УДК 330.131.7:338.49
JEL: D81; H54; O3; O33; O5
DOI: https://doi.org/10.32983/2222-4459-2024-4-300-306

РИЗИКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ КРАЇНИ

©2024 МАГДИСЮК С. В.

УДК 330.131.7:338.49
JEL: D81; H54; O3; O33; O5

Магдисюк С. В. Ризики критичної інфраструктури країни

Мета статті – на основі опрацювання світового досвіду вдосконалити класифікацію та систематизацію ризиків критичної інфраструктури країни. Аналізуючи й узагальнюючи світові науково-практичні надбання щодо підходів до класифікації та систематизації ризиків критичної інфраструктури, було з'ясовано, що, незважаючи на дещо різні підходи до їх класифікації та систематизації, відслідковується також і певна схожість, але, з урахуванням зростання кількості та різноманітності ризиків, їх класифікація та систематизація потребує вдосконалення. У результаті дослідження було запропоновано класифікацію та систематизацію ризиків критичної інфраструктури країни, що включає низку ознак: за рівнем виникнення; за належністю до об'єктів та послуг критичної інфраструктури; за характером впливу; за джерелом виникнення; за сектором виникнення. Класифікація та систематизація ризиків є необхідною, щоб краще розробляти, планувати та впроваджувати заходи та інвестиції, які дозволять обмежити, нейтралізувати або уникнути негативних наслідків (енергетичних, соціальних, економічних тощо), що виникають через вплив ризиків. Перспективами подальших розвідок у цьому напрямі є підходи до оцінки фінансово-економічних і соціальних наслідків можливих і реальних ризиків критичної інфраструктури країни, враховуючи каскадний характер сучасних ризиків.

Ключові слова: *критична інфраструктура, загрози, ризики, класифікація, систематизація.*
Табл.: *2.* ***Бібл.:*** *21.*

Магдисюк Сергій Володимирович *– аспірант кафедри управління та адміністрування, Харківський національний університет імені В. Н. Каразіна (майдан Свободи, 4, Харків, 61022, Україна)*
E-mail: *serhij.magdisyk@student.karazin.ua*
ORCID: *https://orcid.org/0009-0002-6946-1537*

UDC 330.131.7:338.49
JEL: D81; H54; O3; O33; O5

Mahdysiuk S. V. Risks of the Country's Critical Infrastructure

The aim of the article is to improve the classification and systematization of risks of the country's critical infrastructure based on the study of world experience. Analyzing and summarizing the world's scientific and practical achievements regarding approaches to the classification and systematization of critical infrastructure risks, it was found that, despite slightly different approaches to their classification and systematization, a certain similarity is also traced, but still, taking into account the growth in the number and variety of risks, their classification and systematization need to be improved. As a result of the study, a classification and systematization of risks of the country's critical infrastructure has been proposed, which includes a number of features: by the level of occurrence; by belonging to critical infrastructure facilities and services; by the nature of the impact; by source of origin; by sector of occurrence. The classification and systematization of risks is necessary in order to better design, plan and implement measures and investments that will limit, neutralize or avoid negative consequences (energy, social, economic, etc.) arising from the impacts of risks. Prospects for further research in this direction are approaches to assessing the financial, economic and social consequences of possible and real risks to the country?s critical infrastructure, taking into account the cascading nature of modern risks.

Keywords: *critical infrastructure, threats, risks, classification, systematization.*
Tabl.: *2.* ***Bibl.:*** *21.*

Mahdysiuk Serhii V. *– Postgraduate Student of the Department of Management and Administration, V. N. Karazin Kharkiv National University (4 Svobody Square, Kharkiv, 61022, Ukraine)*
E-mail: *serhij.magdisyk@student.karazin.ua*
ORCID: *https://orcid.org/0009-0002-6946-1537*

Функціонування, відновлення та розвиток усього комплексу критичної інфраструктури, виконання функцій та надання критично важливих послуг відбувається, з певних причин, як реагування на сучасні виклики, загрози, ризики. Всі зазначені процеси так чи інакше залежать від певних явищ та подій. Тобто на функціонування, відновлення та розвиток критичної інфраструктури впливає безліч явищ і ризиків.

