УДК 351.862:338.49:005.33

В. Є. Хаустова,
д. е. н., професор, директор, Науково-дослідний центр
індустріальних проблем розвитку НАН України, м. Харків
ORCID ID: https://orcid.org/0000-0002-5895-9287
Н. В. Трушкіна,
к. е. н., старший дослідник, старший науковий співробітник сектора промислової політики
та інноваційного розвитку відділу промислової політики та енергетичної безпеки,
Науково-дослідний центр індустріальних проблем розвитку НАН України, м. Харків
ORCID ID: https://orcid.org/0000-0002-6741-7738

DOI: 10.32702/2306-6792.2026.7.64

КОНЦЕПТУАЛЬНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ЗАКОРДОННИЙ ДОСВІД ТА НАПРЯМИ ІМПЛЕМЕНТАЦІЇ В УКРАЇНІ

V. Khaustova,
Doctor of Economic Sciences, Professor, Research Center for Industrial Problems of Development
of the National Academy of Sciences of Ukraine, Kharkiv, Ukraine
N. Trushkina,
PhD in Economics, Senior Research Fellow, Research Center for Industrial Problems
of Development of the National Academy of Sciences of Ukraine, Kharkiv, Ukraine

CONCEPTUAL FOUNDATIONS FOR ENSURING THE RESILIENCE OF CRITICAL INFRASTRUCTURE: FOREIGN EXPERIENCE AND DIRECTIONS FOR IMPLEMENTATION IN UKRAINE

У статті здійснено комплексне узагальнення концептуальних підходів до забезпечення стійкості критичної інфраструктури в умовах сучасних безпекових викликів і зростаючої невизначеності. Обґрунтовано доцільність інтеграції ризик-орієнтованого, системного, сервісно-орієнтованого та безпекового підходів до управління критичною інфраструктурою з урахуванням міжсекторальної взаємодії та багаторівневого характеру загроз. Систематизовано ключові фактори вразливості та визначено принципи формування стійкості інфраструктурних систем на національному та муніципальному рівнях. Запропоновано концептуальну модель забезпечення стійкості критичної інфраструктури, що поєднує ідентифікацію загроз, оцінювання ризиків, інституційне забезпечення, інструменти реагування та механізми відновлення. Практичне значення результатів полягає у можливості їх використання органами публічного управління для підвищення резильєнтності критичної інфраструктури України в умовах воєнних та посткризових трансформацій.

The article provides a comprehensive synthesis and critical analysis of contemporary conceptual approaches to ensuring the resilience of critical infrastructure under conditions of escalating security challenges, increasing systemic risks, and a high level of uncertainty. The necessity of transitioning from fragmented managerial decisions to an integrated model is substantiated, combining risk-oriented, systemic, service-oriented, and security-based approaches, taking into account cross-sectoral interaction, critical interdependencies, and cascading effects in the functioning of infrastructure systems. The key vulnerability factors of critical infrastructure under conditions of military threats, energy shocks, digital risks, and institutional instability are identified, and the principles of resilience formation at the national, regional, and municipal levels are systematized.

ISSN 2306-6792

The study advances the theoretical understanding of critical infrastructure resilience as the ability of a system to ensure the continuity of essential services, adapt to destabilizing influences, respond effectively to crisis situations, and rapidly recover its functionality. A conceptual model for ensuring the resilience of critical infrastructure is proposed, encompassing sequential stages of identifying threats and critical elements, risk assessment, development of institutional and regulatory support, implementation of preventive protection and response instruments, as well as mechanisms for recovery and further development. Particular emphasis is placed on the integration of digital technologies, strengthening coordination among governance actors, and expanding international cooperation in the field of critical infrastructure protection.

The practical significance of the results lies in their applicability by public authorities and local self-government bodies for shaping an effective policy of critical infrastructure resilience in Ukraine, improving risk management mechanisms, enhancing preparedness for crisis situations, and ensuring the sustainable functioning of infrastructure systems under conditions of wartime and post-crisis transformations.

Ключові слова: національна економіка, критична інфраструктура, стійкість критичної інфраструктури, безпековий підхід, ризик-орієнтований підхід, управління ризиками, вразливість, загрози, кризи, невизначеність, каскадні ефекти, інфраструктурні системи, публічне управління, цифрові технології, кризове управління, резильєнтність, сталий розвиток, національна безпека.

Key words: national economy, critical infrastructure, critical infrastructure resilience, security-based approach, risk-oriented approach, risk management, vulnerability, threats, crises, uncertainty, cascading effects, infrastructure systems, public administration, digital technologies, crisis management, resilience, sustainable development, national security.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Сучасний етап розвитку України характеризується безпрецедентними викликами, зумовленими повномасштабною війною, що супроводжується системними руйнуваннями об'єктів критичної інфраструктури, порушенням функціонування життєво важливих систем та зростанням рівня загроз для національної безпеки. Цілеспрямовані атаки на енергетичну, транспортну, комунальну та цифрову інфраструктуру призводять до масштабних соціально-економічних втрат, дестабілізації функціонування територіальних громад і зниження якості життя населення. Особливої гостроти набувають ризики, які пов'язано з втратою безперервності постачання електроенергії, води, тепла, а також функціонування систем зв'язку та логістичних ланцюгів.

В умовах воєнних дій критична інфраструктура виступає не лише як базис забезпечення життєдіяльності суспільства, але й як ключовий елемент національної стійкості, здатний впливати на обороноздатність держави, ефективність функціонування економіки та здатність країни до відновлення. Руйнування інфраструктурних об'єктів має мультиплікативний ефект, спричиняючи порушення міжгалузевих зв'язків, зростання витрат бізнесу, зниження інвестиційної привабливості та посилення соціальної вразливості.

Паралельно із загостренням безпекових ризиків у світі відбувається трансформація підходів до управління критичною інфраструктурою. Традиційна модель, що орієнтована переважно на фізичний захист об'єктів, поступово поступається місцем концепції стійкості, яка передбачає здатність інфраструктурних систем не лише протидіяти загрозам, але й адаптуватися до змін, швидко відновлюватися після кризових впливів і забезпечувати безперервність надання життєво важливих послуг. Такий підхід формується під впливом глобальних викликів, включаючи геополітичну нестабільність, енергетичні кризи, кіберзагрози та кліматичні зміни.

Особливої актуальності набуває інтеграція принципів стійкості у практику державного управління та розвиток інституційних механізмів забезпечення функціонування критичної інфраструктури в умовах високої невизначеності. У цьому контексті важливим є врахування міжнародного досвіду, зокрема підходів, що реалізуються в країнах Європейського Союзу та інших розвинених державах, де питання стійкості критичної інфраструктури розглядається як складова комплексної політики безпеки та сталого розвитку.

