомендації щодо підтримки стійкості для операторів критичної інфраструктури; сприяння розвитку/використанню професійних стандартів; механізм стимулювання операторів критичної інфраструктури для оцінки ризиків і вразливостей; механізми стимулювання інвестування в стійкість; розробка професійних стандартів стійкості критичної інфраструктури, таких як контрольні показники можливостей, стандарти виконання операцій та інші.

Застаріла інфраструктура в різних країнах потребує інвестування в її інноваційний розвиток та підтримку стійкості. Аналіз Організації економічного співробітництва та розвитку (далі — ОЕСР) вказує на те, що для забезпечення інвестиційних, інноваційних потреб сектору інфраструктури потрібно 95 трлн. дол. на період 2016–2030 років [13].

Для забезпечення ефективності інвестування в інновації варто переглянути моделі публічного управління інфраструктурою. Власне тому ОЕСР впровадила концепцію «кращого управління», спрямовану на реалізацію проектів в економічно ефективний спосіб з врахуванням доступності для громадян та користувачів. У концепції наголошується на доцільності врахування стійкості на початкових етапах інвестування в інновації у різних секторах інфраструктури для забезпечення її безперебійної роботи при можливих стихійних лихах та надзвичайних ситуаціях [14–15].

У сучасному управлінні об'єктами критичної інфраструктури спостерігається ряд важливих тенденцій та інноваційних практик, що спрямовані на підвищення ефективності та безпеки цих об'єктів.

За даними статистики в Україні внаслідок воєнних дій критичній інфраструктурі завдано збитків на суму $36,6 млрд. [1]. Захист критичної інфраструктури від ракетних обстрілів є важливим аспектом національної безпеки, особливо в прикордонних регіонах, що включає в себе заходи з мінімізації можливих збитків та збереження функціональності об'єктів критичної інфраструктури у разі ракетних нападів. Одним з основних методів захисту є розробка та впровадження систем протиракетної оборони, які здатні вчасно виявляти та перехоплювати ворожі ракети до досягнення цілей [4]. Ці системи можуть включати в себе ракетні комплекси з протиракетами, системи обліку та виявлення ракет, а також системи управління та командування. Крім того, важливим є також застосування інженерних рішень для зміцнення критичної інфраструктури та зменшення можливих збитків від ракетних обстрілів, що може включати в себе будівництво захисних споруд, використання спеціальних матеріалів, що зменшують пошкодження від вибухів, та розробку евакуаційних планів для персоналу та мешканців прилеглих територій.

Успішними прикладами захисту критичної інфраструктури від ракетних обстрілів є системи, що використовуються в державі Ізраїль та США, країнах ЄС, Королівстві Саудівська Аравія та ін., де розроблені та впроваджені ефективні системи протиракетного захисту, такі як «Залізний купол» в Ізраїлі та система «Patriot» в США [5]. Ці системи демонструють успішність у виявленні та знищенні ворожих ракет, захищаючи критичну інфраструктуру та населення від потенційної загрози.

Іншою важливою тенденцією є перехід до інтегрованих та гнучких систем управління, які забезпечують комплексний підхід до захисту критичної інфраструктури в умовах нападів, що включає в себе розробку мережевих систем управління, які забезпечують зв'язок між різними об'єктами та забезпечують швидкий обмін інформацією [6]. Наприклад, створення стандартів та протоколів для взаємодії між різними системами критичної інфраструктури допомагає забезпечити сумісність та ефективність роботи. Також впровадження роботизації та автоматизації процесів управління може підвищити ефективність та швидкість реагування на надзвичайні ситуації, в тому числі наслідки ракетних атак [7].

Україна в умовах повномасштабної військової агресії з боку Російської Федерації, має свої власні виклики та особливості управління об'єктами критичної інфраструктури. Деякі з найважливіших тенденцій та інноваційних практик в цій галузі включають:

1. Створення протиракетних заходів захисту. Україна активно впроваджує технології та методи захисту об'єктів критичної інфраструктури від воєнних загроз, що включає в себе впровадження систем раннього попередження про атаки, підвищення кібербезпеки та забезпечення фізичного захисту об'єктів.

2. Розвиток альтернативних джерел енергії та комунікацій. У зв'язку з ризиком збоїв у постачанні енергії та комунікаційному зв'язку через можливі атаки, Україна розвиває альтернативні джерела енергії, такі як сонячна та вітрова енергія, а також розширює мережі зв'язку і системи переключення споживачів за мережами [8].

