УДК 330.34:338.4:351.86:005.591.6
JEL Classification: E61; H11; H54; O18

ДЕРЖАВНА ПОЛІТИКА РОЗВИТКУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У КРАЇНАХ СВІТУ: ПРИНЦИПИ ПОБУДОВИ, МЕХАНІЗМИ ПІДТРИМКИ ТА РЕАЛІЗАЦІЇ

©2026 КИЗИМ М. О., ТРУШКІНА Н. В.

УДК 330.34:338.4:351.86:005.591.6
JEL Classification: E61; H11; H54; O18

Кизим М. О., Трушкіна Н. В.

Державна політика розвитку критичної інфраструктури у країнах світу: принципи побудови, механізми підтримки та реалізації

У статті здійснено комплексний порівняльний аналіз державної політики розвитку критичної інфраструктури у країнах світу з акцентом на принципи її побудови, механізми підтримки та моделі реалізації. Обґрунтовано, що в умовах зростання природних, техногенних, кібернетичних і гібридних загроз державна політика у сфері критичної інфраструктури еволюціонує від об'єктно-орієнтованої логіки захисту до сервісної парадигми резильєнтності, у межах якої ключовим критерієм критичності та ефективності виступає безперервність надання життєво важливих послуг і управління міжсекторальними та транскордонними залежностями. Методологічну основу дослідження становить комплексний міждисциплінарний підхід, що поєднує інструменти публічного управління, економічного та інституційного аналізу. Застосовано методи порівняльного, структурно-функціонального та логіко-аналітичного аналізу, а також матричний підхід до зіставлення національних моделей державної політики розвитку критичної інфраструктури. Інформаційну базу сформовано на основі аналітичних матеріалів ОЕСР, Світового банку, Європейської комісії, ENISA, нормативно-правових актів ЄС, а також наукових публікацій вітчизняних і зарубіжних учених. У результаті дослідження систематизовано ключові принципи формування державної політики розвитку критичної інфраструктури, зокрема сервісну орієнтацію, ризик-орієнтованість, резильєнтність повного циклу, партнерські взаємовідносини, інституційну визначеність та кіберпріоритет. Узагальнено механізми підтримки такої політики, включаючи інституційні, регуляторні, фінансові, партнерські та інформаційно-аналітичні інструменти. Проведений порівняльний аналіз європейської CER-орієнтованої моделі, північноамериканської секторної моделі, балтійського кіберорієнтованого підходу та азійських технокібермоделей дозволив виявити їхні переваги й обмеження з позицій результативності та керованості ризиків. На основі отриманих результатів обґрунтовано практичні рекомендації щодо вдосконалення механізмів підтримки та реалізації державної політики розвитку критичної інфраструктури, а також визначено напрями імплементації кращих світових практик у процес повоєнної відбудови економіки України з фокусом на підвищення національної стійкості та економічної безпеки.

Ключові слова: *сектори економіки, критична інфраструктура, державна політика, резильєнтність, життєво важливі послуги, управління ризиками, міжсекторальні залежності, механізми підтримки, інституційна спроможність, публічно-приватне партнерство, кіберстійкість, секторальне врядування, економічна безпека, національна стійкість, повоєнне відновлення економіки.*

DOI: *https://doi.org/10.32983/2222-0712-2026-22-33*

Табл.: *7.* ***Бібл.:*** *31.*

Кизим Микола Олександрович *– доктор економічних наук, професор, член-кореспондент НАН України, головний науковий співробітник сектора енергетичної безпеки та енергозбереження відділу промислової політики та енергетичної безпеки, Науково-дослідний центр індустріальних проблем розвитку НАН України (пров. Інженерний, 1а, 2 пов., Харків, 61166, Україна)*

E-mail: *m.kyzym@gmail.com*

ORCID: *https://orcid.org/0000-0001-8948-2656*

Researcher ID: *https://www.webofscience.com/wos/author/record/1859367*

Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57216130870*

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*

UDC 330.34:338.4:351.86:005.591.6
JEL Classification: E61; H11; H54; O18

Kyzym M. O., Trushkina N. V. The State Policy for the Development of Critical Infrastructure in Countries Around the World: Principles of Construction, Support Mechanisms, and Implementation

The article provides a comprehensive comparative analysis of State policy for the development of critical infrastructure in countries around the world, focusing on the principles of its construction, support mechanisms, and implementation models. It is substantiated that under conditions of increasing natural, man-made,