Сьогодні як у всьому світі, так і в нашій країні підвищуються загрози, а отже, і чутливість до значної кількості небезпек. Загрози, ризики та небезпеки техногенного та природного характеру, пандемія COVID-19, збройні конфлікти, значна активізація кіберзлочинності та багато інших загроз становлять значний ризик для країн світу загалом та України зокрема. Зазначене суттєво підвищує вразливість як окремих об'єктів та послуг, так і всього комплексу критичної інфраструктури, які на теперішній час мають велике значення для функціонування держави, суспільства та безпеки населення [2].

Враховуючи значну невизначеність, постійні зміни соціально-економічної ситуації, моніторинг

ризиків критичної інфраструктури в Україні стає особливо актуальним, а питання їх аналізу, класифікації та систематизації, як спосіб нейтралізації загроз та подолання викликів і перешкод на шляху відновлення та розвитку, потребують безперервного ґрунтовного вивчення.

За таких умов актуалізується значущість наукових доробок щодо загроз і ризиків стосовно як окремих об'єктів та послуг, так і всієї системи критичної інфраструктури країни.

Аналізу ризиків окремих економічних суб'єктів присвячено широкий пласт наукових доробок. Над питаннями ризиків критичної інфраструктури активно працювали закордонні фахівці: Карпіньяно А., Гроссо Д., Джербоні Р., Болонья А., Пурсіайнен К., Рьод Б., Теохаріду М., Джаннопулос Г. та ін.

Дослідження ризиків критичної інфраструктури України, підвищення залежності від загроз і ризиків не знайшло відображення у працях вітчизняних науковців. Тому питання аналізу, класифікації та систематизації ризиків критичної інфраструктури країни потребують наукового опрацювання та вирішення.

Метою статті є вдосконалення класифікації та систематизації ризиків критичної інфраструктури країни на основі опрацювання світового досвіду.

Дослідження аргументує такі три тези. *По-перше*, як у короткостроковій, так і в довгостроковій перспективі небезпеки, загрози та ризики критичної інфраструктури в усьому світі будуть тільки зростати. *По-друге,* незважаючи на дещо різні підходи до класифікації та систематизації ризиків критичної інфраструктури, відслідковується також і певна їх схожість, але, з урахуванням зростання кількості та різноманітності ризиків, їх класифікація та систематизація потребує розширення та вдосконалення. *По-третє,* управлінці мають підтримувати інтерес до вивчення ризиків критичної інфраструктури в умовах швидкої зміни світових тенденцій.

Спочатку розглянемо сучасні ризики критичної інфраструктури. Далі дослідимо світові підходи до класифікації та систематизації ризиків критичної інфраструктури. Нарешті, запропонуємо власний підхід до класифікації та систематизації ризиків критичної інфраструктури країни.

Аналіз ризиків у світі загалом є значно дослідженою і навіть дещо стандартизованою сферою (наприклад, ISO 31000 [9]; ISO/IEC [10]; ISO/IEC 27002:2022 [11]). Вивчення передового світового досвіду свідчить, що, наприклад, з 2013 р. держави ЄС мають проводити національну оцінку ризиків відповідно до Механізму цивільного захисту ЄС, також включаючи сферу критичної інфраструктури, значною мірою спираючись на стандарти ISO [16].

Але потреба в наукових підходах до ризиків критично важливих інфраструктур, наприклад до стихійних лих (таких як повені, землетруси, зсуви ґрунту, урагани та лісові пожежі тощо), за останні десятиліття стала актуальним питанням для країн світу загалом та ЄС зокрема. Фактично, наукові підходи до аналізу ризиків могли б дозволити розробити та реалізувати ефективні заходи для запобігання або пом'якшення негативних соціально-економічних наслідків, які можуть спричинити можливу руйнацію інфраструктури, спричинену різноманітними загрозами та ризиками (екстремальними природними явищами) [6].