3. Удосконалення систем моніторингу та реагування. Уряд України зосереджує увагу на покращенні систем моніторингу та реагування на надзвичайні ситуації, що включає в себе розробку та впровадження програм швидкого реагування, координацію дій між різними органами влади та підвищення готовності до можливих ракетних атак на критичну інфраструктуру з урахуванням песимістичних сценаріїв їх потенційних наслідків.

4. Модернізація та інтеграція систем управління. Україна працює над модернізацією систем управління об'єктами критичної інфраструктури з метою підвищення ефективності та стійкості, що включає в себе впровадження сучасних технологій та інтеграцію різних систем для забезпечення більшої оперативності.

Закон України «Про критичну інфраструктуру» встановлює юридичні та організаційні основи для створення та операційної діяльності національної системи захисту критичної інфраструктури і є невід'ємною частиною законодавства у сфері національної безпеки [9].

Після початку повномасштабного військового вторгнення у 2022 році в Україні, було створено Реєстр збитків, завданих агресією Російської Федерації проти України (RD4U), який вже розпочав свою діяльність за підтримки міжнародних партнерів. Окрім збитків, завданих громадянам України, Реєстр також пріоритетно вирішує питання про оцінку наслідків руйнування критичної інфраструктури [10].

5. Залучення міжнародної допомоги та експертизи. Україна активно співпрацює з міжнародними партнерами для отримання допомоги та експертизи у сфері управління критичною інфраструктурою, що допомагає впроваджувати найкращі світові практики та забезпечує підтримку в умовах військової агресії.

Описані вище тенденції та інноваційні практики є важливими для забезпечення стійкості та безпеки критичної інфраструктури в умовах війни. Вони

Розробка імовірних сценаріїв кризових ситуацій

• Органи публічної влади повинні залучити експертів з різних галузей для розробки імовірних сценаріїв кризових ситуацій, що можуть виникнути в області критичної інфраструктури, що допоможе підготуватися до можливих загроз та швидко реагувати на них, зокрема моделювання анслідків ракетних обстрілів та терористичних актів з боку країни-агресора

Створення механізмів реагування на кризові ситуації

• Необхідно розробити ефективні механізми реагування на кризові ситуації, включаючи швидке виявлення та ліквідацію можливих загроз для критичної інфраструктури, що може включати в себе розробку планів дій, тренування персоналу та впровадження сучасних технологій моніторингу та комунікації.

Сприяння інноваційним технологічним рішенням

• Органи влади повинні стимулювати розвиток та впровадження інноваційних технологій у сфері критичної інфраструктури, таких як IoT, ШІ та блокчейн, що допоможе підвищити ефективність та безпеку об'єктів інфраструктури.

Збільшення співпраці між зацікавленими сторонами

• Урядові органи, приватні підприємства, академічна громадськість та міжнародні партнери повинні активно співпрацювати для забезпечення ефективного управління критичною інфраструктурою, що може включати в себе обмін інформацією, розробку спільних проєктів та координацію заходів в кризових ситуаціях.

Рис. 1. Рекомендації для практичного впровадження інноваційних підходів сфері публічного управління для трансформації об'єктів критичної інфраструктури

Джерело: узагальнено автором на основі [11–12]

допомагають зменшити ризики та наслідки можливих атак, а також підвищують готовність країни до надзвичайних ситуацій.

Після проведеного аналізу ситуації в сфері публічного управління та трансформації об'єктів критичної інфраструктури, пропонується низка рекомендації, зображених на рис. 1.

Ефективність та результативність практичного впровадження інноваційних підходів у сфері публічного управління для трансформації об'єктів критичної інфраструктури залежить від ефективності виконання цих рекомендацій та активної співпраці між усіма зацікавленими сторонами.

Висновки і перспективи подальших досліджень. У контексті війни та загрози безпеці критичної інфраструктури, інновації в публічному управлінні сферою критичної інфраструктури в Україні виявляються надзвичайно важливими. Вони стають не лише ключовими, але й необхідними для забезпечення стійкості, безпеки та ефективності цих об'єктів у умовах постійної загрози. Узагальнюючи, інноваційні підходи у публічному управлінні сферою критичної інфраструктури в Україні в умовах війни відіграють ключову роль у забезпеченні безпеки та стійкості країни, що вимагає поєднання стратегічного планування, застосування передових технологій з метою ефективного захисту критичної інфраструктури та забезпечення безпеки національних інтересів. У перспективах подальших досліджень є розробка методологій оцінки економічної ефективності впровадження інновацій, аналізу впливу інновацій на економічну стабільність та розвиток у публічному управлінні критичною інфраструктурою. Розвиток інноваційної культури є основою формування наукового підґрунтя для подальших досліджень.

