

alyze the Development State of the EU and Ukraine IT Sector. *Visnyk Khmelnytskoho natsionalnoho universytetu*, 6, 429–436. <https://doi.org/10.31891/2307-5732-2023-329-6-429-436>

Chesnokova N. V. (2020). Metodolohichni pidkhody do otsinky tsyfrovoy transformatsii ekonomiky [Methodological approaches to the assessment of digital transformation of the economy]. *Rynkova ekonomika: suchasna teoriia i praktyka upravlinnia*, 2(19), 413–427. [https://doi.org/10.18524/2413-9998/2020.2\(45\).201932](https://doi.org/10.18524/2413-9998/2020.2(45).201932)

De Rojas F. H., Pita P. R. & Martinez J. E. P. (2024). Assessing the European association between digitalization and innovation. *Telecommunications Policy*, 7(48). <https://doi.org/10.1016/j.telpol.2024.102810>

Duarte M. P., Pereira F. M. & de Carvalho O. (2024). How digital transformation shapes European union countries' national systems of innovation: A configurational moderation approach. *Journal of Innovation & Knowledge*, 4(9). <https://doi.org/10.1016/j.jik.2024.100578>

European Commission. *The Digital Economy and Society Index (DESI)*. <https://digital-strategy.ec.europa.eu/en/policies/desi>

European Commission. *Digital Decade Policy Programme 2030*. <https://digital-strategy.ec.europa.eu/en/library/digital-decade-policy-programme-2030>

Eurostat. *Database*. <https://ec.europa.eu/eurostat/data/database>

Stavytskyy A., Kharlamova G. & Stoica E. A. (2019). The analysis of the digital economy and society index in the EU. *TalTech Journal of European Studies*, 3(9), 245–261. <https://doi.org/10.1515/bjes-2019-0032>

Strutynska I. (2019). Metryky tsyfrovoy transformatsii biznesu: svitovi ta vitchyzniani realii [Metrics of business digital transformation: world and domestic realities]. *Halytskyi ekonomichnyi visnyk*, 6, 30–45. https://doi.org/10.33108/galicianvisnyk_tntu2019.06.030

2030 digital compass: *The European way for the digital decade*. <https://op.europa.eu/en/publication-detail/-/publication/d4220021-8d20-11eb-b85c-01aa75ed71a1/language-en>

Стаття надійшла до редакції / Received: 23.02.2026
Статтю прийнято до публікації / Accepted: 07.03.2026
Оприлюднено / Published: 30.04.2026

УДК 351.82:338.2:339.9:005.3

JEL: D81; H54; H83; R58

DOI: <https://doi.org/10.32983/2222-4459-2026-3-113-127>

РЕЗИЛЬЄНТНІСТЬ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА МУНІЦИПАЛЬНОМУ РІВНІ: ДОСВІД ГМІН ПОЛЬЩІ*

©2026 ХАУСТОВА В. Є., ТРУШКІНА Н. В., КАЛАШНІКОВА К. Ю.

УДК 351.82:338.2:339.9:005.3

JEL: D81; H54; H83; R58

Хаустова В. Є., Трушкіна Н. В., Калашнікова К. Ю. Резильєнтність критичної інфраструктури на муніципальному рівні: досвід гмін Польщі

У статті здійснено дослідження й аналітичне узагальнення досвіду гмін Польщі щодо забезпечення резильєнтності критичної інфраструктури на муніципальному рівні в умовах зростання природних, техногенних, кібернетичних і гібридних загроз. Обґрунтовано, що сучасний підхід до управління критичною інфраструктурою поступово зміщується від об'єктно-орієнтованої логіки захисту інфраструктурних елементів до сервісної логіки управління безперервністю життєво важливих послуг, які безпосередньо визначають соціально-економічну стійкість територіальних громад. Показано, що на муніципальному рівні резильєнтність критичної інфраструктури формується як інтегрована система публічного управління, у межах якої гміна, не будучи оператором інфраструктурних мереж, виконує ключові координуючі, організаційну та комунікаційну функції. На основі аналізу інституційної архітектури кризового управління в Польщі визначено роль гмін у забезпеченні готовності, реагування та відновлення життєво важливих послуг у взаємодії з операторами, екстремими службами та населенням. Наведено практичні приклади муніципального управління резильєнтністю у Варшаві, Вроцлаві та Кракові, які демонструють значущість завчасно підготовлених механізмів оповіщення, мережевої координації на локальному рівні, інституційної визначеності кризових функцій і чітких регламентів реагування. Доведено, що ефективна резильєнтність на рівні гмін базується на поєднанні інституційної чіткості багаторівневого управління, сервісно орієнтованого планування, стійкої міжвідомчої взаємодії, сценарного підходу до реагування та використання вимірюваних показників готовності, реагування та відновлення. Запропоновано систему ключових показників ефективності (КПІ), яка забезпечує регулярний моніторинг резильєнтності життєво важливих послуг, проведення внутрішнього аудиту управлінських практик і міжмуніципальних порівнянь. Сформульовано практичні рекомендації щодо забезпечення резильєнтності критичної інфраструктури на муніципальному рівні, що передбачають інституційне посилення ролі гміни в досягненні безперервності життєво важливих послуг; застосування сервісно орієнтованого підходу до планування; розвиток мережевої взаємодії та кризової координації; використання сценарного й антикризового підходів в управлінні; запровадження системи моніторингу та оцінювання резильєнтності; зміцнення людського та організаційного потенціалу місцевого самоврядування. Обґрунтовано, що польський досвід є релевантним для України з огляду на децентралізовану модель управління та актуальність забезпечення безперервності базових сервісів в умовах воєнних дій і повоєнного відновлення.

Ключові слова: національна економіка; критична інфраструктура; резильєнтність; муніципальний рівень; гміни; життєво важливі послуги; публічне управління; безперервність послуг; загрози, кризове управління; ризик-менеджмент; мережева взаємодія; сценарне планування; показники резильєнтності; просторовий розвиток; місцеве самоврядування; територіальні громади; комплексний підхід; ефективність; сталий розвиток.
Tabl.: 5. **Bibl.:** 36.

Хаустова Вікторія Євгенівна – доктор економічних наук, професор, директор Науково-дослідного центру індустріальних проблем розвитку НАН України (пров. Інженерний, 1а, 2 пов., Харків, 61166, Україна)

E-mail: v.khaust@gmail.com

ORCID: <https://orcid.org/0000-0002-5895-9287>

Researcher ID: <https://www.webofscience.com/wos/author/record/629132>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57216123094>

Трушкіна Наталія Валеріївна – кандидат економічних наук, старший науковий співробітник, старший науковий співробітник сектора промислової політики та інноваційного розвитку відділу промислової політики та енергетичної безпеки, Науково-дослідний центр індустріальних проблем розвитку НАН України (пров. Інженерний, 1а, 2 пов., Харків, 61166, Україна)

E-mail: trushkina@nas.gov.ua

ORCID: <https://orcid.org/0000-0002-6741-7738>

Researcher ID: <https://www.webofscience.com/wos/author/record/894686>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57210808778>

Калашнікова Катерина Юріївна – аспірантка Науково-дослідного центру індустріальних проблем розвитку НАН України (пров. Інженерний, 1а, 2 пов., Харків, 61166, Україна)

E-mail: Kalashnikova2903@gmail.com

ORCID: <https://orcid.org/0009-0008-4619-9947>

UDC 351.82:338.2:339.9:005.3

JEL: D81; H54; H83; R58

Khaustova V. Yu., Trushkina N. V., Kalashnikova K. Yu. Resilience of Critical Infrastructure at the Municipal Level: Experience of Polish Gminas

The article examines and analytically summarizes the experience of Polish gminas in ensuring the resilience of critical infrastructure at the municipal level in the context of increasing natural, man-made, cyber, and hybrid threats. It is substantiated that the modern approach to managing critical infrastructure is gradually shifting from an object-oriented logic of protecting infrastructure elements to a service-oriented logic of managing the continuity of vital services, which directly determine the socioeconomic stability of territorial communities. It is shown that at the municipal level, the resilience of critical infrastructure is formed as an integrated system of public governance, within which the gmina, without being an operator of infrastructure networks, performs the key coordinating, organizational, and communication functions. Based on the analysis of the institutional architecture of crisis management in Poland, the role of gminas in ensuring preparedness, response, and recovery of vital services in cooperation with operators, emergency services, and the population has been identified. Practical examples of municipal resilience management in Warsaw, Wrocław, and Kraków are provided, which demonstrate the importance of pre-prepared alert mechanisms, network coordination at the local level, institutional clarity of crisis functions, and clear response regulations. It has been proved that efficient resilience at the gmina level is based on a combination of institutional clarity of multilevel governance, service-oriented planning, sustainable interagency interaction, a scenario-based approach to response, and the use of measurable indicators of preparedness, response, and recovery. A system of key performance indicators (KPI) has been proposed, which ensures regular monitoring of the resilience of vital services, conducting internal audits of management practices, and inter-municipal comparisons. Practical recommendations have been formulated for ensuring the resilience of critical infrastructure at the municipal level, which include institutional strengthening of the gmina's role in achieving continuity of vital services; applying a service-oriented approach to planning; developing network interaction and crisis coordination; using scenario and crisis management approaches in administration; implementing a system for monitoring and evaluating resilience; and strengthening the human and organizational capacity of local self-government. It is substantiated that the Polish experience is relevant for Ukraine given the decentralized management model and the importance of ensuring continuity of basic services in the context of military actions and postwar recovery.