Визначеність критичної інфраструктури щодо можливості ризиків, контролю за ризиками стає необхідною умовою забезпечення безпечного життя населення, громад, функціонування та розвитку держави загалом. Це вимагає усвідомленої класифікації та систематизації ризиків критичної інфраструктури, що дозволяє краще сфокусуватись на невизначеностях, з якими слід працювати.

На сьогодні можна констатувати, що як в Україні, так і у світі загалом підвищується невизначеність. Ландшафт ризиків, з якими стикаються як уряди країн, так і населення, залишається складним, багатокомпонентним. На думку іноземних фахівців [13], ландшафт ризиків критичної інфраструктури включає екологічні загрози, загрози іноземного втручання, загрози кібербезпеці, економічний тиск, кризу в галузі охорони здоров'я, ризики глобально розподілених ланцюжків постачання, які підтримують критично важливу інфраструктуру. Також до ризиків критичної інфраструктури слід віднести зміни клімату та потепління, що, за прогнозами, у майбутньому посилюватимуться. Це впливає на навколишнє середовище, економіку та здоров'я населення. Екстремальні погодні явища загрожують спроможності критично важливої інфраструктури надавати послуги, викликають збої в транспортних системах, телекомунікаційних мережах і ланцюжках поставок «в строк». Цифровізація систем і процесів, а також можливість віддаленого управління операціями критично важливої інфраструктури також посилюють наявні та створюють нові проблеми кібербезпеки. Водночас зростає впровадження систем цифрової інфраструктури поряд із традиційною фізичною інфраструктурою, що, начебто, покращує загальні можливості підключення, зв'язку та надання послуг суспільству, але використання систем з підтримкою інтернету збільшує ймовірність і масштаб як навмисних, так і ненавмисних збоїв.

Критично важлива інфраструктура будь-якої країни залишається об'єктом серйозного іноземного втручання, у тому числі з метою навмисних збоїв у роботі служб і крадіжки інтелектуальної власності. Високий рівень взаємопов'язаності критично важливих секторів інфраструктури країни створює ефект збою, що виникає в одному секторі, але зазвичай набуває каскадних наслідків для інших секторів [13]. Пандемія також виявила різні вразливості критичної інфраструктури, такі як залежність від глобально розподілених ланцюжків постачання товарів першої необхідності. Наприклад, у Канаді покладаються лише на кілька м'ясопереробних підприємств у Канаді та США щодо постачання м'яса населенню. Багато з цих об'єктів були змушені тимчасово закритися та скоротити потужності через ризики для здоров'я, тим самим підриваючи ще й продовольчу безпеку. Ще одна проблема полягає в тому, що більшість канадських фармацевтичних препаратів надходить з однієї країни, що залишає мало можливостей для відновлення в разі збою. Всі критично важливі сектори інфраструктури покладаються на товари та послуги, вироблені ланцюжками поставок, розташованими по всьому світу, за межами компетенції Канади, що може становити певні ризики [13].

Фахівці наголошують, що специфіка сучасних процесів в Україні характеризується суттєвим загостренням кризових явищ, які негативно впливають на стан економіки, на соціальний розвиток, призводячи до погіршення умов життя тощо [1]. Також, узагальнюючи сучасні виклики, ризики та небезпеки країни, можна визначити недостатність фінансування [3–5] та державної підтримки, непривабливість певних секторів, підсекторів та окремих об'єктів критичної інфраструктури для інвесторів, геополітичні ризики [1; 2], недостатність платоспроможності, низький виробничо-технічний потенціал та інші.

Тобто сучасні ризики та загрози надають нові виклики, тому має бути сформований комплексний підхід до аналізу ризиків комплексу критичної інфраструктури. Всі загрози, небезпеки та ризики необхідно моніторити, аналізувати, щоб визначати їхній вплив на критичну інфраструктуру та ймовірність їхньої реалізації. Важливим стає сфокусуватись саме на питанні класифікації та систематизації ризиків критичної інфраструктури, що розкриє додаткові можливості сформувати як практичні заходи та ефективні механізми реагування на загрози, небезпеки та ризики, так і стратегічні пріоритети щодо функціонування, відновлення та розвитку критичної інфраструктури.