Література

1. Strahnitskyi Y. O. Features of the current state policy in the sphere of protection of critical infrastructure in the conditions of war in Ukraine. *Modernization of the system of public management and administration in Ukraine: the experience of the Republic of Latvia: Scientific monograph*. Riga, Latvia: «Baltija Publishing», 2023. P. 115–142 p. doi: https://doi.org/10.30525/978-9934-26-279-1-5.

2. Деякі питання фінансування робіт з відновлення зруйнованого майна та інфраструктури: Постанова КМУ від 29 липня 2022 р. № 879. URL: https://zakon.rada.gov.ua/laws/show/879-2022-п#Text (дата звернення: 29.03.2024).

3. Домарацький М. Б. Забезпечення безпеки та підвищення ефективності захисту критично важливих об'єктів на державному рівні. *Публічне управління і адміністрування в Україні*. 2019. Вип. 14. С. 82–85. doi: https://doi.org/10.32843/2663-5240-2019-14-16.

4. 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. doi: https://doi.org/10.54929/2786-5746-2022-6-01-09.

5. Al-Mhdawi M. K. S., O'connor A., Qazi A., Rahimian F., Dacre N. Review of studies on risk factors in critical infrastructure projects from 2011 to 2023. *Smart and Sustainable Built Environment, Vol. ahead-of-print No. ahead-of-print*. 2024. doi: https://doi.org/10.1108/SASBE-09-2023-0285.

6. Плахотнюк Р. В. Концептуальні засади вдосконалення взаємодії між уповноваженими органами у сфері захисту критичної інфраструктури. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2023. 7. doi: https://doi.org/10.54929/2786-5746-2023-7-01-17.

7. Espada R., Apan A., 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. P. 375–411. doi: https://doi.org/10.1108/IJDRBE-03-2015-0010.

8. Sun J., Balakrishnan S., Zhang Z. A resource allocation framework for predisaster resilience management of interdependent infrastructure networks. *Built Environment Project and Asset Management*. 2021. Vol. 11, No. 2. P. 284–303. doi: https://doi.org/10.1108/BEPAM-06-2020-0109.

9. Про критичну інфраструктуру : Закон України від 16 листопада 2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 29.03.2024).

10. *Реєстр збитків для України: офіційний вебсайт*. URL: https://rd4u.coe.int/uk/news (дата звернення: 29.03.2024).

11. Garcia-Perez A., Sallos M. P., 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. P. 465–486. doi: https://doi.org/10.1108/JIC-06-2021-0166.

12. Плахотнюк Р. В. Засади та напрями вдосконалення державно-приватного партнерства у сфері захисту критичної інфраструктури. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2022. 6. doi: https://doi.org/10.54929/2786-5746-2022-6-01-15.

13. Investing in Climate, Investing in Growth. Paris: OECD Publishing, 2017. 309 p. doi: https://dx.doi.org/10.1787/9789264273528-en.

14. Getting Infrastructure Right. A framework for better governance. Paris: OECD Publishing, 2017. 93 p. doi: https://dx-.doi.org/10.1787/9789264272453-en.

15. Good Governance for Critical Infrastructure Resilience, OECD Reviews of Risk Management Policies. Paris: OECD Publishing, 2019. 114 p. doi: https://doi.org/10.1787/02f0e5a0-en.

References

1. Strahnitskyi, Y. O. (2023). Features of the current state policy in the sphere of protection of critical infrastructure in the conditions of war in Ukraine. *Modernization of the system of public management and administration in Ukraine: the experience of the Republic of Latvia: Scientific monograph*. Riga, Latvia: "Baltija Publishing", 115–142. doi: https://doi.org/10.30525/978-9934-26-279-1-5.

2. Deyaki pytannya finansuvannya robit z vidnovlennya zruynovanoho mayna ta infrastruktury [Resolution of the CMU "Some issues of financing works to restore destroyed property and infrastructure"]: Postanova KMU vid 29 lypnya 2022 r. № 879. URL: https://zakon.rada.gov.ua/laws/show/879–2022-п#Text [in Ukrainian].