Keywords: national economy; critical infrastructure; resilience; municipal level; gminas; vital services; public administration; continuity of services; threats; crisis management; risk management; network interaction; scenario planning; resilience indicators; spatial development; local self-government; territorial communities; integrated approach; efficiency; sustainable development.

Tabl.: 5. **Bibl.:** 36.

Khaustova Viktoriia Ye. – D. Sc. (Economics), Professor, Director of the Research Centre for Industrial Problems of Development of NAS of Ukraine (2 floor 1a Inzhenernyi Ln., Kharkiv, 61166, Ukraine)

E-mail: v.khaust@gmail.com

ORCID: <https://orcid.org/0000-0002-5895-9287>

Researcher ID: <https://www.webofscience.com/wos/author/record/629132>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57216123094>

Trushkina Nataliia V. – PhD (Economics), Senior Research Fellow, Senior Research Fellow of the Sector of Industrial Policy and Innovative Development of the Department of Industrial Policy and Energy Security, Research Centre for Industrial Problems of Development of NAS of Ukraine (2 floor 1a Inzhenernyi Ln., Kharkiv, 61166, Ukraine)

E-mail: trushkina@nas.gov.ua

ORCID: <https://orcid.org/0000-0002-6741-7738>

Researcher ID: <https://www.webofscience.com/wos/author/record/894686>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57210808778>

Kalashnikova Kateryna Yu. – Postgraduate Student of the Research Centre for Industrial Problems of Development of NAS of Ukraine (2 floor 1a Inzhenernyi Ln., Kharkiv, 61166, Ukraine)

E-mail: Kalashnikova2903@gmail.com

ORCID: <https://orcid.org/0009-0008-4619-9947>

В умовах зростання частоти та комплексності природних, техногенних і гібридних загроз [1] критична інфраструктура (КІ) дедалі більше розглядається не лише як сукупність об'єктів, що потребують охорони, а як система життєво важливих послуг [2], безперервність яких визначає соціально-економічну стійкість територій та довіру населення до публічної влади. У цьому контексті ключовою стає концепція резильєнтності [3; 4] – здатності систем критичної інфраструктури передбачати, витримувати, адаптуватися та відновлюватися після руйнівних впливів із мінімізацією наслідків для населення та економіки. Європейський регуляторний дискурс також фіксує зміщення акценту від охорони об'єктів до забезпечення стійкості критичних суб'єктів і безперервності суспільно значущих сервісів, що відображено в Директиві (ЄС) 2022/2557 щодо резильєнтності критичних суб'єктів [5].

Резильєнтність критичної інфраструктури має найбільш відчутний управлінський вимір саме на локальному (муніципальному) рівні, оскільки органи місцевого самоврядування забезпечують організацію та координацію електро- і теплопостачання, водопостачання та водовідведення, транспортної доступності, зв'язку, роботи закладів охорони здоров'я та інших сервісів, без яких громада не може функціонувати у кризових умовах. З практичної точки зору це означає необхідність інституційно закріплених процедур взаємодії з операторами критичної інфраструктури, наявності планів безперервності та відновлення, регулярних навчань і перевірок готовності, а також дієвих каналів кризової комунікації з населенням. Саме такі інструменти перетворюють резильєнтність із декларативної характеристики на керовану спроможність громади підтримувати життєво важливі послуги в умовах збоїв і атак [5].

Польща є показовою країною для аналізу муніципальних механізмів резильєнтності критичної інфраструктури з огляду на масштаб і структурованість базового рівня місцевого самоврядування. За офіційними статистичними даними Statistics Poland, адміністративно-територіальна структура Польщі охоплює 16 воєводств, 314 повітів, 66 міст на правах повіту та 2477 гмін, а чисельність населення становить 37 489 тис. осіб [6]. Це означає, що результативність загальнодержавних підходів до

стійкості критичних сервісів значною мірою визначається реальними управлінськими практиками гмін – їхньою спроможністю інтегрувати вимоги безпеки та безперервності в просторове планування, розвиткові програми та кризове управління [6].

Актуальність проблематики підсилюється зростанням інтенсивності подій, які прямо або опосередковано впливають на інфраструктурні системи та муніципальні послуги. За офіційним статистичним підсумком Команди Головної Державної пожежної служби Польщі [7], у 2024 році зафіксовано понад 550 тис. інтервенцій, з яких 394 тис. становили місцеві загрози; 103 тис. – пожежі; 53 тис. – хибні виклики. Окремо наголошено, що понад 29 тис. інтервенцій було пов'язано з катастрофічною повинню на півдні Польщі [7]. Такі масштаби подій формують постійне навантаження на системи життєзабезпечення та актуалізують питання локальної готовності, резервування та відновлення – тобто тих компонентів, які й утворюють практичний каркас резильєнтності критичної інфраструктури на рівні гмін [7].

Крім цього, варто зазначити й про кібер- і гібридні загрози для критичних сервісів. Так, у щорічному звіті CERT Polska [8] зафіксовано 147 інцидентів, пов'язаних з атаками програм-вимагачів у 2024 році, що свідчить про стійкість цього класу кіберзагроз для організацій і сервісів, які потенційно належать до критичної інфраструктури. Публічні оцінки [9; 10] також вказують на інтенсивність спроб втручання саме в інфраструктурні системи: зокрема, у 2025 році в повідомленнях про протидію кібератакам зазначалося про спроби ураження лікарень і міських систем водопостачання, а також про те, що кількість спроб може сягати десятків на добу.

Окремо повідомлялося про запобігання кібератаці, яка могла спричинити зупинку водопостачання у великому місті, а також про те, що переважну більшість атак вдається нейтралізувати завдяки швидкому реагуванню [11]. Сукупність таких фактів підкреслює, що резильєнтність критичної інфраструктури на муніципальному рівні дедалі більше залежить не лише від фізичного захисту, а й від організаційних і кіберстійких практик управління послугами [8; 10].

Інституційна організація політики захисту та стійкості критичної інфраструктури в Польщі ґрунтується на багаторівневій моделі кризового менеджменту, де координуючу та програмну роль відіграє Government Centre for Security (RCB). У 2023 році розпочалася реалізація Національної програми захисту критичної інфраструктури [12], у якій визначено рамкові цілі запобігання порушенням, підготовки до криз, реагування на по-

* Наукову статтю підготовлено завдяки грантовій підтримці Національного фонду досліджень України в рамках реалізації проекту «Розбудова резильєнтних розподілених енергетичних систем територіальних громад України» (реєстраційний № 2025.07/0056), який відібрано для виконання за конкурсом «Передова наука в Україні 2026–2028».

шкодження/збої та відновлення функціональності критично важливих об'єктів і послуг. Водночас прикладна результативність цих підходів значною мірою зумовлюється тим, як саме гміни організують взаємодію з операторами, впроваджують стандарти безперервності, вибудовують комунікацію з населенням і забезпечують готовність до подій різної природи [12].

Отже, актуальність обраної тематики дослідження визначається поєднанням трьох факторів: 1) інституційною вагою гмін як базової ланки забезпечення життєво важливих послуг у країні з масштабною територіальною структурою [6]; 2) високою частотою надзвичайних подій та інтервенцій, що створюють системне навантаження на інфраструктурні сервіси й потребують від місцевого управління застосування дієвих механізмів готовності та відновлення [7]; 3) інтенсифікацією кібер- і гібридних загроз для критичних сервісів, що підвищує значущість локальних інструментів координації, кіберстійкості та безперервності [8–11].

При цьому слід зазначити, що аналітичне узагальнення польських муніципальних практик у цій сфері має прикладну цінність і для України, оскільки створює основу для адаптації управлінських рішень у територіальних громадах з урахуванням безпекових ризиків та потреби забезпечення безперервності базових послуг.

Аналіз останніх досліджень і публікацій. Як свідчить аналіз джерел, сучасний науковий дискурс щодо критичної інфраструктури дедалі виразніше зміщується від вузького підходу «захист об'єктів» до ширшої логіки «резильєнтність життєво важливих послуг», у межах якої ключовими стають безперервність надання сервісів, здатність до адаптації та відновлення після інцидентів. Це, своєю чергою, цілком відповідає сучасним підходам до управління ризиками та кризової готовності.