Для України, яка перебуває у стані глибоких трансформацій та одночасно здійснює курс

ISSN 2306-6792

на європейську інтеграцію, формування сучасної концепції забезпечення стійкості критичної інфраструктури є не лише актуальним, але й стратегічно необхідним завданням. Це потребує переосмислення існуючих підходів, адаптації світових практик до національних умов та розроблення ефективних механізмів імплементації відповідних рішень на державному та регіональному рівнях.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проблематика забезпечення стійкості критичної інфраструктури в останні роки набула значного поширення у наукових дослідженнях, що зумовлено зростанням глобальних безпекових викликів, ускладненням міжсистемних взаємозв'язків та підвищенням вразливості інфраструктурних систем до різнотипних загроз. У сучасному науковому дискурсі відбувається поступовий перехід від традиційної парадигми захисту критичної інфраструктури до концепції її стійкості, яка передбачає здатність систем функціонувати в умовах невизначеності, адаптуватися до змін і відновлюватися після деструктивних впливів [1; 2].

Аналіз наукових праць дозволяє виокремити кілька базових підходів до трактування стійкості критичної інфраструктури. По-перше, функціонально-відновлювальний підхід, у межах якого стійкість розглядається як здатність системи зберігати або оперативно відновлювати виконання ключових функцій після порушень [1]. По-друге, адаптивно-системний підхід, що акцентує увагу на здатності інфраструктурних систем змінювати свою структуру та поведінку під впливом зовнішніх факторів [2]. По-третє, ризик-орієнтований підхід, який фокусується на ідентифікації, оцінці та мінімізації загроз як основі забезпечення стійкості. Водночас, зазначені підходи здебільшого розглядаються ізольовано, що обмежує можливості формування цілісного бачення стійкості як багатовимірної характеристики інфраструктурних систем.

Суттєвий вплив на розвиток концепції стійкості критичної інфраструктури мають підходи, закріплені у нормативно-правових актах і стратегічних документах. Зокрема, у межах Європейського Союзу сформовано інституційний підхід до забезпечення стійкості, який відображено у Директиві (EU) 2022/2557. У цьому документі стійкість визначається як здатність критичних суб'єктів запобігати загрозам, протидіяти їм, адаптуватися до їх впливу та відновлюватися після порушень [3; 4]. При цьому акцент робиться на необхідності впровадження систем управління ризиками, забезпечення безперервності надання послуг та розвитку координаційних механізмів між державами та секторами [3; 5; 6].

Водночас аналіз аналітичних матеріалів і практик імплементації цієї Директиви свідчить про домінування інституційно-регуляторного підходу, у межах якого стійкість розглядається переважно через призму нормативного забезпечення та організаційних механізмів [3; 6; 7]. Такий підхід є необхідним, однак недостатнім, оскільки не повною мірою враховує технологічні, поведінкові та міжсистемні аспекти функціонування критичної інфраструктури.

У сучасних дослідженнях також простежується тенденція до інтеграції різних підходів через формування комплексних моделей забезпечення стійкості. Зокрема, наголошується на важливості поєднання ризик-орієнтованого управління, цифрових технологій, міжсекторальної взаємодії та систем моніторингу для підвищення здатності інфраструктури реагувати на багатовимірні загрози [3; 6; 7]. Водночас такі моделі часто мають фрагментарний характер і не забезпечують достатнього рівня узагальнення для їх адаптації в умовах конкретних національних систем.

Окрему увагу в наукових працях приділено питанням гармонізації національних систем захисту критичної інфраструктури з міжнародними стандартами. У цьому контексті підкреслюється необхідність формування єдиних підходів до ідентифікації критичних об'єктів, проведення національних оцінок ризиків та забезпечення ефективної взаємодії між державними органами і приватним сектором [1—2; 7—8]. Разом з тим, у більшості досліджень недостатньо враховується специфіка країн, що функціонують в умовах воєнних загроз, де стійкість інфраструктури набуває не лише економічного, але й стратегічного безпекового значення.

Таким чином, проведений аналіз дозволяє зробити висновок про відсутність єдиного узгодженого підходу до визначення та забезпечення стійкості критичної інфраструктури. Існуючі наукові та практичні підходи або зосереджуються на окремих аспектах (ризики, відновлення, регулювання), або не враховують повною мірою взаємозв'язок між ними. Це зумовлює необхідність формування комплексного концептуального підходу, який поєднуватиме функціональні, системні, інституційні та технологічні компоненти стійкості з урахуванням специфіки сучасних безпекових викликів та умов функціонування України.

ISSN 2306-6792

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Метою статті є узагальнення теоретичних підходів до визначення сутності стійкості критичної інфраструктури, аналіз закордонного досвіду її забезпечення та обгрунтування напрямів імплементації відповідних підходів в Україні з урахуванням сучасних безпекових викликів.

Методологічну основу дослідження становить сукупність загальнонаукових і спеціальних методів, що забезпечують комплексний аналіз досліджуваної проблематики. Зокрема, застосовано методи теоретичного узагальнення та систематизації (для дослідження сутності стійкості критичної інфраструктури та класифікації підходів до її забезпечення); порівняльний аналіз (для вивчення закордонного досвіду та виявлення особливостей реалізації політики стійкості в різних країнах); системний підхід (для розгляду критичної інфраструктури як складної багаторівневої системи, що функціонує в умовах взаємодії різних секторів і факторів впливу).

Крім того, у дослідженні використано елементи інституційного підходу, що дозволяє проаналізувати нормативно-правове та організаційне забезпечення стійкості критичної інфраструктури, а також метод логічного узагальнення — для формування висновків і обгрунтування напрямів імплементації кращих світових практик в Україні.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Сучасне розуміння забезпечення стійкості критичної інфраструктури сформувалося як результат поступової еволюції управлінських і наукових підходів — від фокусування на фізичному захисті окремих об'єктів до усвідомлення потреби у підтриманні безперервності життєво важливих функцій у складних умовах багатофакторних ризиків.

На початковому етапі домінував підхід захисту критичної інфраструктури, у межах якого ключова увага приділялася охороні об'єктів, запобіганню диверсіям, терористичним актам та фізичним пошкодженням. Така логіка відповідала відносно лінійному баченню загроз, коли основне завдання полягало у зниженні ймовірності руйнування конкретного активу. Проте зростання взаємозалежності секторів, цифровізації та каскадних ризиків продемонструвало обмеженість такого підходу, оскільки навіть добре захищений окремий об'єкт може виявитися вразливим через порушення в суміжних мережах або ланцюгах постачання [3; 9]. Ця зміна бачення чітко простежується і в документах ЄС, і в американській політиці критичної інфраструктури, де акцент поступово змістився від security до security and resilience.