3. Domaratskyy, M. B. (2019). Zabezpechennya bezpeky ta pidvyshchennya efektyvnosti zakhystu krytychno vazhlyvykh obyektiv na derzhavnomu rivni [Ensuring security and increasing the efficiency of protection of critical objects at the state level]. *Publichne upravlinnya i administruvannya v Ukrayini — Public management and administration in Ukraine,* 14, 82–85. doi: https://doi.org/10.32843/2663-5240-2019-14-16 [in Ukrainian].

4. Bohdan, B. V. (2022). Aktualni pytannya normatyvno-pravovoho rehulyuvannya zakhystu krytychnoyi infrastruktury v umovakh voyennoho stanu v Ukrayini [Current issues of legal regulation of critical infrastructure protection under martial law in Ukraine]. *Problemy suchasnykh transformatsiy. Seriya: pravo, publichne upravlinnya ta administruvannya — Problems of modern transformations. Series: law, public management and administration*, 6. doi: https://doi.org/10.54929/2786-5746-2022-6-01-09 [in Ukrainian].

5. Al-Mhdawi, M. K. S., O'connor, A., Qazi, A., Rahimian, F., & Dacre, N. (2024). Review of studies on risk factors in critical infrastructure projects from 2011 to 2023. *Smart and Sustainable Built Environment, Vol. ahead-of-print No. ahead-of-print*. doi: https://doi.org/10.1108/SASBE-09-2023-0285.

6. Plakhotnyuk, R. V. (2023). Kontseptualni zasady vdoskonalennya vzayemodiyi mizh upovnovazhenymy orhanamy u sferi zakhystu krytychnoyi infrastruktury [Conceptual principles of improving interaction between authorized bodies in the field of critical infrastructure protection]. *Problemy suchasnykh transformatsiy. Seriya: pravo, publichne upravlinnya ta administruvannya — Problems of modern transformations. Series: law, public management and administration*, 7. doi: https://doi.org/10.54929/2786-5746-2023-7-01-17 [in Ukrainian].

7. Espada, R., Apan, A., & McDougall, K. (2017). 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*, 8 (4), 375–411. doi: https://doi.org/10.1108/IJDRBE-03-2015-0010.

8. Sun, J., Balakrishnan, S., & Zhang, Z. (2021). A resource allocation framework for predisaster resilience management of interdependent infrastructure networks. *Built Environment Project and Asset Management*, 11 (2), 284–303. doi: https://doi.org/10.1108/BEPAM-06-2020-0109.

9. Pro krytychnu infrastrukturu: Zakon Ukrayiny [On Critical Infrastructure: Law of Ukraine] vid 16 lystopada 2021 r. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text [in Ukrainian].

10. *Ofitsiynyy sayt Reyestru zbytkiv dlya Ukrayiny — Official website of the Register of Damages for Ukraine.* URL: https://rd4u.coe.int/uk/news [in Ukrainian].

11. Garcia-Perez, A., Sallos, M. P., & Tiwasing, P. (2023). Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective. *Journal of Intellectual Capital*, 24 (2), 465–486. doi: https://doi.org/10.1108/JIC-06-2021-0166.

12. Plakhotnyuk, R. V. (2022). Zasady ta napryamy vdoskonalennya derzhavno-pryvatnoho partnerstva u sferi zakhystu krytychnoyi infrastruktury [Principles and directions for improving public-private partnership in the field of critical infrastructure protection]. *Problemy suchasnykh transformatsiy. Seriya: pravo, publichne upravlinnya ta administruvannya — Problems of modern transformations. Series: law, public management and administration*, 6. https://doi.org/10.54929/2786-5746-2022-6-01-15 [in Ukrainian].

13. OECP. (2017). Investing in Climate, Investing in Growth. OECD Publishing, Paris. 309 p. doi: https://dx.doi.org/10.1787/9789264273528-en.

14. OECP. (2017). Getting Infrastructure Right. A framework for better governance. OECD Publishing, Paris. 93 p. doi: https://dx.doi.org/10.1787/9789264272453-en.

15. OECP. (2019). Good Governance for Critical Infrastructure Resilience, OECD Reviews of Risk Management Policies. OECD Publishing, Paris. 114 p. doi: https://doi.org/10.1787/02f0e5a0-en.

Стаття надійшла до редакції 19.07.2024