Фахівці ООН надають таку класифікацію та систематизацію ризиків та загроз для системи критичної інфраструктури [19]. *Природні загрози:* геофізичні (зсуви ґрунту, землетруси, селеві потоки, обвали, цунамі, вулканічна діяльність та викиди), гідрометеорологічні (зливові паводки, повені, посухи, лавини, сильні конвективні та зимові шторми, спека та похолодання, лісові пожежі, урагани, тайфуни), біологічні (епідемії), космічні явища (метеорити, астероїди, геомагнітні бурі, сонячні спалахи). *Техногенні та антропогенні небезпеки:* промислові аварії/забруднення; масштабні відключення електроенергії; транспортні аварії; деградація та забруднення навколишнього середовища; аварії на дамбах; радіація; розливи хімічних речовин; вибухи на заводах. *Ризики для безпеки:* тероризм; ворожі уряди; розповсюдження зброї масового знищення; зміна клімату; кіберзлочинність, транснаціональна злочинність, ненадійні інвестиції; громадянські війни та конфлікти; атаки на ланцюги поставок; щільність населення.

Фахівці [8] вважають, що всі елементи критичної інфраструктури повинні проводити дослідження ризиків, оцінюючи загрози, на які вони наражаються. Цю норму включають як національні та регіональні, так і європейські та міжнародні нормативні акти, а також і галузеві нормативні акти. Фахівці [8] виокремлюють такі ризики та загрози:

- фізична безпека;
- кібербезпека;
- інформаційна безпека;
- особиста безпека;
- екологічна безпека;
- самозахист і запобігання професійним ризикам.

Для цілей ідентифікації загроз і небезпек та оцінки ризиків, а також з огляду на готовність зацікавлених сторін [20] загрози та небезпеки класифікуються за трьома категоріями:

- *природні загрози:* стихійні лиха;
- *техногенні небезпеки:* аварії або відмова систем і споруд;
- *антропогенна небезпека:* інциденти, спричинені людиною, навмисні дії супротивника.

Фахівці [7] висловлюють думки, що як природні, так і антропогенні (навмисні або випадкові) ризики та інциденти можуть пошкодити, вивести з ладу або взагалі знищити критично важливу інфраструктуру. Тому дуже небезпечно зосереджуватися на одному типі небезпек чи загроз (наприклад, таких як урагани або тероризм). Загрози, небезпеки та ризики можуть бути специфічними як для географічних регіонів, так і для всієї країни, і навіть призводити до глобальних наслідків. Пропонуєть-

ся класифікувати та систематизувати ризики таким чином:

- *кліматологічні події* (посуха, екстремальні температури, лісові пожежі);
- *гідрологічні події* (повені); метеорологічні події (тропічні циклони, сильні зимові бурі);
- *геофізичні події* (цунамі, землетруси, виверження вулканів); пандемії (глобальні спалахи захворювань);
- *події космічної погоди* (геомагнітні бурі);
- *технологічні та промислові аварії* (промислові пожежі, руйнування конструкцій, розливи хімічних речовин, викиди небезпечних речовин);
- *незаплановані збої* (несправність обладнання, старіння інфраструктури, масштабні відключення електроенергії);
- *кримінальні інциденти та терористичні атаки* (крадіжки, вандалізм, пошкодження майна, кінетичні атаки, інциденти з активними стрільцями);
- *кіберінциденти* (шкідливе програмне забезпечення, атаки на відмову в обслуговуванні, фішинг);
- *атаки на ланцюги поставок* (спричинення збою в роботі системи або мережі);
- *операції іноземного впливу* (з метою підриву демократичних процесів або поширення дезінформації);
- *ненадійні інвестиції* (можуть надати іноземним державам значний, надмірний вплив на національну критичну інфраструктуру) [7].