cyber, and hybrid threats, State policy in the field of critical infrastructure is evolving from an object-oriented protection logic to a service-oriented resilience paradigm, within which the key criterion of criticality and effectiveness is the continuity of the provision of vital services and the management of cross-sectoral and transboundary dependencies. The methodological basis of the study is a comprehensive interdisciplinary approach that combines tools of public administration, economic, and institutional analysis. Methods of comparative, structural-functional, and logical-analytical analysis were applied, as well as a matrix approach to comparing national models of State policy for critical infrastructure development. The information base was formed on the basis of analytical materials from the OECD, the World Bank, the European Commission, ENISA, EU regulatory acts, as well as scientific publications by domestic and foreign researchers. As a result of the study, the key principles of forming State policy for critical infrastructure development were systematized, in particular service orientation, risk-orientation, full-cycle resilience, partnership relations, institutional certainty, and cyber priority. Mechanisms for supporting such policy were summarized, including institutional, regulatory, financial, partnership, and information-analytical tools. The conducted comparative analysis of the European CER-oriented model, the North American sectoral model, the Baltic cyber-oriented approach, and the Asian techno-cyber models made it possible to identify their advantages and limitations in terms of effectiveness and risk manageability. Based on the obtained results, practical recommendations were substantiated for improving mechanisms to support and implement State policy for the development of critical infrastructure, as well as directions for implementing the best global practices in the postwar reconstruction of Ukraine's economy with a focus on enhancing national resilience and economic security.

Keywords: *economic sectors, critical infrastructure, State policy, resilience, vital services, risk management, cross-sectoral dependencies, support mechanisms, institutional capacity, public-private partnership, cyber resilience, sectoral governance, economic security, national resilience, postwar economic recovery.*

Tabl.: *7.* ***Bibl.:*** *31.*

Kyzym Mykola O. *– Doctor of Sciences (Economics), Professor, Corresponding Member of NAS of Ukraine, Chief Research Scientist, Sector of Energy Security and Energy Efficiency of 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: *m.kyzym@gmail.com*

ORCID: *https://orcid.org/0000-0001-8948-2656*

Researcher ID: *https://www.webofscience.com/wos/author/record/1859367*

Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57216130870*

Trushkina Nataliia V. *– Candidate of Sciences (Economics), Senior Research Fellow, Senior Research Fellow, 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*

Вступ. У сучасному світі критична інфраструктура відіграє ключову роль у забезпеченні безперервного функціонування економік, життєдіяльності населення та спроможності держав виконувати базові публічні функції. Енергетичні системи, транспортні мережі, водопостачання, цифрова та телекомунікаційна інфраструктура, об'єкти охорони здоров'я й фінансові платіжні системи формують матеріальну основу соціально-економічної стабільності та національної безпеки. Зростання міжсекторальних і транскордонних взаємозалежностей призводить до того, що порушення функціонування окремих елементів критичної інфраструктури дедалі частіше набувають системного характеру, спричиняючи каскадні ефекти в суміжних секторах і регіонах [1; 2].

Масштаби економічних і соціальних втрат, пов'язаних із порушеннями розвитку критично важливих об'єктів інфраструктури, упродовж останніх років суттєво зростають. За оцінками Організації економічного співробітництва та розвитку [3], прямі й непрямі економічні збитки від масштабних інфраструктурних збоїв можуть сягати від 1 до 3% ВВП окремих країн залежно від тривалості та сектору ураження.

Світовий банк [4] наголошує, що лише перебої в електропостачанні та транспортних мережах у країнах із середнім рівнем доходу щорічно призводять до втрати десятків мільярдів доларів через зниження продуктивності, переривання ланцюгів постачання та скорочення інвестиційної активності. За даними міжнародних страхових та аналітичних агентств, економічні збитки одного масштабного інфраструктурного інциденту у розвинених країнах оцінюються у середньому сотнями мільйонів доларів, а у випадку багатоденних відключень або системних аварій – мільярдами доларів [5].

Додатковим чинником актуалізації проблеми є ускладнення глобального середовища ризиків, у якому функціонують життєво важливі сектори економіки. Зміна клімату зумовлює зростання частоти та інтенсивності екстремальних погодних явищ, що безпосередньо впливають на енергетичні, транспортні й комунальні системи. За оцінками Міжурядової групи експертів зі зміни клімату [6], до 2050 р. кліматичні ризики можуть підвищити вразливість інфраструктурних систем у багатьох регіонах світу на 30-50% порівняно з поточним рівнем. Паралельно зростає вплив техногенних і кіберзагроз. Так, Європейське агентство з кібербезпеки (ENISA) [7] фіксує стійку тенденцію до збільшення кількості кібератак на об'єкти критичної інфраструктури, причому енергетика, транспорт і цифрові сервіси входять до трійки найбільш уразливих секторів. Унаслідок мережевого характеру сучасних інфраструктур навіть локальні інциденти можуть трансфор-

муватися у масштабні системні збої з транскордонними наслідками.

У відповідь на ці виклики уряди країн світу дедалі активніше переосмислюють підходи до управління критичною інфраструктурою, переходячи від вузької логіки захисту окремих об'єктів до формування комплексної державної політики її розвитку. Така політика охоплює не лише питання фізичної безпеки, а й довгострокове планування, інституційну координацію, фінансову підтримку, залучення приватного сектору та інтеграцію інфраструктурних рішень у ширші стратегії економічного розвитку й національної безпеки [3; 8].