У цьому контексті дослідники підкреслюють, що резильєнтність критичної інфраструктури формується не лише технічними характеристиками мереж і потужностей, а й інституційною архітектурою управління, якістю координації, процедурою планування та зрілістю кризового менеджменту. Зокрема, у працях з урбаністичних студій показано, що управління ризиками інфраструктур у містах дедалі частіше здійснюється через мережеві, багатосторонні моделі взаємодії між муніципалітетами, операторами та регуляторами, а не через лінійні адміністративні схеми [13; 14]. Це створює підстави розглядати муніципальний рівень як не допоміжний, а системоутворювальний елемент резильєнтності критичної інфраструктури, оскільки

саме тут поєднуються просторове планування, управління послугами, комунікація з населенням і практики реагування на надзвичайні події [13].

Окремий напрям досліджень становлять методичні підходи до оцінювання резильєнтності взаємозалежних інфраструктур. У техніко-економічних роботах наголошується, що вразливість мереж не може оцінюватися ізольовано, оскільки відмова одного компонента запускає каскадні ефекти в суміжних системах (енергія – зв'язок – транспорт – водопостачання тощо). Для цього застосовують моделі динамічних мережевих потоків, сценарне моделювання та інструменти, які дозволяють кількісно оцінювати стійкість і відновлюваність у різних режимах порушень [15]. Такі підходи є важливими для муніципального управління насамперед як аналітична основа визначення критичних вузлів, пріоритетів резервування та критеріїв готовності (зокрема, часу відновлення, допустимих рівнів переривань, пріоритетності споживачів), що надалі може трансформуватися у практичні управлінські рішення на рівні громади [15–18].

Суттєвий пласт публікацій присвячено інституційним і фінансовим механізмам підвищення резильєнтності, зокрема в умовах обмежених ресурсів та різного рівня спроможності місцевої влади. У роботах з управління ризиками й урбаністичної резильєнтності підкреслюється, що ефективність політики залежить від узгодженості багаторівневого управління, наявності стабільних фінансових інструментів (програм модернізації, інвестиційних стимулів, фондів відновлення), а також від інституційної визначеності відповідальності між державою, регіоном і муніципалітетом [19]. Водночас емпіричні приклади свідчать, що там, де муніципалітет виступає активним інтегратором – узгоджує правила взаємодії з операторами, посилює планування безперервності, організовує навчання та розбудовує канали кризової комунікації, – резильєнтність інфраструктур має більш керований характер [14]. Зазначені підходи є особливо релевантними для аналізу гмін Польщі, де базовий рівень місцевого самоврядування поєднує управління життєво важливими послугами з реалізацією рамкових вимог національної політики у сфері критичної інфраструктури.

Дослідження, які орієнтовано на муніципальних акторів, акцентують увагу на операційному середовищі місцевої влади у сфері розвитку критичної інфраструктури, яке характеризується поєднанням юридичних повноважень, відповідальності за надання послуг, залежності від приватних і державних операторів та необхідності діяти в умовах неповної інформації та часових обмежень. У цьому сенсі

для місцевих органів влади резильєнтність критичної інфраструктури означає не стільки управління інфраструктурою як сукупністю активів, скільки управління доступністю та якістю послуг – через контракти, протоколи взаємодії, кризові плани та організаційні спроможності [20]. Цей висновок є принципово важливим для формування аналітичної рамки дослідження гмін Польщі, оскільки зумовляє фокус саме на управлінських механізмах безперервності та готовності, а не на переліку об'єктів або технічних характеристиках мереж.

Варто відзначити, що в контексті порушень енергопостачання дослідники показують, наскільки локальний рівень є критичним для мінімізації соціально-економічних наслідків перебоїв. Це обумовлено тим, що саме тут визначаються пріоритети критичних споживачів, організовується взаємодія служб, координуються тимчасові рішення та здійснюється інформування населення. Так, на прикладі порівняльного аналізу двох муніципалітетів у Швеції продемонстровано, що планування резильєнтності в разі збоїв електропостачання значною мірою залежить від узгодженості місцевих процедур, взаємодії з операторами та якості міжвідомчої координації [21]. Схожі висновки отримано й у дослідженнях практик реагування на перебої електропостачання в уразливих спільнотах, де наголошується, що сталість сервісів визначається не лише ресурсною базою, а й локальними соціально-інституційними практиками, рівнем довіри та ефективністю комунікації [22]. Для гмін Польщі це відкриває важливий напрям аналізу поєднання інженерних рішень (резервування, альтернативні джерела) з управлінськими інструментами (плани, протоколи, навчання).

Окремої уваги заслуговують публікації, у яких розвивається підхід безперервності життєво важливих послуг як одна з провідних концептуальних рамок резильєнтності критичної інфраструктури. Зокрема, у роботі [23] підкреслюється, що фокус на сервісах дозволяє краще пов'язати технічні рішення з потребами населення, стандартизувати вимоги до готовності та перевести управління резильєнтністю у вимір конкретних показників, таких як час відновлення, допустимий рівень переривань і пріоритизація послуг. Такий підхід методологічно узгоджується із завданням узагальнення польського досвіду гмін, оскільки дозволяє структуровано описувати муніципальні механізми в зіставних категоріях.

Поряд із цим, у частині управлінських аспектів резильєнтності критичної інфраструктури простежується стійкий інтерес до проблематики локального врядування, порівняння муніципальних підходів та організаційних моделей. Дослідження

локального врядування резильєнтності підкреслюють, що міста та муніципалітети по-різному інтерпретують межі відповідальності, обирають інструменти та вибудовують взаємодію з операторами, що потребує систематизації моделей і практик для подальшого поширення найкращих рішень [24]. Водночас роботи з організаційної резильєнтності критичних систем узагальнюють інструменти менеджменту – навчання, аудит готовності, стандарти процедур, управління знаннями, – які можуть застосовуватися для підвищення готовності операторів і органів влади до кризових подій [25].

З огляду на посилення цифрових загроз, у літературі активно розвивається й напрям кіберрезильєнтності місцевого самоврядування. Наголошується, що локальні органи влади часто мають обмежені ресурси та неоднорідний рівень цифрової зрілості, що підвищує вразливість муніципальних сервісів і зумовляє необхідність стандартизованих процедур управління інцидентами, резервування даних і координації з національними структурами реагування [26]. У міждисциплінарних роботах також підкреслюється важливість багатозагрозового (*multi-hazard*) підходу, який дозволяє планувати готовність не під окремі типи подій, а під сукупність ризиків, характерних для конкретної території [27]. Для гмін Польщі це є особливо актуальним з огляду на поєднання техногенних, природних і кіберризиків, що впливають на муніципальні послуги.

Таким чином, аналіз сучасних наукових публікацій засвідчує наявність розвинених підходів до теоретичного осмислення резильєнтності життєво важливих послуг, кількісного оцінювання стійкості взаємозалежних інфраструктур, а також до вивчення інституційних, фінансових і організаційних механізмів підвищення готовності інфраструктурних систем до кризових впливів. Значна частина досліджень зосереджується на багаторівневому врядуванні, мережевих моделях взаємодії та управлінських інструментах, що формують спроможність систем до адаптації та відновлення. Водночас ці підходи переважно розглядаються або на загальнодержавному рівні, або в контексті окремих міст і секторів, без належної уваги до базового муніципального рівня як самостійного суб'єкта формування та забезпечення резильєнтності.

У межах наявних наукових напрацювань недостатньо систематизовано питання того, яким чином органи місцевого самоврядування базового рівня інтегрують підходи резильєнтності у практику управління життєво важливими послугами, а також за допомогою яких управлінських механізмів, процедур взаємодії з операторами, інструментів планування безперервності, навчання персоналу

та кризової комунікації з населенням. Особливо виразною є ця прогалина в дослідженнях, присвячених країнам із розвинутою системою місцевого самоврядування, де саме муніципальний рівень відіграє ключову роль у забезпеченні безперервності життєво важливих послуг.

З огляду на це, відсутність комплексних узагальнень досвіду гмін Польщі як базового рівня управління обмежує можливості ідентифікації типових інституційних моделей, набору управлінських інструментів і практик, а також оцінювання їх ефективності з позицій забезпечення резильєнтності критичної інфраструктури. Заповнення окресленої наукової прогалини шляхом аналітичного узагальнення досвіду гмін Польщі створює підґрунтя для формування цілісної управлінської моделі резильєнтності критичної інфраструктури на муніципальному рівні та відкриває можливості для адаптації релевантних інституційних і практичних рішень у діяльності територіальних громад України.

Мета та методологія дослідження. *Метою* статті є дослідження й аналітичне узагальнення досвіду гмін Польщі щодо забезпечення резильєнтності критичної інфраструктури на муніципальному рівні шляхом ідентифікації інституційних, організаційних та управлінських механізмів функціонування життєво важливих послуг в умовах природних, техногенних, кібернетичних і гібридних загроз, а також визначення можливостей імплементації цього досвіду в діяльності територіальних громад України.

Досягнення поставленої мети зумовило застосування комплексного *методологічного підходу*, що поєднує інституційний, порівняльний і структурно-логічний аналіз і спирається на сучасні теоретичні уявлення про резильєнтність життєво важливих послуг. У межах такого підходу муніципальний рівень розглядається як ключова ланка забезпечення стійкості базових сервісів незалежно від форми власності та організаційної підпорядкованості інфраструктурних об'єктів.