Фахівці зі США в Національній оцінці ризиків від 2019 р. [14] пропонують приклади загроз, небезпек і ризиків, що викликають занепокоєння (*табл. 1*).

Інші дослідники [18] запропонували підхід, розроблений на перспективу всіх небезпек і ризиків на основі системного підходу, який вводить три рівні (суспільство, активи та система) і оцінює впливи на економіку, навколишнє середовище та громадян. Згідно зі статистичними даними страхової компанії Munich Re, стосовно глобальних природних втрат у світі (включно з географічними, гідрологічними, метеорологічними та кліматологічними подіями) за період 1980–2015 рр. [12], загальні збитки у 2015 р. становили близько 0,14% від глобального ВВП (дані зі статистики Світового банку [21]). Протягом попередніх років були значно вищі збитки, зокрема у 2011 р., коли збитки досягли максимуму в 380 млрд дол. США (головним чином через цунамі в Японії та землетрус Тохоку), а також у 2005 році, головним чином через ураган Катріна в США. Такі події підкреслюють, що надзвичайні події за участю розвинених країн зазвичай призводять до більш відповідних економічних ефектів навіть у глобальному масштабі. Отже, захист критичної інфраструктури від надзвичайних небезпек, природних лих і ризиків шляхом їх аналізу стає одним із головних завдань багатьох країн або груп країн (наприклад, ЄС).

На думку фахівців [15], коли складові критичної інфраструктури об'єднуються разом, критичні елементи кожної складової стають критичними для всіх через можливість, що збій в одній частині чи одному елементі буде передано іншим. Таким чином, суб'єкти критичної інфраструктури зазвичай знають і можуть певним чином контролювати свої власні ризики, але не ризики інших складових (елементів, суб'єктів), від яких вони залежать. Існують емпіричні докази реальних збоїв критичної інфраструктури, які були спричинені взаємозалежностями між різними численними об'єктами чи секторами критичної інфраструктури. Тому була запропонована корисна класифі-

Таблиця 1

Приклади загроз і небезпек, що викликають занепокоєння

Тип загрози/ небезпеки/ ризику	Загроза/небезпека/ризик	Країна/область/регіон
Природний	Каскадні ефекти (ймовірні паралельні операції)	По всій країні
	Землетрус	Вашингтон, Орегон, Каліфорнія, Айдахо
		600 000 кв. км на Середньому Заході/ Сході
	Ураган	Галвестон, Техас на Середній Захід
		Форт-Лодердейл, Флорида до Алабами
		Гаваї
	Пандемія	По всій країні

Джерело: складено за [14].

кація. Якщо операції залежать від матеріального результату(ів) іншої складової інфраструктури через функціональний і структурний зв'язок, вони вважаються *фізичними*. Якщо операції залежать від інформації та даних, що передаються через інформаційну інфраструктуру через електронні або інформаційні канали, вони вважаються *кібер*. Якщо операції залежать від локального середовища, де подія може викликати зміни в стані операцій у кількох інфраструктурах, їх називають *географічними*. І, нарешті, якщо операції залежать від стану іншої інфраструктури через зв'язки, відмінні від фізичних, кібернетичних чи географічних, вони вважаються *логічними*, оскільки такий вид (взаємо)залежності можна віднести до людських рішень і дій, і вони не є результатом фізичних операцій чи кіберпроцесів. Хоча такі явища, як зміна клімату та нові технології, іноді призводять до неочікуваних або нових ризиків.

Також є особлива категорія ризиків, а саме, *зловмисні гібридні загрози*. Гібридні загрози зазвичай включають, наприклад, кібератаки, зловмисні прямі іноземні інвестиції, дезінформацію та автоматизовані транспортні засоби – усі вони можуть бути інструментами зловмисних дій проти критичної інфраструктури [15].

Як вважають фахівці [17], сучасні взаємопов'язані критичні інфраструктури можна згрупувати у функціональні (кібернетичні, логічні) та топологічні (фізичні, географічні).