Наступним етапом стало утвердження ширшої парадигми безпеки, що охоплює не лише фізичний захист, а й управління ризиками, запобігання інцидентам, координацію дій суб'єктів, підготовку до реагування та відновлення. У цій логіці критична інфраструктура почала розглядатися не як сукупність ізольованих об'єктів, а як система, від якої залежить стабільність держави, економіки та суспільства. Зокрема, у директиві США Presidential Policy Directive/PPD-21 прямо зазначено, що критична інфраструктура має бути захищеною, стійкою до впливу всіх видів небезпек і спроможною до оперативного відновлення, а політика у цій сфері має охоплювати запобігання, захист, пом'якшення наслідків, реагування та відновлення [9]. Аналогічну логіку закладено і в Директиві (EU) 2022/2557, яка створює надсекторальну рамку для підвищення стійкості критичних суб'єктів в умовах природних, техногенних, гібридних та інших загроз [3].

У результаті сформувався сучасний резильєнтний підхід, у межах якого ключовим об'єктом уваги стає не лише запобігання збою, а здатність системи зберігати критичні функції, адаптуватися до порушень, абсорбувати шок, перебудовувати режими роботи і відновлюватися у прийнятні строки. У науковій літературі саме така логіка дедалі частіше визначається як найбільш адекватна для критичної інфраструктури в умовах складних, взаємопов'язаних і невизначених загроз.

Оглядові праці показують, що сучасні дослідження інфраструктурної резильєнтності дедалі більше переходять від вузького об'єктного аналізу до вивчення міжсекторальних зв'язків, багатозагрозових сценаріїв, мережевих залежностей та інституційної спроможності [10—12]. Важливо, що у межах цієї трансформації йдеться не про заміну захисту або безпеки, а про їх включення до ширшої концептуальної конструкції стійкості.

З огляду на це, доцільно виокремити чотири базові підходи до забезпечення стійкості критичної інфраструктури: ризик-орієнтований, системний, функціональний та резильєнтний. Зазначені підходи не є взаємовиключними; навпаки, кожен із них відображає окремий аналітичний зріз проблеми та водночас має власні обмеження. Для цілей подальшого обгрунтування концептуальних засад доцільним

ISSN 2306-6792

є їх більш предметне порівняння (табл. 1).

Таблиця 1. Ключові підходи до забезпечення стійкості критичної інфраструктури

Складові аналізу	Підходи			
	Ризик-орієнтований	Системний	Функціональний	Резильєнтний
Змістовий акцент	Ідентифікація загроз, вразливостей, ймовірності та наслідків порушень	Розгляд критичної інфраструктури як сукупності взаємопов'язаних секторів, мереж і залежностей	Пріоритет життєво важливих функцій і безперервності послуг, а не лише фізичної цілісності об'єктів	Поєднання запобігання, поглинання впливу, адаптації, реагування та відновлення
Переваги	Дає змогу ранжувати загрози, розподіляти ресурси, формувати пріоритети захисту	Дозволяє виявляти каскадні ефекти, міжсекторальні залежності, критичні вузли	Орієнтує управління на суспільно значущий результат – безперервність послуг	Найбільш комплексний; враховує невизначеність, динамічність загроз і трансформаційний потенціал систем
Обмеження	Схильний до надмірної орієнтації на прогнозовані ризики; гірше працює в умовах невизначеності та комбінованих криз	Висока складність моделювання, потреба у великих масивах даних та міжвідомчій координації	Може недооцінювати структурні слабкі місця системи та довгострокові вразливості	Потребує інтеграції різних інструментів, міжсекторальної взаємодії та розвиненої інституційної спроможності
Практичне значення	Базовий для національних і секторальних оцінок ризику, планування заходів захисту	Необхідний для управління міжгалузевими ризиками та складними інфраструктурними системами	Особливо важливий для енергетики, водопостачання, транспорту, зв'язку, охорони здоров'я	Формує сучасну основу державної політики стійкості критичної інфраструктури

Джерело: складено авторами на основі [10—11; 13—15].

Дані табл. 1 засвідчують, що ризик-орієнтований підхід є методологічно важливим, але сам по собі недостатнім. Його сильна сторона полягає в аналітичній чіткості: він дозволяє структурувати ризики, оцінити їхню імовірність і масштаб наслідків, визначити пріоритети реагування. Саме ця логіка лежить в основі державних оцінок ризиків, які прямо передбачені європейським підходом [3], а також американських рамок управління ризиками [16]. Водночас його слабкість полягає в тому, що він орієнтується переважно на ідентифіковані ризики. За умов гібридних атак, війни, багаторівневих криз і швидких технологічних змін значна частина загроз має нелінійний характер, а отже не завжди може бути повноцінно передбачена у класичній ризиковій моделі. Тому в сучасних дослідженнях дедалі частіше підкреслюється, що ризик-менеджмент має бути вбудований у ширшу логіку стійкості, а не підміняти її [3; 12].

Системний підхід, відображений у табл. 1, є відповіддю на зростання мережевої взаємозалежності критичної інфраструктури. Його принципова перевага полягає в тому, що він дає змогу аналізувати не окремий об'єкт, а мережу зв'язків між секторами. У цьому контексті особливо показовою є логіка Директиви ЄС 2022/2557, у якій акцент зроблено на міжсекторальній та транскордонній взаємозалежності у наданні життєво важливих послуг [3]. Наукові огляди також підтверджують, що сучасна стійкість інфраструктури дедалі частіше аналізується через міжсистемні залежності, каскадні ефекти та мережево-орієнтовані підходи [10—11]. Водночас саме системний підхід є найбільш вимогливим до якості даних, інструментів моделювання та рівня міжінституційної координації. Унаслідок цього в практиці публічного управління він часто декларується, але реалізується лише частково.

Функціональний підхід є особливо цінним тим, що змінює саму точку відліку аналізу: у центрі перебуває не об'єкт як такий, а послуга або функція, збій якої створює неприйнятні наслідки для суспільства. Саме тому в українському законодавстві йдеться про життєво важливі функції та/або послуги [17], а в шведській практиці — про функції, підтримання яких є критично необхідним для збереження функціональності суспільства [18]. Такий підхід є надзвичайно продуктивним для України, оскільки в умовах війни питання полягає не лише в охороні активів, а в забезпеченні електропостачання, зв'язку, води, тепла, перевезень та інших критичних сервісів навіть за часткового пошкодження інфраструктури. Разом із тим функціональний підхід може недооцінювати причини системної вразливості, якщо не поєднується з системним і ризиковим аналізом.