У процесі дослідження використано методи аналізу та синтезу, інституційного аналізу, порівняльно-аналітичний метод, контент-аналіз нормативних і програмних документів, а також логіко-структурний метод. Їх поєднання дозволило систематизувати наукові підходи до розуміння резильєнтності критичної інфраструктури, окреслити роль і повноваження гмін у системі багаторівневого управління в Польщі, зіставити управлінські практики в різних сферах життєво важливих послуг і сформувані аналітичну рамку для узагальнення отриманих результатів.

Методологічна логіка дослідження вибудована як послідовний аналітичний процес, у межах якого концептуальні положення щодо резильєнтності критичної інфраструктури поступово трансформуються в інструментальний рівень муніципального управління. Такий підхід дозволяє розглядати гміни не лише як виконавчу ланку в системі реагування на загрози, а як активних суб'єктів формування локальної архітектури стійкості життєво важливих послуг. Це забезпечує можливість ідентифікації повторюваних управлінських рішень, інституційних конфігурацій та організаційних моделей, що формуються на муніципальному рівні в умовах багаторівневого управління критичною інфраструктурою, і створює аналітичні передумови для переходу від фрагментарного опису окремих практик до їх структурованого осмислення.

Отримані узагальнення мають самостійну наукову цінність, оскільки дозволяють поглибити уявлення про роль муніципального рівня в забезпеченні безперервності життєво важливих послуг і розглянути резильєнтність критичної інфраструктури як складний управлінський процес, інтегрований у систему місцевого самоврядування. У такому ракурсі досвід гмін Польщі постає не як сукупність окремих рішень, а як цілісна модель муніципального управління стійкістю, придатна для подальшого теоретичного осмислення та порівняльного аналізу.

Виклад основного матеріалу дослідження. Системний аналіз резильєнтності критичної інфраструктури на муніципальному рівні доцільно здійснювати з позицій управління життєво важливими послугами, а не ізольованими інфраструктурними об'єктами. Така логіка дозволяє поєднати теоретичні підходи до резильєнтності з практикою діяльності гмін Польщі, які виступають базовою ланкою забезпечення безперервності енергетичних, комунальних, транспортних, комунікаційних і соціальних сервісів на муніципальному рівні.

У цьому контексті гміни функціонують не як технічні оператори інфраструктурних мереж, а як публічні координатори локальної стійкості, відповідальні за організацію взаємодії між операторами, службами та населенням, визначення пріоритетів життєво важливих послуг, а також забезпечення стабільності їх надання в повсякденних і кризових умовах. Саме така роль органів місцевого самоврядування обумовлює доцільність аналізу резильєнтності через управління сервісами, а не через технічний стан окремих об'єктів.

На підставі узагальнення польської практики забезпечення резильєнтності критичної інфраструктури на муніципальному рівні в логіці

«резильентності життєво важливих послуг» встановлено, що на даний час фокус зміщується із охорони інфраструктурних елементів на управління безперервністю надання сервісів, здатність системи адаптуватися до збурень та ефективно відновлюватися після інцидентів [23; 27]. Такий підхід є методологічно продуктивним для аналізу гмін Польщі, оскільки органи місцевого самоврядування, не здійснюючи безпосередньої експлуатації мереж, виконують системоутворюючу функцію в локальній архітектурі резильентності, поєднуючи просторове планування, організацію муніципальних послуг, кризове управління та комунікацію з населенням [20; 24]. Це дозволяє перейти від опису інфраструктур як сукупності активів до аналізу управлінських механізмів, через які гміна забезпечує керованість, пріоритизацію та відновлення критичних сервісів.

Інституційна основа резильентності критичної інфраструктури в Польщі формується в межах багаторівневої системи публічного управління, у якій розмежовано стратегічні, координаційні та операційні функції. Нормативну рамку кризового управління визначає Закон Польщі «Про кризове управління» [28], тоді як національний рівень задає загальні підходи до захисту критичної інфраструктури та кризового планування, зокрема на основі затвердження програмних документів Урядового Центру безпеки (*Government Centre for Security*) [12; 29].

Водночас воєводський рівень виконує важливу координаційну роль, забезпечуючи узгодження дій між гмінами, службами та регіональними структурами в разі подій, що виходять за межі однієї територіальної громади або мають каскадні ефекти.

Саме на цьому тлі практична роль гміни постає як ключова: вона організовує безперервність життєво важливих послуг у конкретному просторі проживання населення, узгоджуючи взаємодію операторів мереж, екстрених служб і соціальних інституцій, а також підтримуючи стабільність сервісів у перші фази кризових подій, коли час реагування та якість комунікації безпосередньо впливають на масштаби соціально-економічних втрат [20; 30].

Узагальнений розподіл ролей і управлінських функцій між рівнями влади та операторами критичної інфраструктури (КІ) систематизовано в *табл. 1*.

Перехід від інституційної рамки до практики найкраще простежується через приклади міських гмін, де інструменти комунікації та координації є критично важливими для керованості кризової ситуації. Зокрема, у місті Варшава системно використовуються тестові запуски сигналів тривоги (сирен) як елемент перевірки працездатності системи оповіщення та підготовки населення до коректної реакції, що є важливим для забезпечення безперервності життєво важливих сервісів у разі масштабних загроз [32]. Така практика демонструє, що резильентність у сервісній логіці включає не лише технічне резервування, а й організацію завчасних процедур інформування, які знижують ризики дезорганізації, паніки та невиконання рекомендацій під час надзвичайних ситуацій.

У місті Вроцлав важливим елементом протипаводкової готовності є мережевий формат взаємодії на рівні локальних спільнот: місто інституціоналізувало роботу координаторів повеневих ризиків, підготовлених центром кризового управ-

Таблиця 1

Рівні управління та роль гміни у забезпеченні резильентності критичної інфраструктури Польщі

Рівень	Ключова управлінська роль	Типові інструменти / документи	Практичний внесок
Національний	Формування рамкової політики КІ та координації безпеки	Національна програма захисту КІ, національне кризове планування	Єдині підходи, координація операторів і адміністрації, стандарти планування
Регіональний (воєводство)	Координація між гмінами, службами та регіональними структурами	Регіональні плани реагування, координаційні процедури	Узгодження ресурсів, між-муніципальна взаємодія, підтримка в масштабних НС
Муніципальний (гміна)	Організація безперервності життєво важливих послуг і локальної готовності	Гмінні плани кризового управління, локальні регламенти, протоколи взаємодії, канали оповіщення	Скорочення часу реагування, стабілізація сервісів, адресна підтримка населення
Операторський рівень	Технічна експлуатація мереж і об'єктів	Плани аварійного відновлення, резервні рішення, технічні регламенти	Технічна стійкість, ремонт, відновлення подачі ресурсів

Джерело: складено авторами на основі опрацювання [12; 20; 24; 29; 31].

ліній, які діють у прибережних районах і забезпечують навчання, узгодження локальних дій та підтримку міських служб у ситуаціях загрози [33]. Цей приклад показує, що громада може підсилювати резильєнтність послуг через організаційні механізми, які скорочують часові втрати на узгодження дій і дозволяють швидше стабілізувати критичні функції території (доступність, евакуація, логістика, інформування).

У місті Краків практичну реалізацію кризових функцій підкріплено організаційною структурою міської адміністрації: у профільному підрозділі визначено завдання координації, взаємодії зі службами та реалізації функцій кризового управління на рівні громади, що створює інституційну визначеність відповідальності та забезпечує безперервність управлінського циклу «планування – реагування – відновлення» [34].

У сукупності такі приклади підтверджують тезу, що на муніципальному рівні резильєнтність критичної інфраструктури реалізується насамперед як здатність громади забезпечувати керованість, комунікацію та координацію навколо сервісів, навіть не будучи оператором мереж.

Сервісно орієнтований підхід до резильєнтності дозволяє розглядати критичну інфраструктуру через призму різних сфер життєво важливих послуг, кожна з яких має власний профіль ризиків та управлінських викликів. У сфері електро- та теплопостачання управлінський фокус громади зміщується від безпосереднього відновлення подачі ресурсу до пріоритизації критичних споживачів, підтримки критичних установ та узгодження з операторами графіків відновлення послуги. У сфері водопостачання та водовідведення визначальними є резервні схеми, диспетчеризація та оперативне інформування населення, що дозволяє підтримувати мінімально прийнятний рівень доступності та санітарної безпеки. У транспортній сфері ключовим завданням стає забезпечення функціональної доступності території через пріоритизацію критичних маршрутів і сценарії мобільності, а у сфері зв'язку та інформування – збереження керованості ситуації через багатоканальну комунікацію та узгоджені протоколи взаємодії з провайдером [13; 21; 23; 27].

У практичному вимірі диференціацію типових ризиків і відповідних муніципальних механізмів забезпечення резильєнтності життєво важливих послуг узагальнено в *табл. 2*. Логіка «безперервності послуг» у цьому випадку забезпечує методологічний місток між потребами населення та технічними рішеннями операторів, дозволяючи формалізувати цілі управління через показники

часу відновлення, допустимого рівня переривань та пріоритизації послуг [27].