З огляду на розширення та багатогранність переліку загроз і ризиків критичної інфраструктури важливо запропонувати їх класифікацію та систематизацію, спрямовану на критичні інфраструктури для їх вчасного реагування та захисту. Тому, узагальнюючи сучасні світові виклики та ризики, а також науково-практичні доробки в цьому напрямку, ми пропонуємо класифікацію та систематизацію ризиків критичної інфраструктури країни, що включає низку класифікаційних ознак та ризиків (*табл. 2*).

Якщо сформовано достатню інформацію про ризики критичної інфраструктури на основі запропонованої класифікації та систематизації, можна говорити про розуміння, що відбувається та які можуть бути зміни, тоді можна належним чином реагувати.

Тобто класифікація та систематизація ризиків є необхідною, щоб на основі цього краще розробляти, планувати та впроваджувати заходи та інвестиції, які дозволять обмежити, нейтралізувати або уникнути негативних наслідків (енергетичних, соціальних, економічних тощо), що виникають через вплив ризиків.

Таблиця 2

Класифікація ризиків критичної інфраструктури

Ознака	Класифікація ризиків
За рівнем виникнення	глобальні
	національні
	регіональні
	секторальні (підсекторальні)
	окремого об'єкта чи послуги
По відношенню до об'єктів та послуг критичної інфраструктури	внутрішні
	зовнішні
За характером впливу	загальні
	локальні
За джерелом виникнення	природні
	антропогенні (техногенні)
За сектором виникнення	енергетичні
	економічні
	інформаційні
	продовольчі
	екологічні
	транспортні

Джерело: авторська розробка.

ВИСНОВКИ

Дослідження, класифікація та систематизація ризиків критичної інфраструктури має бути системним процесом, який передбачає ймовірність того, що загроза (небезпека) може завдати шкоди громаді, особі, активу чи функції, що, своєю чергою, стає підґрунтям для визначення дій для зменшення ризику (загроз, небезпек) і пом'якшення наслідків.

Виявлення, аналіз, класифікація та систематизація ризиків критичної інфраструктури – це як основа розробки, так і інструмент підтримки прийняття рішень, планування безпекових заходів. Слід визначати всі ризики для критичної інфраструктури, що, своєю чергою, дозволить більш ефективно і раціонально управляти, планувати та розподіляти ресурси.

Перспективами подальших розвідок у цьому напрямі є підходи до оцінки фінансово-економічних і соціальних наслідків можливих і реальних ризиків критичної інфраструктури країни, враховуючи каскадний характер сучасних ризиків. ■

БІБЛІОГРАФІЯ

1. Колосовська І. І. Соціальні детермінанти та пріоритети розвитку публічного управління. *Право*