Найбільш комплексним, як видно з табл. 1, є резильєнтний підхід. Його перевага полягає в інтеграції різних фаз управління: від запобігання до адаптації та відновлення. У Директиві ЄС 2022/2557 прямо закріплено, що критичні суб'єкти повинні здійснювати належні технічні, безпекові та організаційні заходи для запобігання інцидентам, захисту від них, реагування, протидії, пом'якшення їх наслідків, поглинання впливів, адаптації та відновлення після інци-

ISSN 2306-6792

дентів [3]. У США аналогічно наголошується на необхідності функціонування в умовах усіх видів загроз, забезпечення швидкого відновлення та узгодженості дій державних, місцевих і приватних суб'єктів [9]. У Швеції стійкість критичної інфраструктури пов'язується з управлінням ризиками, забезпеченням безперервності діяльності, інформаційною та кібербезпекою, а також управлінням небажаними подіями [18]. Отже, резильєнтний підхід не заперечує попередні підходи, а інтегрує їх у цілісну аналітичну рамку. Саме тому він є найбільш продуктивним для країн, які функціонують у середовищі високої невизначеності та багаторазових шоків.

Таким чином, теоретичний аналіз дозволяє зробити принциповий висновок: перехід від моделі захисту до моделі стійкості відображає не просто зміну термінології, а зміну управлінської парадигми. Якщо модель захисту орієнтується переважно на недопущення пошкодження, то модель стійкості виходить із того, що порушення можуть статися, а тому головним стає збереження функціональності системи, її адаптаційна спроможність і швидкість відновлення. Саме ця логіка є методологічною основою подальшого уточнення сутності стійкості критичної інфраструктури.

Слід наголосити, що у сучасній літературі відсутнє повністю уніфіковане визначення стійкості критичної інфраструктури, однак у більшості праць воно формується навколо кількох повторюваних змістовних компонентів.

По-перше, стійкість пов'язується зі здатністю системи протидіяти збуренням і зменшувати вразливість.

По-друге, вона розглядається як здатність зберігати або відновлювати необхідний рівень функціонування після впливу.

По-третє, дедалі частіше наголошується на адаптивній складовій — здатності змінювати внутрішню конфігурацію, режими роботи та управлінські процедури відповідно до нових умов. Наприклад, D. Rehak et al. [19] розглядають стійкість як якість, що зменшує вразливість, мінімізує наслідки загроз, прискорює реагування та відновлення і полегшує адаптацію до руйнівної події. Оглядові дослідження також підтверджують, що у фокусі сучасних визначень перебувають стійкість до впливів, адаптивність, здатність до відновлення та безперервність функціонування [10—12].

Разом з тим, самі визначення часто акцентують різні сторони явища. У нормативних документах ЄС стійкість критичних суб'єктів описується через здатність запобігати, захищатися, реагувати, витримувати, пом'якшувати, поглинати, пристосовуватися і відновлюватися [3]. У шведських матеріалах акцент зроблено на створенні умов для продовження діяльності у кризах і навіть у воєнний час [18].

У фінській практиці стійкість критичних суб'єктів безпосередньо пов'язується із забезпеченням безперервності надання життєво важливих послуг за будь-яких обставин, здатністю до випереджального реагування, управлінням порушеннями функціонування та відновленням [16].

Американський підхід додає до цього ще й виразну міжсекторальну та державно-приватну координацію [9]. Отже, у міжнародному дискурсі стійкість дедалі більше тлумачиться не як технічна характеристика окремого об'єкта, а як інтегральна властивість системи, інституцій та процесів управління.

На цій підставі доцільно запропонувати таке авторське трактування: стійкість критичної інфраструктури — це інтегрована характеристика інфраструктурної системи та механізмів її управління, що відображає здатність забезпечувати безперервність життєво важливих функцій і послуг, протидіяти дестабілізуючим впливам, адаптуватися до змін середовища, абсорбувати наслідки кризових подій та відновлювати належний рівень функціонування в прийнятні строки. Запропоноване визначення, на відміну від вузьких технічних трактувань, поєднує функціональну, системну, інституційну та часову складові. Саме в цьому полягає його методологічна придатність для аналізу критичної інфраструктури в умовах війни та післякризового відновлення.

Для розкриття змісту цього визначення доцільно виокремити чотири базові характеристики стійкості: стійкість до впливів, адаптивність, відновлюваність і безперервність функціонування. Стійкість до впливів відображає спроможність інфраструктури протистояти загрозам або знижувати їх руйнівний ефект ще до моменту повномасштабного порушення. Вона тісно пов'язана з robust design, резервуванням, диверсифікацією, фізичним захистом і кіберзахистом.

Адаптивність характеризує здатність змінювати управлінські, технологічні та організаційні параметри функціонування відповідно до нових умов. Відновлюваність означає спроможність повертати систему до прийнятного рівня працездатності після інциденту, причому важливим є не лише факт відновлення, а його швидкість, пріоритетність та ефективність. Безперервність функціонування є результативним

ISSN 2306-6792

Таблиця 2. Порівняння міжнародних підходів до забезпечення стійкості критичної інфраструктури

Складові порівняння	Країна / наднаціональний рівень			
	ЄС	США	Фінляндія	Швеція
Домінуючий підхід	Інституційно-регуляторний, орієнтований на всі види загроз	Ризик-орієнтований і партнерський	Стратегічно-координаційний, орієнтований на безперервність	Системно-кооперaційний, модель цивільної готовності та всеохоплюючої оборони
Ключові інструменти	Директива ЄС 2022/2557, національні оцінки ризиків, ідентифікація критичних суб'єктів, заходи забезпечення стійкості, повідомлення про інциденти, міждержавна координація	Директива PPD-21, національна координація, державно-приватне партнерство, планування з урахуванням усіх видів загроз, ситуаційна обізнаність, секторальні агентства	Законодавство у сфері стійкості, національний план, національна оцінка ризиків, система управління, процеси ідентифікації та підтримки критичних суб'єктів	Управління ризиками, забезпечення безперервності діяльності, інформаційна та кібербезпека, навчання і тренування, кооперaційне планування
Сильні сторони моделі	Уніфікація підходів, поєднання управління ризиками та забезпечення стійкості, врахування транскордонних і міжсекторальних залежностей	Сильна координація, визнання міжсекторальної взаємозалежності, розвинуті механізми обміну інформацією	Поєднання законодавчого регулювання, стратегічного планування, оцінки ризиків і забезпечення безперервності життєво важливих послуг	Висока інтеграція держави, муніципалітетів і приватного сектору; орієнтація на забезпечення функціонування суспільства
Уроки для України	Гармонізація законодавства, формування єдиної рамки ідентифікації критичних суб'єктів, запровадження обов'язкової оцінки ризиків і заходів забезпечення стійкості	Посилення державно-приватної взаємодії, розвиток ситуаційної обізнаності, поглиблення секторальної спеціалізації	Формування національного плану забезпечення стійкості, регулярна оцінка міжсекторальних і транскордонних залежностей	Розвиток системної підготовки, проведення навчань, впровадження управління безперервністю діяльності та залучення бізнесу до політики забезпечення стійкості

Джерело: складено авторами на основі [3; 9; 13—16; 18; 20—21].