Важливим виміром резильєнтності гмін є взаємодія з операторами та службами, яка має бути не ситуативною, а інституціоналізованою через стійкі процедури. Дослідження мережевого управління ризиками інфраструктур підкреслюють, що ефективність залежить від узгодженості правил взаємодії, наявності контактних протоколів, механізмів обміну інформацією та кризових команд, які можуть бути активовані без затримок [14; 24]. Практично це означає, що громада має заздалегідь формалізувати порядок доступу до об'єктів, обмін оперативними даними, узгодження пріоритетів відновлення та канали кризової комунікації. Ключові інструменти взаємодії гмін з операторами та службами та їх вплив на практичну резильєнтність наведено в *табл. 3*.

Окрім увагу необхідно приділяти цифровому та кібернетичному виміру, зважаючи на зростаючу залежність муніципальних сервісів від інформаційних систем і диспетчеризації. Як свідчить аналіз літературних джерел з кіберрезильєнтності місцевого самоврядування, на даний час виникла гостра потреба у стандартизованих процедурах управління інцидентами, резервуванні даних, навчанні персоналу та координації з національними структурами реагування [26]. У практичній площині ці вимоги узгоджуються з рекомендаціями ENISA щодо управління кіберкризами, які акцентують необхідність підготовлених процесів, ролей і механізмів відновлення [36]. Таким чином, кіберготовність на рівні гмін має розглядатися як складова безперервності послуг, а не як додаткова функція IT-підрозділів.

Оскільки критична інфраструктура функціонує в середовищі одночасного впливу природних, техногенних, енергетичних, кібернетичних і гібридних загроз, управлінські відповіді гмін мають формуватися в мультизагрозовій логіці. Мультизагрозовий підхід дозволяє планувати готовність не під один тип події, а під сукупність ризиків, характерних для конкретної території, та враховувати каскадні ефекти у взаємозалежних інфраструктурах (енергія – зв'язок – вода – транспорт), що обґрунтовується як у роботах із кількісного оцінювання взаємозалежних систем, так і в дослідженнях multi-hazard оцінювання резильєнтності послуг [15; 27].

На муніципальному рівні це означає пріоритизацію критичних установ, розгортання пунктів життєзабезпечення, підтримку альтернативних каналів комунікації та організацію локальної логістики незалежно від типу первинної загрози, що

Таблиця 2

Життєво важливі послуги та муніципальні механізми забезпечення їх резильєнтності на рівні гмін Польщі

Сфера послуг	Типові порушення / ризики	Ключовий управлінський фокус гміни	Прикладний результат
Електро- та теплопостачання	Дефіцит потужності, відключення, аварії мереж, масштабні блекаути	Пріоритизація критичних споживачів, координація з операторами, підтримка критичних установ	Мінімізація тривалості перерв, захист критичних функцій громади
Вода та водовідведення	Аварії, забруднення, відмова насосних станцій	Резервні схеми, диспетчеризація, аварійні бригади, оповіщення населення	Підтримка мінімального рівня доступності води, санітарна безпека
Транспорт і доступність	Блокування шляхів, руйнування мостів, погодні явища	Сценарії мобільності, пріоритет критичних маршрутів, взаємодія зі службами	Збереження доступу до лікарень / укриттів / логістики
Зв'язок та інформування	Відмова мереж, кібератаки на диспетчеризацію	Альтернативні канали комунікації, протоколи інформування, взаємодія з провайдерами	Збереження керованості та довіри населення
Соціальні сервіси (медицина, допомога)	Перевантаження систем, перебої ресурсів	Плани забезпечення критичних установ, взаємодія з постачальниками	Захист уразливих груп, стабільність базових сервісів

Джерело: складено авторами на основі опрацювання [1; 4; 13; 20; 21; 23; 30; 31; 35].

Таблиця 3

Інструменти взаємодії гмін з операторами та службами в забезпеченні резильєнтності критичної інфраструктури

Блок взаємодії	Що саме узгоджується	Інструмент	На що впливає
Координація з операторами	Критичні споживачі, графіки відновлення, доступ до об'єктів	Протоколи взаємодії, контактні карти, процедурні регламенти	Швидкість відновлення, зниження втрат
Міжвідомча взаємодія	Розподіл ролей між службами, визначення, хто за що відповідає	Кризові штаби / команди, сценарні карти	Керованість під час надзвичайних і кризових ситуацій
Комунікація з населенням	Оповіщення, інструкції поведінки, довіра	Багатоканальне інформування, локальні платформи	Зниження паніки, підвищення дотримання рекомендацій
Дані та кіберстійкість	Інцидент-менеджмент, резервні копії, доступність сервісів	Процедури кіберреагування, резервування, навчання персоналу	Безперервність цифрових сервісів, зниження кіберризиків
Навчання та вправи	Перевірка планів, готовність персоналу	Тренування / симуляції, аудит готовності	Зростання практичної готовності

Джерело: складено авторами на основі опрацювання [1; 4; 14; 20; 24; 26; 31; 35; 36].

узгоджується із сервісною рамкою резильєнтності та практиками мережевого управління [14; 23; 24]. Типологію загроз і пріоритетні управлінські дії гмін у мультизагрозовому контексті доцільно застосовувати як основу для сценарного планування та підвищення готовності на місцевому рівні (табл. 4).

Перехід від концептуального розуміння резильєнтності до її практичного управління потребує

запровадження системи показників для оцінювання. У цьому контексті резильєнтність доцільно розглядати як керований процес, що охоплює готовність, реагування та відновлення в межах компетенцій гміни, а ефективність управління – оцінювати через систему показників (KPI). Ця система показників відображає наявність і актуальність планів безперервності, відпрацьованість процедур

Типологія загроз розвитку критичної інфраструктури та управлінські дії на муніципальному рівні

Тип загроз	Типові наслідки для послуг	Першочергові управлінські дії гміни	Критичний ресурс / умова
Природні (повені, шторми, пожежі)	Пошкодження мереж, обмеження доступності територій	Мобілізація служб, тимчасова логістика, оповіщення	Готовність планів і сил, зв'язок з населенням
Техногенні аварії	Локальні відключення / зупинка сервісів	Взаємодія з оператором, аварійні бригади, локальні резерви	Наявність протоколів і резервних схем
Масштабні енергетичні збої/блекаути	Каскадні відмови (вода / зв'язок / тепло)	Пріоритизація критичних установ, підтримка пунктів життєзабезпечення	Організаційна готовність, сценарне планування
Кіберінциденти	Зупинка диспетчеризації / цифрових сервісів	Реагування за протоколами, відновлення даних, координація з кіберструктурами	Резервні копії, навчені відповідальні особи
Гібридні впливи	Комбіновані порушення та дезінформація	Єдина координація, кризові комунікації, верифікація повідомлень	Довіра, швидкість прийняття рішень

Джерело: складено авторами на основі опрацювання [1; 4; 7; 27; 30; 31; 35].

взаємодії, частоту навчань і вправ, час запуску кризової координації, параметри відновлення мінімального рівня послуг, наявність резервних рішень і кіберготовність [25–27].

Система показників (KPI) резильєнтності на муніципальному рівні, яку подано в табл. 5, забезпечує можливість внутрішнього аудиту та порівняльного аналізу управлінських практик гмін. Її застосування переводить резильєнтність із площини декларативних положень у площину регулярного моніторингу й управлінського контролю, що є особливо важливим для адаптації відповідних інструментів у діяльності територіальних громад України.

Отже, польський досвід підтверджує, що резильєнтність критичної інфраструктури на муніципальному рівні формується не як сукупність ізольованих технічних рішень, а як інтегрована система публічного управління, орієнтована на безперервність життєво важливих послуг. У центрі цієї системи перебуває гміна, яка, не будучи оператором мереж, виконує ключову координуючу, організаційну та комунікаційну функцію. Приклади Варшави, Вроцлава та Кракова демонструють практичну значущість завчасно підготовлених механізмів оповіщення, локальної мережевої координації та інституційної визначеності кризових функцій. У поєднанні з плануванням реагування на різні типи загроз, кіберготовністю та KPI-підходом це формує цілісну управлінську модель, придатну для аналітичного узагальнення та подальшої адап-

тації до умов розвитку критичної інфраструктури на рівні територіальних громад України.

ВИСНОВКИ

У результаті проведеного дослідження встановлено, що ключовим методологічним зрушенням у розумінні муніципальної резильєнтності критичної інфраструктури є перехід від об'єктно-орієнтованої логіки «захисту елементів» до сервісної логіки управління безперервністю життєво важливих послуг. Це дозволило обґрунтувати аналітичну рамку, у межах якої гміна Польщі розглядаються як базові актори забезпечення стійкості локальних сервісів – енергетичних, комунальних, транспортних, комунікаційних і соціальних – через координацію, планування та організацію взаємодії з операторами та службами в повсякденних і кризових умовах.