та державне управління. 2021. № 2. С. 281–284. DOI: https://doi.org/10.32840/pdu.2021.2.42
2. Кузьменко Є. Занадто критична інфраструктура. *Юридична газета*. 2021. № 20. URL: https://yurgazeta.com/publications/practice/transportne-pravo/zanadto-kritichna-infrastruktura.html
3. Кульомза Д. Р., Портна О. В. Світовий досвід фінансового управління компаніями: стейкхолдери підвищення його ефективності. *Бізнес Інформ*. 2019. № 12. С. 403–408. DOI: https://doi.org/10.32983/2222-4459-2019-12-403-408
4. Портна О. В., Дереза Б. П. Вплив стану національної економіки на запровадження антикризового управління на підприємствах. *Бізнес Інформ*. 2020. № 1. С. 352–359. DOI: https://doi.org/10.32983/2222-4459-2020-1-352-359
5. Портна О. В. Фінансова стабільність як індикатор ефективності управління змінами в усіх сферах національної фінансово-економічної системи. *Соціальна економіка*. 2018. Вип. № 56. С. 50–55.
6. Carpignano A., Gerboni R., Grosso D., Bologna, A. Resilience of Critical Infrastructures: A Risk Assessment Methodology for Energy Corridors. In: *Issues on Risk Analysis for Critical Infrastructure Protection*. 2020. DOI: https://doi.org/10.5772/intechopen.94755
7. A Guide to Critical Infrastructure Security and Resilience. CISA. November 2019. URL: https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf
8. Перелік документів міжнародних організацій у сфері захисту критичної інфраструктури. *Державна служба спеціального зв'язку та захисту інформації*. 2023. URL: https://cip.gov.ua/ua/news/perelik-dokumentiv-mizhnarodnikh-organizacii-u-sferi-zakhistu-kritichnoyi-infrastrukturi
9. ISO 31000. Risk management – guidelines. 2018. URL: https://www.iso.org/iso-31000-risk-management.html
10. ISO/IEC. Risk management – risk assessment techniques. Edition 2.0. IEC 31010: 2019. URL: https://www.iso.org/standard/72140.html
11. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection. Information security controls. 2022. URL: https://www.iso.org/standard/75652.html
12. Loss events worldwide 1980–2015. *Münchener Rückversicherungs-Gesellschaft*. 2016. URL: https://www.preventionweb.net/publication/loss-events-worldwide-1980-2015
13. National Cross Sector Forum 2021–2023 Action Plan for Critical Infrastructure. *Public Safety Canada*. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/index-en.aspx
14. National Threat and Hazard Identification and Risk Assessment (THIRA) Overview and Methodology. *Domestic Preparedness*. 2019. URL: https://domprep.com/reports/2019-national-threat-and-hazard-identification-and-risk-assessment-thira-overview-and-methodology
15. Pursiainen C., Kytömaa E. From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure*. 2023. Vol. 8. Iss. Sup. 1. P. 85–101. DOI: https://doi.org/10.1080/23789689.2022.2128562
16. Pursiainen C., Rød B. National disaster risk assessments in Europe. How comparable are they and why? *Risk, Hazards & Crisis in Public Policy*. 2021. Vol. 12. Iss. 2. P. 194–214. DOI: https://doi.org/10.1002/rhc3.12215
17. Giannopoulos G., Flippini R., Schimmer M. Risk assessment methodologies for critical infrastructure protection. Part I: A state of the art. Workshop proceedings 25–26 April 2012. Ranco, Italy. URL: https://op.europa.eu/en/publication-detail/-/publication/3d4a53c4-3d43-4ce2-a36f-32bdfc2949cb/language-en
18. Theocharidou M., Giannopoulos G. Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. Luxembourg : Publications Office of the European Union, 2015. DOI: https://doi.org/10.2788/621843
19. Guidance notes on building critical infrastructure resilience in Europe and Central Asia. *UNDP*. 2022. URL: https://www.undp.org/eurasia/publications/guidance-notes-building-critical-infrastructure-resilience-europe-and-central-asia
20. Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide. Comprehensive Preparedness Guide (CPG). 3rd Edition. May 2018. URL: https://www.govinfo.gov/app/details/GOVPUB-HS-PURL-gpo146632
21. World Bank statistical database. 2020. URL: https://databank.worldbank.org/

REFERENCES

"A Guide to Critical Infrastructure Security and Resilience". *CISA*. November 2019. https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf

Carpignano, A. et al. "Resilience of Critical Infrastructures: A Risk Assessment Methodology for Energy Corridors". In: *Issues on Risk Analysis for Critical Infrastructure Protection*, 2020. DOI: https://doi.org/10.5772/intechopen.94755

"Guidance notes on building critical infrastructure resilience in Europe and Central Asia". *UNDP*. 2022. https://www.undp.org/eurasia/publications/guidance-notes-building-critical-infrastructure-resilience-europe-and-central-asia

Giannopoulos, G., Flippini, R., and Schimmer, M. "Risk assessment methodologies for critical infrastructure protection. Part I: A state of the art". *Workshop proceedings* April 25-26, 2012. Ranco, Italy. https://op.europa.eu/en/publication-detail/-/

publication/3d4a53c4-3d43-4ce2-a36f-32bdfc2949cb/language-en

"ISO 31000. Risk management – guidelines". 2018. https://www.iso.org/iso-31000-risk-management.html

"ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection. Information security controls". https://www.iso.org/standard/75652.html