виміром стійкості, оскільки саме вона показує, чи спроможна система забезпечувати безперервність надання життєво важливих послуг навіть в умовах порушених режимів функціонування [3; 16; 18; 19].

Логіку взаємозв'язку цих характеристик можна подати так: загроза або шок → стійкість до впливу → часткове порушення або поглинання впливу → адаптація режимів функціонування → відновлення елементів і зв'язків → безперервність або відновлення критичних послуг.

У такій послідовності безперервність не є ізольованою характеристикою, а виступає кінцевим функціональним результатом взаємодії трьох попередніх складових. Саме тому оцінювати стійкість лише за наявністю захисних механізмів недостатньо; потрібна оцінка повного циклу — від підготовки до відновлення. Цей висновок узгоджується із сучасними підходами до оцінювання стійкості, де поряд із показниками міцності враховуються часові характеристики відновлення, кумулятивні ефекти та динамічна поведінка системи [11—12].

Порівняльний аналіз закордонного досвіду показує, що попри спільну тенденцію до переходу від захисту до стійкості різні країни реалізують цю модель через відмінні інституційні конфігурації (табл. 2). Так, у Європейському Союзі домінує надсекторальна регуляторна рамка, у США — мережевий партнерський підхід із вагомою роллю управління ризиками та публічно-приватної кооперації, у Фінляндії —

ISSN 2306-6792

стратегічно інституціоналізована модель забезпечення безперервності та готовності, а у Швеції — модель цивільної готовності та всеохоплюючої оборони, у межах якої захист критичної інфраструктури інтегрований із забезпеченням безперервності суспільних функцій і кризовою готовністю [3; 9; 16; 18].

Таблиця 2 демонструє, що модель Європейського Союзу є найбільш нормативно структурованою. Її принципова цінність полягає в тому, що вона переводить забезпечення стійкості з декларативної площини у площину обов'язкових процедур. Директива ЄС 2022/2557 вимагає від держав-членів здійснювати національні оцінки ризиків, ідентифікувати критичних суб'єктів, забезпечувати підтримку їхньої стійкості, запроваджувати повідомлення про інциденти та періодично оновлювати відповідні оцінки [3]. Важливо, що аналіз ризиків охоплює природні та техногенні ризики, міжсекторальні та транскордонні залежності, надзвичайні ситуації у сфері громадського здоров'я, гібридні загрози та інші антагоністичні загрози [3]. Отже, європейська модель вирізняється саме процедурною завершеністю, оскільки формує цілісний цикл — від ідентифікації ризиків до встановлення вимог щодо забезпечення стійкості критичних суб'єктів. Водночас її потенційним обмеженням є високий рівень регуляторної складності та потреба у значній адміністративній спроможності для належного виконання цих вимог.

Особливо важливим для розуміння європейського підходу є те, що він виходить із секторно-мережевої логіки. У додатку до Директиви перелічено широкий спектр секторів і підсекторів, серед яких енергетика, транспорт, банківський сектор, фінансова ринкова інфраструктура, охорона здоров'я, питна вода, цифрова інфраструктура, державне управління та інші [3]. Це означає, що ЄС фактично розглядає стійкість як багатосекторний режим функціонування суспільства, а не як питання окремих об'єктів. Для України це особливо значуще, оскільки в умовах війни саме міжсекторальні залежності: енергетика — зв'язок; енергетика — водопостачання; транспорт — логістика -постачання — визначають масштаб каскадних наслідків.

Американська модель, на відміну від європейської, менш централізована в правовому сенсі, але дуже розвинена в координаційному й партнерському аспектах. PPD-21 визначає критичну інфраструктуру як сферу спільної відповідальності уряду, субнаціональних органів влади та приватних власників і операторів [9]. У документі підкреслюється необхідність комплексного та цілісного підходу з урахуванням взаємопов'язаності та взаємозалежності інфраструктур [9].

Таким чином, центральною ідеєю є не лише встановлення правил, а й формування постійно діючої системи обміну інформацією, секторальної спеціалізації, забезпечення ситуаційної обізнаності та координації реагування. Перевагою цієї моделі є її висока адаптивність і практична орієнтованість. Водночас надмірна залежність від партнерських механізмів може зумовлювати нерівномірність реалізації між секторами та територіями.

Фінська модель, відображена в табл. 2, є особливо цікавою для України як приклад поєднання європейської нормативної рамки з національною стратегічною логікою. Після набуття чинності Законом про стійкість критичних суб'єктів 1 липня 2025 року у Фінляндії послідовно розбудовується система, у межах якої національна оцінка ризиків у сфері стійкості, національний план, система управління та процеси ідентифікації і підтримки критичних суб'єктів формують єдиний управлінський цикл [16].

У фінській моделі особливої уваги заслуговує те, що оцінка ризиків безпосередньо охоплює значущі ризики для надання життєво важливих послуг, транскордонні залежності та міжсекторальні взаємозв'язки [16]. Її сильна сторона полягає у тісному поєднанні оцінки ризиків, стратегічного планування та підтримки критичних суб'єктів. Це саме той елемент, якого часто бракує в країнах, де існують окремі документи, але відсутній механізм їх узгодженого поєднання в цілісну систему.

Шведська модель має інший акцент. Вона історично пов'язана з концепцією цивільної готовності та всеохоплюючої оборони, тому критична інфраструктура розглядається не лише крізь призму захисту об'єктів, а як передумова функціонування суспільства в умовах криз і воєнного часу. У матеріалах MSB (Swedish Civil Contingencies Agency) прямо підкреслюється, що суб'єкти, які забезпечують функціонування критичної інфраструктури, мають розвивати стійкість через управління ризиками, забезпечення безперервності діяльності, інформаційну та кібербезпеку, а також управління небажаними подіями [18]. \Крім того, шведський підхід традиційно базується на відповідальності та співпраці між суб'єктами різних рівнів і сфер суспільства [18]. Отже, його сильна сторона полягає у поєднанні інституційної координації з практиками забезпечен-

ISSN 2306-6792

ня безперервності, проведення навчань, розвитку експертних знань і залучення приватного сектору. Для України такий досвід є особливо цінним у частині формування системи цивільної стійкості, у межах якої критична інфраструктура виступає складовою ширшої архітектури національної готовності.

Узагальнюючи закордонний досвід, можна зробити кілька висновків. По-перше, жодна ефективна модель більше не спирається лише на фізичний захист. По-друге, усі результативні системи поєднують ризиковий аналіз, управління безперервністю, координацію суб'єктів і вимірювання спроможності до відновлення. По-третє, вирішальним стає питання не лише правового закріплення, а й інституційної спроможності, обміну даними, вправ і планування. Саме в цій площині міжнародний досвід є найбільш корисним для адаптації в Україні.