Одержані результати свідчать, що ефективна резильєнтність критичної інфраструктури на рівні гмін базується на поєднанні п'яти взаємопов'язаних елементів, а саме:

- ✦ інституційної чіткості багаторівневої архітектури управління, де національний, регіональний, муніципальний та операторський рівні виконують комплементарні функції, а гміна виступає інтегратором локальної готовності та безперервності послуг;
- ✦ управління портфелем життєво важливих послуг, що передбачає диференційовані управлінські механізми залежно від сфери

**Показники (KPI) резильєнтності критичної інфраструктури на рівні гмін:
готовність – реагування – відновлення**

Вимір резильєнтності	KPI	Як вимірюється / перевіряється	Для яких послуг критично
Планувальна готовність	Частка життєво важливих послуг, охоплених планами безперервності	Реєстр послуг, наявність планів / додатків, дата оновлення	Усі
Актуальність планування	Періодичність оновлення кризових планів	Контрольний цикл оновлення, протоколи перегляду	Усі
Координаційна спроможність	Наявність протоколів взаємодії з операторами	Перелік угод / процедур, контактні карти 24/7	Енергія, вода, зв'язок
Навчання та вправи	Кількість тренувань / симуляцій на рік	Плани навчань, звіти про вправи	Усі (особливо енергія/ вода)
Час реагування	Час до запуску кризової координації після інциденту	Журнали подій, регламент «першої години» реагування	Енергія, вода, транспорт
Параметри відновлення	Час відновлення до мінімального рівня послуги	Фіксація SLA / цільових значень, фактичні дані	Енергія, вода, тепло
Резервування	Наявність резервних рішень (генерація/пункти води/зв'язок)	Інвентаризація резервів, місця розгортання	Енергія, вода, зв'язок
Кіберготовність	Наявність процедур інцидент-менеджменту та резервних копій	Чек-лист процедур, тест відновлення даних	Цифрові сервіси / диспетчеризація
Комунікаційна стійкість	Охоплення населення системами оповіщення	Кількість каналів, тестові повідомлення	Усі

Джерело: складено авторами на основі опрацювання [1; 4; 23; 25; 26; 31; 35; 36].

сервісів, характеру ризиків і соціальної значущості послуг;

- ✦ мережеву взаємодію між гмінами, операторами, екстреними службами та населенням, яка забезпечує практичну реалізацію планів і процедур у кризових умовах;
- ✦ планування реагування на різні типи загроз, що дозволяє враховувати комбінований вплив природних, техногенних, енергетичних, кібернетичних і гібридних ризиків та переходити від реактивних дій до сценарного планування управлінських рішень;
- ✦ переведення резильєнтності в систему вимірюваних показників готовності, реагування та відновлення, придатних для регулярного моніторингу й аудиту на муніципальному рівні.

З урахуванням результатів дослідження та специфіки інституційної ролі гмін у системі управління критичною інфраструктурою Польщі необхідно сформулювати комплекс практичних рекомендацій, спрямованих на посилення їхньої управлінської спроможності у сфері резильєнтності.

1) *Інституційне посилення ролі гміни у забезпеченні безперервності послуг.* Слід наголосити, що гмінам доцільно послідовно закріплювати свою роль не лише як органів місцевого самоврядування, а як центральних координаторів безперервності життєво важливих послуг на локальному рівні. Це передбачає: формалізацію координаційних функцій гміни у кризових і докризових процедурах; чітке визначення відповідальності за інтеграцію дій операторів, екстрених служб і соціальних інституцій; включення питань резильєнтності критичної інфраструктури до стратегічних документів розвитку гмін. Таке інституційне позиціонування підсилює керованість системи у кризових ситуаціях і забезпечує узгодженість дій усіх залучених акторів.

2) *Застосування сервісно орієнтованого підходу до планування резильєнтності.* Для підвищення практичної ефективності резильєнтності гмінам доцільно перейти від формального кризового планування до управління портфелем життєво важливих послуг. Це передбачає: ідентифікацію ключових сервісів з точки зору соціальної значущості; визначення критичних споживачів та уразливих груп населення; встановлення мінімально

допустимих рівнів надання послуг у кризових умовах; формування чітких пріоритетів відновлення. Такий підхід дозволяє орієнтувати управлінські рішення на потреби населення, а не лише на технічні параметри інфраструктурних об'єктів.

3) *Інституціоналізація мережевої взаємодії та кризової координації.* Ефективна резильєнтність на рівні гміни неможлива без стійкої мережевої взаємодії. У цьому контексті доцільно: розробляти та регулярно оновлювати протоколи взаємодії з операторами критичної інфраструктури; створювати постійно діючі або мобілізовані кризові команди; забезпечувати доступність контактних каналів 24/7; впроваджувати багатоканальні системи інформування населення. Особливу увагу слід приділяти узгодженості дій у перші години після інциденту, коли швидкість координації має вирішальне значення.

4) *Інтеграція антикризового та сценарного підходу в муніципальне управління.* З огляду на зростання частоти та складності кризових ситуацій гмінам доцільно переходити від однотипних сценаріїв реагування до планування, орієнтованого на поєднання різних типів загроз. Такий підхід дозволяє враховувати каскадні відмови між секторами критичної інфраструктури, одночасний вплив природних, техногенних, енергетичних і кібернетичних ризиків, а також підвищене навантаження на людські, фінансові та організаційні ресурси. Застосування сценарного планування створює можливість завчасно виявляти критичні вразливості системи та готувати резервні управлінські рішення на муніципальному рівні.

5) *Запровадження системи моніторингу та оцінювання резильєнтності.* Для переходу від декларативних підходів до керованої резильєнтності гмінам доцільно впроваджувати систему ключових показників ефективності (КПІ), яка: охоплює готовність, реагування та відновлення; базується на управлінських, а не на суто технічних параметрах; дозволяє здійснювати внутрішній аудит і міжмуніципальні порівняння; створює основу для обґрунтування бюджетних та інвестиційних рішень. Системне використання КПІ сприяє підвищенню прозорості муніципальної політики та формуванню культури управління резильєнтністю.

6) *Посилення людського та організаційного виміру резильєнтності.* Окремим напрямом є розвиток кадрової та організаційної спроможності гмін, що передбачає: регулярні навчання та симуляційні вправи для персоналу; підвищення компетентності посадових осіб у сфері кризового управління; розвиток міжмуніципального обміну досвідом і кращими практиками. Цей вимір є критичним для трансформації формальних планів у реальні управлінські дії.

Польський досвід забезпечення резильєнтності критичної інфраструктури є релевантним для України, особливо в умовах воєнних дій і повоєнного відновлення, з огляду на спільні риси децентралізованої системи управління та зростаючу роль територіальних громад. Результати дослідження свідчать про доцільність інституційного закріплення ролі громад як координаторів безперервності життєво важливих послуг, переходу до сервісної логіки управління, розвитку мережевих механізмів взаємодії з операторами та службами, впровадження планування реагування на різні типи загроз і застосування системи показників резильєнтності для моніторингу готовності та обґрунтування рішень у процесі відновлення.

У подальших дослідженнях планується приділити увагу обґрунтуванню методичного підходу до оцінювання резильєнтності життєво важливих послуг на муніципальному рівні, порівняльному аналізу діяльності гмін із різним соціально-економічним профілем, а також розробленню практичних рекомендацій щодо адаптації європейських практик до умов повоєнного відновлення територіальних громад України. ■

БІБЛІОГРАФІЯ

1. Хаустова В. Є., Трушкіна Н. В. Загрози розвитку критичної інфраструктури: сутність і класифікація. *Проблеми економіки*. 2025. № 3. С. 89–104. DOI: <https://doi.org/10.32983/2222-0712-2025-3-89-104>
2. Хаустова В. Є., Трушкіна Н. В. Теоретичні підходи до сутності поняття «критична інфраструктура»: міжнародний, просторовий і резильєнтнісний виміри. *Проблеми економіки*. 2025. № 4. С. 336–351. DOI: <https://doi.org/10.32983/2222-0712-2025-4-336-351>
3. Хаустова В. Є., Решетняк О. І. Резильєнтність економіки: сутність і виклики для України. *Бізнес Інформ*. 2023. № 7. С. 30–41. DOI: <https://doi.org/10.32983/2222-4459-2023-7-30-41>
4. Кизим М. О., Хаустова В. Є., Решетняк О. І., Попович М. В., Юденко Є. В. Оцінювання резильєнтності економічних систем в умовах невизначеності: існуючі підходи та їх практична імплементація. *Бізнес Інформ*. 2025. № 10. С. 48–65. DOI: <https://doi.org/10.32983/2222-4459-2025-10-48-65>
5. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union. 2022. L 333. P. 164–198. URL: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>
6. Poland in figures 2025. Warszawa : Statistics Poland, 2025. URL: <https://plwliczbach.stat.gov.pl/EN/index.html>