"ISO/IEC. Risk management – risk assessment techniques. Edition 2.0. IEC 31010: 2019". https://www.iso.org/standard/72140.html

Kolosovska, I. I. "Sotsialni determinanty ta priorytety rozvytku publichnoho upravlinnia" [Social Determinants and Priorities for the Public Administration Development]. *Pravo ta derzhavne upravlinnia*, no. 2 (2021): 281-284.
DOI: https://doi.org/10.32840/pdu.2021.2.42

Kulomza, D. R., and Portna, O. V. "Svitovyi dosvid finansovoho upravlinnia kompaniiamy: steikkholdery pidvyshchennia yoho efektyvnosti" [Global Experience in Financial Management of Companies: Stakeholders which Increase its Efficiency]. *Biznes Inform*, no. 12 (2019): 403-408.
DOI: https://doi.org/10.32983/2222-4459-2019-12-403-408

Kuzmenko, Ye. "Zanadto krytychna infrastruktura" [Too Critical Infrastructure]. *Yurydychna hazeta*. 2021. https://yur-gazeta.com/publications/practice/transportne-pravo/zanadto-kritichna-infrastruktura.html

"Loss events worldwide 1980-2015". *Munchener Ruckversicherungs-Gesellschaft*. 2016. https://www.preventionweb.net/publication/loss-events-worldwide-1980-2015

"National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure". *Public Safety Canada*. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/index-en.aspx

"National Threat and Hazard Identification and Risk Assessment (THIRA) Overview and Methodology". *Domestic Preparedness*. 2019. https://domprep.com/reports/2019-national-threat-and-hazard-identification-and-risk-assessment-thira-overview-and-methodology

"Perelik dokumentiv mizhnarodnykh orhanizatsii u sferi zakhystu krytychnoi infrastruktury" [List of Documents of International Organizations in the Field of Critical Infrastructure Protection]. *Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii*. 2023. https://cip.gov.ua/ua/news/perelik-dokumentiv-mizhnarodnikh-organizacii-u-sferi-zakhistu-kritichnoyi-infrastrukturi

Portna, O. V. "Finansova stabilnist yak indykator efektyvnosti upravlinnia zminamy v usikh sferakh natsionalnoi finansovo-ekonomichnoi systemy" [Financial Stability as an Indicator of the Effectiveness of Change Management in all Areas of the National Financial and Economic System]. *Sotsialna ekonomika*, no. 56 (2018): 50-55.

Portna, O. V., and Dereza, B. P. "Vplyv stanu natsionalnoi ekonomiky na zaprovadzhennia antykryzovoho upravlinnia na pidpryiemstvakh" [The Influence of the Status of the National Economy on the Application of Crisis Management in Enterprises]. *Biznes Inform*, no. 1 (2020): 352-359.
DOI: https://doi.org/10.32983/2222-4459-2020-1-352-359

Pursiainen, C., and Kytomaa, E. "From European critical infrastructure protection to the resilience of European critical entities: what does it mean?" *Sustainable and Resilient Infrastructure*, vol. 8, no. 1 (2023): 85-101.
DOI: https://doi.org/10.1080/23789689.2022.2128562

Pursiainen, C., and Rod, B. "National disaster risk assessments in Europe. How comparable are they and why?" *Risk, Hazards & Crisis in Public Policy*, vol. 12, no. 2 (2021): 194-214.
DOI: https://doi.org/10.1002/rhc3.12215

"Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide. Comprehensive Preparedness Guide (CPG)". May 2018. https://www.govinfo.gov/app/details/GOVPUB-HS-PURL-gpo146632

Theocharidou, M., and Giannopoulos, G. *Risk assessment methodologies for critical infrastructure protection*. Part II: A new approach. Luxembourg: Publications Office of the European Union, 2015.
DOI: https://doi.org/10.2788/621843

World Bank statistical database. 2020. https://databank.worldbank.org/

Науковий керівник – Портна О. В., доктор економічних наук, професор, професор кафедри управління та адміністрування, Харківський національний університет імені В. Н. Каразіна