Україна вже має базові правові засади у сфері критичної інфраструктури та кібербезпеки. Закон України "Про критичну інфраструктуру" визначає правові та організаційні засади створення та функціонування національної системи захисту критичної інфраструктури [17], а Закон України "Про основні засади забезпечення кібербезпеки України" формує рамку для захисту державних інформаційних ресурсів і критичної інформаційної інфраструктури [22]. Водночас воєнний досвід і міжнародні практики показують, що наявність базового законодавства сама по собі не гарантує належної стійкості. Потрібне подальше поглиблення інституційної, технологічної й координаційної складових.

З огляду на це, першим напрямом має стати нормативно-правова гармонізація. Доцільно розробити й запровадити таку систему вторинного регулювання, яка б зближувала українську модель із логікою CER Directive: національні та секторальні оцінки ризиків, чіткі критерії ідентифікації критичних суб'єктів, вимоги до resilience measures, процедури повідомлення про інциденти, регулярність перегляду ризикових профілів. Це дозволить перейти від загального законодавчого регулювання до більш операціоналізованої моделі управління стійкістю [3; 16; 17].

Другим напрямом є посилення інституційного забезпечення та координації. Закон України "Про критичну інфраструктуру" вже визначає наявність уповноваженого органу, секторальних і функціональних органів, режимів функціонування системи та планів взаємодії [17]. Однак міжнародний досвід показує, що результативність цієї архітектури залежить від якості обміну інформацією, розподілу відповідальності, аналітичної підтримки та міжсекторальної координації. Тому доцільно створити стійкий механізм координації між органами державної влади, операторами, регуляторами, силами безпеки, секторальними міністерствами та органами місцевого самоврядування, який працював би не лише в режимі реагування, а й у режимі постійного планування та профілактики [9; 16—18].

Третім напрямом має бути цифровізація управління критичною інфраструктурою. Йдеться про створення інтегрованих систем моніторингу, ситуаційної обізнаності, обміну даними про загрози, інциденти та залежності між секторами. У США ключовими елементами національної політики у цій сфері визначено спроможність до забезпечення ситуаційної обізнаності та формування базових вимог до даних [9]. Для України це набуває особливої ваги через необхідність оперативного виявлення пошкоджень, оцінки каскадних ефектів та пріоритизації відновлювальних робіт у воєнних умовах. Цифровізація також має охоплювати геоінформаційні системи, цифрові двійники, моделі міжсекторальних залежностей та інструменти сценарного аналізу.

Четвертий напрям — розвиток енергетичної стійкості, безпеки та резильєнтності. Саме енергетика є системоутворюючим сектором, від якого залежать інші інфраструктури. Європейська рамка прямо виокремлює енергетичний сектор як один із ключових [3], тоді як у США енергетичні та комунікаційні системи розглядаються як унікально критичні через їхню базову роль у забезпеченні функціонування всіх інших секторів [9].

Для України доцільно розвивати диверсифікацію джерел енергії, розподілену генерацію, резервні схеми живлення, мікромережі, підвищення гнучкості енергосистеми та пріоритетний захист вузлів, відмова яких спричиняє найбільші каскадні наслідки. У цьому напрямі поняття стійкості має тлумачитися ширше за фізичний захист і включати забезпечення функціональної спроможності енергетичних систем у кризових режимах.

П'ятим напрямом є посилення кіберзахисту об'єктів критичної інфраструктури. Воєнні та гібридні загрози засвідчили, що фізична і цифрова вразливість дедалі частіше формують єдиний контур ризику. Саме тому шведський підхід поєднує забезпечення стійкості з інформаційною та кібербезпекою [18], а українське законодавство у сфері кібербезпеки вже ство-

ISSN 2306-6792

рює основу для подальшого зміцнення захисту критичної інформаційної інфраструктури [20]. Доцільно розробити єдині вимоги до кіберстійкості операторів критичної інфраструктури, запровадити регулярні кібернавчання, алгоритми спільного реагування та інтегрувати кіберризики у загальні оцінки ризиків об'єктів і секторів.

Шостим напрямом є розвиток міжсекторальної взаємодії та партнерства. У всіх розглянутих міжнародних моделях критична інфраструктура більше не є виключно сферою держави. Ефективна політика стійкості потребує залучення операторів, бізнесу, місцевих громад, галузевих асоціацій, наукових центрів і структур цивільного захисту [9; 18]. Для України доцільно створити постійні координаційні механізми, спільні програми навчань, секторальні та міжсекторальні протоколи обміну інформацією, а також формати, в яких бізнес буде не лише об'єктом регулювання, а повноцінним партнером формування стійкості. Саме ця логіка дозволяє перевести систему із реактивного режиму в превентивно-адаптивний.

Отже, імплементація міжнародного досвіду в Україні не повинна зводитися до механічного перенесення окремих норм чи організаційних моделей. Йдеться про формування власної національної моделі стійкості критичної інфраструктури, в якій європейська регуляторна логіка, американська координаційна гнучкість, фінська планувальна послідовність і шведська культура суспільної готовності будуть адаптовані до українських безпекових реалій. Саме така комбінація може стати підгрунтям для переходу від фрагментарного захисту окремих об'єктів до системного забезпечення життєво важливих функцій держави, економіки та суспільства.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У статті узагальнено теоретичні підходи до забезпечення стійкості критичної інфраструктури та встановлено, що сучасний науковий і управлінський дискурс відображає перехід від моделі захисту об'єктів до інтегрованої моделі стійкості, орієнтованої на забезпечення безперервності життєво важливих функцій, адаптацію до змін і відновлення після кризових впливів. Показано, що ризик-орієнтований, системний, функціональний і resilience-підхід розкривають різні аспекти забезпечення стійкості, але лише їх комплексне поєднання формує цілісну основу державної політики.

Уточнено сутність категорії стійкість критичної інфраструктури як інтегрованої характеристики інфраструктурних систем і механізмів їх управління, що відображає здатність забезпечувати безперервність життєво важливих послуг, протидіяти загрозам, адаптуватися до змін і відновлювати функціонування у прийнятні строки. Виокремлено ключові характеристики стійкості: стійкість до впливів, адаптивність, відновлюваність і безперервність функціонування.

На основі аналізу міжнародного досвіду обгрунтовано, що найбільш результативні моделі поєднують нормативно-правове регулювання, управління ризиками, планування безперервності, цифровий моніторинг, кіберзахист та міжсекторальну координацію. Встановлено доцільність адаптації елементів європейської регуляторної моделі, американського партнерського підходу, фінської системи стратегічного планування та шведської моделі цивільної стійкості до умов України.