7. Statystyczne podsumowanie 2024 roku. Warszawa: Komenda Główna Państwowej Straży Pożarnej, 2025. URL: <https://www.gov.pl/web/kgpsp/statystyczne-podsumowanie-2024-roku>
8. Annual report from the actions of CERT Polska 2024. The Polish security landscape. Warsaw : NASK National Research Institute, 2025. 111 p. URL: https://cert.pl/en/uploads/docs/Report_CP_2024.pdf
9. Minder R. Russian hackers target Polish hospitals and city water supply. *Financial Times*. 2025. 16 September. URL: <https://www.ft.com/content/3e7c7a96-09e7-407f-98d7-a29310743d28>
10. Wojtasik K., Szlachter D. et al. Terrorist and sabotage threats to critical infrastructure. Warszawa : Agencja Bezpieczeństwa Wewnętrznego, 2025. 342 p. URL: https://www.abw.gov.pl/ftp/foto/Wydawnictwo/terroryzm/wydanie-specjalne-2025/T-SAP_-_special_edition_-_CALOSC_NOWY.pdf
11. Gawkowski K. Poland foiled cyberattack on big city's water supply, deputy PM says. *Reuters*. 2025. 14 August. URL: <https://www.reuters.com/en/poland-foiled-cyberattack-big-citys-water-supply-deputy-pm-says-2025-08-14/>
12. National Critical Infrastructure Protection Program. *Government Centre for Security*. 2023. URL: <https://www.gov.pl/web/rcb-en/national-critical-infrastructure-protection-program>
13. Monstadt J., Schmidt M. Urban resilience in the making? The governance of critical infrastructures in German cities. *Urban Studies*. 2019. Vol. 56. Iss. 11. P. 2353–2371. DOI: <https://doi.org/10.1177/0042098018808483>
14. Huck A., Monstadt J., Driessen P.P.J., Rudolph-Cleff A. Towards resilient Rotterdam? Key conditions for a networked approach to managing urban infrastructure risks. *Journal of Contingencies and Crisis Management*. 2021. Vol. 29. Iss. 1. P. 12–22. DOI: <https://doi.org/10.1111/1468-5973.12295>
15. Goldbeck N., Angeloudis P., Ochieng W. Y. Resilience assessment for interdependent urban infrastructure systems using dynamic network flow models. *Reliability Engineering & System Safety*. 2019. Vol. 188. P. 62–79. DOI: <https://doi.org/10.1016/j.ress.2019.03.007>
16. Rezvani S. M. H. S., Falcão Silva M. J., de Almeida N. M. The risk-informed asset-centric (RIACT) urban resilience enhancement process: An outline and pilot-case demonstrator for earthquake risk mitigation in Portuguese municipalities. *Applied Sciences*. 2024. Vol. 14. Iss. 2. Art. 634. DOI: <https://doi.org/10.3390/app14020634>
17. Dong B. X., Shan M., Hwang B. G. Simulation of transportation infrastructures resilience: a comprehensive review. *Environmental Science and Pollution Research*. 2022. Vol. 29. P. 12965–12983. DOI: <https://doi.org/10.1007/s11356-021-18033-w>
18. Sfetos A., Giroud F., Clemencau A. et al. Assessing the Effects of Forest Fires on Interconnected Critical Infrastructures under Climate Change. Evidence from South France. *Infrastructures*. 2021. Vol. 6. Iss. 2. Art. 16. DOI: <https://doi.org/10.3390/infrastructures6020016>
19. Govindarajulu D. Strengthening institutional and financial mechanisms for building urban resilience in India. *International Journal of Disaster Risk Reduction*. 2020. Vol. 47. Art. 101549. DOI: <https://doi.org/10.1016/j.ijdrr.2020.101549>
20. Heino O., Takala A., Jukarainen P. et al. Critical Infrastructures: The Operational Environment in Cases of Severe Disruption. *Sustainability*. 2019. Vol. 11. Iss. 3. Art. 838. DOI: <https://doi.org/10.3390/su11030838>
21. Olausson P. M. Planning for resilience in the case of power shortage: The Swedish STYREL policy. *Central European Journal of Public Policy*. 2019. Vol. 13. Iss. 1. P. 12–22. DOI: <https://doi.org/10.2478/cejpp-2019-0004>
22. Eledi Kuusaana J. A., Monstadt J., Smith S. Practicing urban resilience to electricity service disruptions in Accra, Ghana. *Energy Research & Social Science*. 2023. Vol. 95. Art. 102885. DOI: <https://doi.org/10.1016/j.erss.2022.102885>
23. Wiśniewski M., Szwarz K., Skomra W. Continuity of Essential Services as an Emerging Challenge for Societal Resilience. *IEEE Access*. 2023. Vol. 11. P. 44614–44635. DOI: <https://doi.org/10.1109/ACCESS.2023.3271751>
24. Knodt M., Fraune C., Engel A. Local governance of critical infrastructure resilience: Types of coordination in German cities. *Journal of Contingencies and Crisis Management*. 2022. Vol. 30. Iss. 3. P. 307–316. DOI: <https://doi.org/10.1111/1468-5973.12386>
25. McAlister M. M., Murali P. S., Zhang Q., Wells E. C., Mohebbi S. Improving and quantifying organizational resilience for sustainable management of critical infrastructures: A multi-level system dynamics approach. *International Journal of Disaster Risk Reduction*. 2024. Vol. 115. Art. 105079. DOI: <https://doi.org/10.1016/j.ijdrr.2024.105079>
26. Holmström A., Große C. Not All Heroes Wear Capes: Cyber Resilience of the Social Administration at a Swedish Municipality. *Risk, Hazards & Crisis in Public Policy*. 2025. Vol. 16. Iss. 3. Art. e70024. DOI: <https://doi.org/10.1002/rhc3.70024>
27. Haro-Báez A. G., Posso E., Rojas S., Arcos-Aviles D. Simplified Multi-Hazard Assessment to Foster Resilience for Sustainable Energy Infrastructure on Santa Cruz Island, Galapagos. *Sustainability*. 2025. Vol. 17. Iss. 1. Art. 106. DOI: <https://doi.org/10.3390/su17010106>
28. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. *Dziennik Ustaw*. 2007. Nr. 89, poz. 590. URL: <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20070890590/U/D20070590Lj.pdf>
29. Krajowy Plan Zarządzania Kryzysowego. *Rządowe Centrum Bezpieczeństwa*. 2024. URL: <https://www.gov.pl/web/rcb/krajowy-plan-zarzadzania-kryzysowego>

30. Majchrzak D., Michalski K., Reginia-Zacharski J. Readiness of the Polish crisis management system to respond to long-term, large-scale power shortages and failures (Blackouts). *Energies*. 2021. Vol. 14. Iss. 24. Art. 8286. DOI: <https://doi.org/10.3390/en14248286>
31. Кизим М. О., Козирєва О. В., Трушкіна Н. В. Міжнародні інструменти повоєнної відбудови критичної інфраструктури та їх адаптація для регіонів України. *Ефективна економіка*. 2026. № 1. DOI: <https://doi.org/10.32702/2307-2105.2026.1.22>
32. Tests of the alarm system. *City Hall of Warsaw*. 2024. 08 October. URL: <https://en.um.warszawa.pl/-/tests-of-the-alarm-system>
33. Największe zagrożenie minęło. Oto podsumowanie działań przeciwpowodziowych we Wrocławiu. *Biuro Prasowe Urzędu Miejskiego Wrocławia*. 2024. 23 September. URL: <https://www.wroclaw.pl/dla-mieszkanca/podumowanie-dzialan-przeciwpowodziowych-wewroclawiu>
34. Wydział Bezpieczeństwa i Zarządzania Kryzysowego (OC). *Biuletyn Informacji Publicznej Miasta Krakowa*. 2025. URL: <https://www.bip.krakow.pl/struktura/OC>
35. Zaporozhets A., Khaustova V., Hubarieva I., Trushkina N. Digitization as a Modern Challenge for the Energy Systems' Transformation in the World. *Systems, Decision and Control in Energy VII. Studies in Systems, Decision and Control* : monograph. Berlin : Springer Science and Business Media Deutschland GmbH, 2025. Vol. 596. P. 3–31. DOI: https://doi.org/10.1007/978-3-031-90462-2_1
36. Best Practices for Cyber Crisis Management. *European Union Agency for Cybersecurity (ENISA)*. February 2024. URL: <https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Study%20Best%20Practices%20Cyber%20Crisis%20Management.pdf>
- pl/isap.nsf/download.xsp/WDU20070890590/U/D20070590Lj.pdf
- Eledi Kuusaana J. A., Monstadt J. & Smith S. (2023). Practicing urban resilience to electricity service disruptions in Accra, Ghana. *Energy Research & Social Science*, 95. Art. 102885. <https://doi.org/10.1016/j.erss.2022.102885>
- European Union Agency for Cybersecurity (ENISA). Best Practices for Cyber Crisis Management. <https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Study%20Best%20Practices%20Cyber%20Crisis%20Management.pdf>
- Gawkowski K. (2025, August 14). Poland foiled cyberattack on big city's water supply, deputy PM says. *Reuters*. <https://www.reuters.com/en/poland-foiled-cyberattack-big-citys-water-supply-deputy-pm-says-2025-08-14/>
- Goldbeck N., Angeloudis P. & Ochieng W. Y. (2019). Resilience assessment for interdependent urban infrastructure systems using dynamic network flow models. *Reliability Engineering & System Safety*, 188, 62–79. <https://doi.org/10.1016/j.ress.2019.03.007>
- Government Centre for Security. (2023). National Critical Infrastructure Protection Program. <https://www.gov.pl/web/rcb-en/national-critical-infrastructure-protection-program>
- Govindarajulu D. (2020). Strengthening institutional and financial mechanisms for building urban resilience in India. *International Journal of Disaster Risk Reduction*, 47. Art. 101549. <https://doi.org/10.1016/j.ijdr.2020.101549>
- Haro-Báez A. G., Posso E., Rojas S. & Arcos-Aviles D. (2025). Simplified Multi-Hazard Assessment to Foster Resilience for Sustainable Energy Infrastructure on Santa Cruz Island, Galapagos. *Sustainability*, 17(17). Art. 106. <https://doi.org/10.3390/su17010106>
- Heino O., Takala A., Jukarainen P. & et al. (2019). Critical Infrastructures: The Operational Environment in Cases of Severe Disruption. *Sustainability*, 3(11), Art. 838. <https://doi.org/10.3390/su11030838>
- Holmström A. & Große C. (2025). Not All Heroes Wear Capes: Cyber Resilience of the Social Administration at a Swedish Municipality. *Risk, Hazards & Crisis in Public Policy*, 3(16). Art. e70024. <https://doi.org/10.1002/rhc3.70024>
- Huck A., Monstadt J., Driessen P. P. J. & Rudolph-Cleff A. (2021). Towards resilient Rotterdam? Key conditions for a networked approach to managing urban infrastructure risks. *Journal of Contingencies and Crisis Management*, 1(29), 12–22. <https://doi.org/10.1111/1468-5973.12295>
- Khaustova V. Ye. & Reshetniak O. I. (2023). Rezyliientnist ekonomiky: sutnist i vyklyky dlia Ukrainy [Economic resilience: essence and challenges for Ukraine]. *Biznes Inform*, 7, 30–41. <https://doi.org/10.32983/2222-4459-2023-7-30-41>

REFERENCES

- Biuletyn Informacji Publicznej Miasta Krakowa. (2025). Wydział Bezpieczeństwa i Zarządzania Kryzysowego (OC). <https://www.bip.krakow.pl/struktura/OC>
- Biuro Prasowe Urzędu Miejskiego Wrocławia. (2024, September 23). Największe zagrożenie minęło. Oto podsumowanie działań przeciwpowodziowych we Wrocławiu. <https://www.wroclaw.pl/dla-mieszkanca/podumowanie-dzialan-przeciwpowodziowych-wewroclawiu>
- City Hall of Warsaw. (2024, October 8). Tests of the alarm system. <https://en.um.warszawa.pl/-/tests-of-the-alarm-system>
- Dong B. X., Shan M. & Hwang B. G. (2022). Simulation of transportation infrastructures resilience: a comprehensive review. *Environmental Science and Pollution Research*, 29, 12965–12983. <https://doi.org/10.1007/s11356-021-18033-w>
- Dziennik Ustaw. (2007). Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. <https://isap.sejm.gov>

- Khaustova V. Ye. & Trushkina N. V. (2025). Zahrozy rozvytku krytychnoi infrastruktury: sutnist i klasyfikatsiia [Threats to the development of critical infrastructure: essence and classification]. *Problemy ekonomiky*, 3, 89–104. <https://doi.org/10.32983/2222-0712-2025-3-89-104>
- Khaustova V. Ye. & Trushkina N. V. (2025). Teoretychni pidkhody do sutnosti poniattia «krytychna infrastruktura»: mizhnarodnyi, prostorovyi i rezylentnisnyi vymiry [Theoretical approaches to the essence of the concept of "critical infrastructure": international, spatial and resilience dimensions]. *Problemy ekonomiky*, 4, 336–351. <https://doi.org/10.32983/2222-0712-2025-4-336-351>
- Knodt M., Fraune C. & Engel A. (2022). Local governance of critical infrastructure resilience: Types of coordination in German cities. *Journal of Contingencies and Crisis Management*, 3(30), 307–316. <https://doi.org/10.1111/1468-5973.12386>
- Komenda Główna Państwowej Straży Pożarnej. (2025). Statystyczne podsumowanie 2024 roku. <https://www.gov.pl/web/kgpsp/statystyczne-podsumowanie-2024-roku>
- Kyzym M. O., Khaustova V. Ye., Reshetniak O. I., Popovych M. V. & Yudenko Ye. V. (2025). Otsiniuvannia rezylentnosti ekonomichnykh system v umovakh nevyznachenosti: isnuichi pidkhody ta yikh praktychna implementatsiia [Assessment of the resilience of economic systems under uncertainty: existing approaches and their practical implementation]. *Biznes Inform*, 10, 48–65. <https://doi.org/10.32983/2222-4459-2025-10-48-65>
- Kyzym M. O., Kozryieva O. V. & Trushkina N. V. (2026). Mizhnarodni instrumenty povoiennoi vidbudovy krytychnoi infrastruktury ta yikh adaptatsiia dlia rehioniv Ukrainy [International instruments of post-war reconstruction of critical infrastructure and their adaptation for the regions of Ukraine]. *Efektivna ekonomika*, 1. <https://doi.org/10.32702/2307-2105.2026.1.22>
- Majchrzak D., Michalski K. & Regina-Zacharski J. (2021). Readiness of the Polish crisis management system to respond to long-term, large-scale power shortages and failures (Blackouts). *Energies*, 24(14), Art. 8286. <https://doi.org/10.3390/en14248286>
- McAlister M. M., Murali P. S., Zhang Q., Wells E. C. & Mohebbi S. (2024). Improving and quantifying organizational resilience for sustainable management of critical infrastructures: A multi-level system dynamics approach. *International Journal of Disaster Risk Reduction*, 115, Art. 105079. <https://doi.org/10.1016/j.ijdr.2024.105079>
- Minder R. (2025, September 16). Russian hackers target Polish hospitals and city water supply. *Financial Times*. <https://www.ft.com/content/3e7c7a96-09e7-407f-98d7-a29310743d28>
- Monstadt J. & Schmidt M. (2019). Urban resilience in the making? The governance of critical infrastructures in German cities. *Urban Studies*, 11(56), 2353–2371. <https://doi.org/10.1177/0042098018808483>
- NASK National Research Institute. (2025). Annual report from the actions of CERT Polska 2024. The Polish security landscape. https://cert.pl/en/uploads/docs/Report_CP_2024.pdf
- Official Journal of the European Union. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>
- Olausson P. M. (2019). Planning for resilience in the case of power shortage: The Swedish STYREL policy. *Central European Journal of Public Policy*, 1(13), 12–22. <https://doi.org/10.2478/cejpp-2019-0004>
- Rezvani S. M. H. S., Falcão Silva M. J. & de Almeida N. M. (2024). The risk-informed asset-centric (RIACT) urban resilience enhancement process: An outline and pilot-case demonstrator for earthquake risk mitigation in Portuguese municipalities. *Applied Sciences*, 2(14), Art. 634. <https://doi.org/10.3390/app14020634>
- Rządowe Centrum Bezpieczeństwa. (2024). Krajowy Plan Zarządzania Kryzysowego. <https://www.gov.pl/web/rcb/krajowy-plan-zarządzania-kryzysowego>
- Sfetsos A., Giroud F., Clemencau A. & et al. (2021). Assessing the Effects of Forest Fires on Interconnected Critical Infrastructures under Climate Change. Evidence from South France. *Infrastructures*, 2(6), Art. 16. <https://doi.org/10.3390/infrastructures6020016>
- Statistics Poland. (2025). Poland in figures 2025. <https://plwliczbach.stat.gov.pl/EN/index.html>
- Wiśniewski M., Szwarc K. & Skomra W. (2023). Continuity of Essential Services as an Emerging Challenge for Societal Resilience. *IEEE Access*, 11, 44614–44635. <https://doi.org/10.1109/ACCESS.2023.3271751>
- Wojtasik K., Szlachter D. & et al. (2025). *Terrorist and sabotage threats to critical infrastructure*. Warszawa: Agencja Bezpieczeństwa Wewnętrznego. https://www.abw.gov.pl/ftp/foto/Wydawnictwo/terrorizm/wydanie-specjalne-2025/T-SAP_-_special_edition_-_CALOSC_NOWY.pdf
- Zaporozhets A., Khaustova V., Hubarieva I. & Trushkina N. (2025). Digitization as a Modern Challenge for the Energy Systems' Transformation in the World. *Systems, Decision and Control in Energy VII. Studies in Systems, Decision and Control* (p. 3–31). Berlin: Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-90462-2_1

Стаття надійшла до редакції / Received: 05.03.2026
 Статтю прийнято до публікації / Accepted: 18.03.2026
 Оприлюднено / Published: 30.04.2026