З урахуванням отриманих результатів запропоновано такі адресні практичні рекомендації:

— Кабінету Міністрів України та Міністерству економіки, довкілля та сільського господарства України доцільно розробити та затвердити національну стратегію забезпечення стійкості критичної інфраструктури, яка б інтегрувала вимоги європейських підходів і передбачала регулярні національні та секторальні оцінки ризиків;

— Раді національної безпеки і оборони України необхідно посилити координацію міжвідомчої взаємодії у сфері стійкості критичної інфраструктури шляхом створення єдиного аналітично-координаційного механізму управління міжсекторальними ризиками та кризовими ситуаціями;

— Міністерству розвитку громад та територій України спільно з обласними військовими адміністраціями варто запровадити регіональні програми забезпечення стійкості критичної інфраструктури з урахуванням територіальної специфіки, ризиків та критичних залежностей між секторами;

— Міністерству енергетики України доцільно активізувати розвиток розподіленої генерації, резервних енергетичних систем і мікромереж з метою підвищення стійкості енергетичного сектору як базового елементу критичної інфраструктури;

— Міністерству цифрової трансформації України та Державній службі спеціального зв'язку та захисту інформації України необхі-

ISSN 2306-6792

дно створити інтегровану цифрову систему моніторингу, обміну даними та ситуаційної обізнаності щодо стану критичної інфраструктури і кіберзагроз;

— Службі безпеки України та Національному координаційному центру кібербезпеки доцільно посилити систему кіберзахисту критичної інфраструктури шляхом впровадження єдиних стандартів кіберстійкості, проведення регулярних кібернавчань і вдосконалення механізмів реагування на інциденти.

Практичне значення отриманих результатів полягає у можливості їх використання під час формування державної політики у сфері забезпечення стійкості критичної інфраструктури, розроблення стратегічних і нормативних документів, а також удосконалення організаційно-управлінських механізмів функціонування інфраструктурних систем в умовах сучасних безпекових викликів і післявоєнного відновлення України.

Перспективи подальших досліджень полягають у розробленні методичних підходів до кількісного оцінювання рівня стійкості критичної інфраструктури з урахуванням міжсекторальних залежностей і каскадних ефектів, а також формуванні моделей управління стійкістю критичної інфраструктури на регіональному та муніципальному рівнях із урахуванням специфіки територіальних громад і процесів децентралізації.

Таким чином, забезпечення стійкості критичної інфраструктури трансформується з вузького завдання захисту об'єктів у стратегічний пріоритет державної політики, від реалізації якого залежить здатність України до відновлення, розвитку та інтеграції у європейський простір.

Література:

1. Mentges A., Halekotte L., Schneider M., Demmer T., Lichte D. A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures. International Journal of Disaster Risk Reduction. 2023. Vol. 96. Article 103893. DOI: https://doi.org/10.1016/j.ijdrr.-2023.103893.

2. Trump B. D. et al. Threat-Agnostic Resilience: Framing and Application for Critical Infrastructure. ArXiv. Cornell University. 2025. DOI: https://doi.org/10.48550/arXiv.2501.01318.

3. 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/eng (дата звернення: 15.03.2026).

4. Fernandez J. M., Johnson T., Magnus K. Navigating the EU Critical Entities Resilience Directive. Deloitte. 2026. URL: https://www.deloitte.com/tr/tr/ services/consulting-risk/perspectives/navigating-the-eu-critical-entities-resilience-directive.html (дата звернення: 11.03.2026).

5. Critical Entities Resilience Directive. CER. 2026. 12 March. URL: https://www.critical-entities-resilience-directive.com/ (дата звернення: 16.03.2026).

6. CER Directive: where does Europe stand on critical infrastructure resilience? Wavestone. 2026. 26 January. URL: https://www.wavestone.com/en/ insight/critical-infrastructure-cybersecurity-cer-directive/ (дата звернення: 11.03.2026).

7. Holl J., Antos M. Critical Entities' Resilience Directive: Deloitte Cyber Regulatory Compliance. Deloitte. 2025. URL: https://www.deloitte.com/content/dam/assets-zone2/cz-sk/cs/docs/services/consulting/cyber/Critical-Entities-Resilience-CER-leaflet-ENG.pdf (дата звернення: 09.03.2026).

8. Critical infrastructure resilience at EU-level. European Commission. 2026. 13 January. URL: https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en (дата звернення: 07.03.2026).

9. Directive on Critical Infrastructure Security and Resilience: Presidential Policy Directive/PPD-21. 2013. February 12. URL: https://www.govinfo.-gov/content/pkg/DCPD-201300092/html/DCPD-201300092.htm (дата звернення: 09.03.2026).

10. Liu W., Shan M., Zhang S., Zhao X., Zhai Z. Resilience in Infrastructure Systems: A Comprehensive Review. Buildings. 2022. Vol. 12. No. 6. Article. 759. DOI: https://doi.org/10.3390/buildings12060759.

11. Sathurshan M., Saja A., Thamboo J., Haraguchi M., Navaratnam S. Resilience of Critical Infrastructure Systems: A Systematic Literature Review of Measurement Frameworks. Infrastructures. 2022. Vol. 7. No. 5. Article. 67. DOI: https://doi.org/10.3390/infrastructures7050067.

12. Rathnayaka B., Siriwardana C., Robert D., Amaratunga D., Setunge S. Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review. International Journal of Disaster Risk Reduction. 2022. Vol. 81. Article 103123. DOI: https://doi.org/10.1016/j.ijdrr.2022.103123.

13. Хаустова В. Є., Трушкіна Н. В. Загрози розвитку критичної інфраструктури: сутність і класифікація. Проблеми економіки. 2025. № 3.

ISSN 2306-6792

С. 89—104. DOI: https://doi.org/10.32983/2222-0712-2025-3-89-104.

14. 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. https://doi.org/10.32983/2222-0712-2025-4-336-351.

15. 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.

16. National plan and risk assessment to guide operations. Ministry of the Interior, Finland. 2026. URL: https://intermin.fi/en/national-plan-and-risk-assessment (дата звернення: 10.03.2026).

17. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX (із змінами, у редакції від 21.09.2024). Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 12.03.2026).

18. Critical infrastructure protection — Increased resilience through risk management, business continuity management, information and cybersecurity, and managing unwanted events. Swedish Civil Contingencies Agency (MSB). 2024. December. URL: https://rib.msb.se/filer/pdf/30973.pdf (дата звернення: 12.03.2026).

19. Rehak D., Senovsky P., Slivkova S. Resilience of Critical Infrastructure Elements and Its Main Factors. Systems. 2018. Vol. 6. No. 2. Article 21. DOI: https://doi.org/10.3390/systems6020021.

20. Caetano H. O., Desuo N. L., Fogliatto M. S. S., Maciel C. D. Resilience assessment of critical infrastructures using dynamic Bayesian networks and evidence propagation. Reliability Engineering and System Safety. 2024. Vol. 241. Article 109691. DOI: https://doi.org/10.1016/j.ress.2023.109691.

21. Swedish Civil Contingencies Agency to cooperate with Ukraine to improve protection of critical infrastructure. Government Offices of Sweden. 2025. 27 February. URL: https://www.government.se/press-releases/2025/02/swedish-civil-contingencies-agency-to-cooperate-with-ukraine-to-improve-protection-of-critical-infrastructure/ (дата звернення: 13.03.2026).

22. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII (із змінами, у редакції від 21.09.2024). Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/ laws/show/2163-19#Text (дата звернення: 13.03.2026).

References:

1. Mentges, A., Halekotte, L., Schneider, M., Demmer, T. and Lichte, D. (2023), "A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures", International Journal of Disaster Risk Reduction, vol. 96, 103893, https://doi.org/10.1016/j.ijdrr.-2023.103893.

2. Trump, B. D. et al. (2025), "Threat-Agnostic Resilience: Framing and Application for Critical Infrastructure", ArXiv, Cornell University, https://doi.org/10.48550/arXiv.2501.01318.

3. European Parliament and Council (2022), "Directive (EU) 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC", Official Journal of the European Union, L 333, pp. 164—198, Available at: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng (Accessed 15 March 2026).

4. Fernandez, J. M., Johnson, T. and Magnus, K. (2026), "Navigating the EU Critical Entities Resilience Directive", Deloitte, Available at: https://www.deloitte.com/tr/tr/services/consulting-risk/perspectives/navigating-the-eu-critical-entities-resilience-directive.html (Accessed 11 March 2026).

5. Critical Entities Resilience Directive (2026), Available at: https://www.critical-entities-resilience-directive.com/ (Accessed 16 March 2026).

6. Wavestone (2026), "CER Directive: where does Europe stand on critical infrastructure resilience?", 26 January, Available at: https://www.wavestone.com/en/insight/critical-infrastructure-cybersecurity-cer-directive/ (Accessed 11 March 2026).

7. Holl, J. and Antos, M. (2025), "Critical Entities' Resilience Directive: Deloitte Cyber Regulatory Compliance", Deloitte, Available at: https://www.deloitte. com/content/dam/assets-zone2/cz-sk/cs/docs/services/consulting/cyber/Critical-Entities-Resilience-CER-leaflet-ENG.pdf (Accessed 9 March 2026).

8. European Commission (2026), "Critical infrastructure resilience at EU-level", 13 January, Available at: https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en (Accessed 7 March 2026).

9. The White House (2013), "Directive on Critical Infrastructure Security and Resilience: Presidential Policy Directive/PPD-21", 12 February, Available at: https://www.govinfo.gov/content/pkg/DCPD-201300092/html/DCPD-201300092.htm (Accessed 9 March 2026).

ISSN 2306-6792

10. Liu, W., Shan, M., Zhang, S., Zhao, X. and Zhai, Z. (2022), "Resilience in Infrastructure Systems: A Comprehensive Review", Buildings, vol. 12 (6), 759, https://doi.org/10.3390/buildings12060759.

11. Sathurshan, M., Saja, A., Thamboo, J., Haraguchi, M. and Navaratnam, S. (2022), "Resilience of Critical Infrastructure Systems: A Systematic Literature Review of Measurement Frameworks", Infrastructures, vol. 7 (5), 67, https://doi.org/10.3390/infrastructures7050067.

12. Rathnayaka, B., Siriwardana, C., Robert, D., Amaratunga, D. and Setunge, S. (2022), "Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review", International Journal of Disaster Risk Reduction, vol. 81, 103123, https://doi.org/10.1016/j.ijdrr.-2022.103123.

13. Khaustova, V. Ye. and Trushkina, N. V. (2025), "Threats to critical infrastructure development: essence and classification", The Problems of Economy, vol. 3, pp. 89—104, https://doi.org/10.32983/2222-0712-2025-3-89-104.

14. Khaustova, V. Ye. and Trushkina, N. V. (2025), "Theoretical approaches to the essence of the concept of critical infrastructure: international, spatial and resilience dimensions", The Problems of Economy, vol. 4, pp. 336—351, https://doi.org/10.32983/2222-0712-2025-4-336-351.

15. Kyzym, M. O., Kozyrieva, O. V. and Trushkina, N. V. (2026), "International instruments for post-war reconstruction of critical infrastructure and their adaptation for the regions of Ukraine", Efektyvna ekonomika, vol. 1, https://doi.org/10.32702/2307-2105.2026.1.22.

16. Ministry of the Interior, Finland (2026), "National plan and risk assessment to guide operations", Available at: https://intermin.fi/en/national-plan-and-risk-assessment (Accessed 10 March 2026).

17. Verkhovna Rada of Ukraine (2024), "On Critical Infrastructure: Law of Ukraine No. 1882-IX of 16 November 2021 (as amended)", Available at: https://zakon.rada.gov.ua/laws/show/1882-20#Text (Accessed 12 March 2026).

18. Swedish Civil Contingencies Agency (MSB) (2024), "Critical infrastructure protection — Increased resilience through risk management, business continuity management, information and cybersecurity, and managing unwanted events", Available at: https://rib.msb.se/filer/pdf/30973.pdf (Accessed 12 March 2026).

19. Rehak, D., Senovsky, P. and Slivkova, S. (2018), "Resilience of Critical Infrastructure Elements and Its Main Factors", Systems, vol. 6(2), 21, https://doi.org/10.3390/systems6020021.

20. Caetano, H.O., Desuo, N.L., Fogliatto, M.S.S. and Maciel, C.D. (2024), "Resilience assessment of critical infrastructures using dynamic Bayesian networks and evidence propagation", Reliability Engineering and System Safety, vol. 241, 109691, https://doi.org/10.1016/j.ress.2023.109691.

21. Government Offices of Sweden (2025), "Swedish Civil Contingencies Agency to cooperate with Ukraine to improve protection of critical infrastructure", 27 February, Available at: https://www.government.se/press-releases/2025/02/swedish-civil-contingencies-agency-to-cooperate-with-ukraine-to-improve-protection-of-critical-infrastructure/ (Accessed 13 March 2026).

22. Verkhovna Rada of Ukraine (2024), "On the Basic Principles of Cybersecurity of Ukraine: Law of Ukraine No. 2163-VIII of 5 October 2017 (as amended)", Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text (Accessed 13 March 2026).

Отримано редакцією журналу / Received: 27.03.26
Прорецензовано / Revised: 03.04.26
Схвалено до друку / Accepted: 09.04.26

ISSN 2306-6792