Водночас міжнародний досвід свідчить про істотні відмінності між країнами щодо принципів побудови державної політики у сфері критичної інфраструктури, механізмів її підтримки та моделей реалізації. Ці відмінності зумовлюються рівнем економічного розвитку, інституційною спроможністю держави, характером загроз і доступом до фінансових ресурсів.

Таким чином, на глобальному рівні формується комплексна науково-практична проблема, що полягає у необхідності системного осмислення державної політики розвитку критичної інфраструктури в умовах зростання ризиків, ускладнення інфраструктурних взаємозалежностей і посилення транскордонних ефектів. Актуальність цієї проблеми підтверджується масштабами економічних втрат від інфраструктурних збоїв, результатами міжнародних емпіричних досліджень і практикою країн світу, що дедалі частіше розглядають критичну інфраструктуру як стратегічний ресурс довгострокової стійкості та конкурентоспроможності.

Аналіз останніх досліджень і публікацій. Проблематика розвитку критичної інфраструктури та формування державної політики у цій сфері є предметом активних наукових досліджень зарубіжних і вітчизняних учених, а також аналітичних матеріалів міжнародних організацій. У сучасному науковому дискурсі критична інфраструктура здебільшого розглядається не лише як сукупність стратегічно важливих об'єктів, а як складна соціально-економічна система, що потребує комплексних управлінських і політичних рішень.

Вагомий внесок у дослідження питань резильєнтності та управління критичною інфраструктурою зроблено експертами Організації економічного співробітництва та розвитку [3]. У відповідних аналітичних звітах підкреслюється, що ефективність державної політики у сфері критичної інфраструктури визначається якістю публічного управління, міжвідомчою координацією та здатністю інтегрувати питання інфраструктурної стійкості у ширші стратегії соціально-економічного розвитку [3]. Особлива увага приділяється переходу від реактивних заходів захисту до проактивної політики розвитку та управління ризиками.

Інституційні й економічні аспекти державної політики розвитку критичної інфраструктури ґрунтовно представлено у працях експертів Світового банку [4]. У дослідженнях критична інфраструктура розглядається як ключовий чинник довгострокової економічної стійкості, а державна політика – як інструмент зменшення системних економічних втрат, пов'язаних з інфраструктурними збоями [4]. Обґрунтовується доцільність поєднання інвестиційних, регуляторних і партнерських механізмів у реалізації політики розвитку критичної інфраструктури.

Європейський вимір державної політики у сфері критичної інфраструктури відображено у матеріалах Європейського парламенту та аналітичних дослідженнях Європейської парламентської дослідницької служби. У роботі [8] наголошується, що політика держав-членів ЄС все більше орієнтується на принципи резильєнтності, безперервності надання життєво важливих послуг і транскордонної координації, водночас зберігаючи істотні відмінності між національними моделями реалізації.

Окремий напрям досліджень присвячено безпековому та кібернетичному вимірам розвитку критичної інфраструктури. У звіті Європейського агентства з кібербезпеки [7] аналізуються тенденції зростання кіберзагроз для інфраструктурних мереж і підкреслюється необхідність інтеграції кіберстійкості в загальну архітектуру державної політики розвитку критичної інфраструктури.

Теоретико-методологічні засади формування державної політики та публічного управління критичною інфраструктурою розкрито у працях зарубіжних дослідників. Так, у публікації E. Wells et al. [9] інфраструктурна політика трактується як складова багаторівневого управління, що поєднує стратегічне планування, регулювання та реалізацію через взаємодію державних і недержавних акторів.

У вітчизняній науковій літературі проблематика критичної інфраструктури розглядається крізь призму організаційно-правових засад, інституційного забезпечення та безпекових аспектів державної політики. Значну увагу цим питанням приділено у працях українських учених (Д. Бірюков, С. Кондратов, О. Насвіт, О. Суходоля [10]; Л. Арсенович [11]; О. Єрменчук [12] та ін.), у яких аналізуються підходи до захисту, управління та розвитку критичної інфраструктури в умовах зростання зовнішніх загроз.

Питання стійкості критичної інфраструктури та інституційних механізмів її забезпечення у міжнародному вимірі досліджуються також у порівняльних роботах, присвячених досвіду країн ЄС, НАТО та України. У цих дослідженнях [13] наголошується на ролі державної координації та міжсекторальної взаємодії у забезпеченні резильєнтності критичної інфраструктури.

На підставі узагальнення результатів аналізу публікацій виявлено низку наукових прогалин, які обмежують цілісне осмислення державної політики розвитку критичної інфраструктури у міжнародному вимірі.

По-перше, у значній частині досліджень домінує безпеково-захисний підхід, тоді як проблематику розвитку критичної інфраструктури як самостійного напряму державної політики розкрито фрагментарно. Недостатньо систематизовано питання поєднання інфраструктурного планування, модернізації, інвестиційної політики та резильєнтності в єдиній архітектурі державної стратегії розвитку критичної інфраструктури.

По-друге, наявні роботи часто зосереджуються на окремих секторах або інструментах без належного врахування міжсекторальних взаємозалежностей і каскадних

ефектів, що є визначальною характеристикою сучасної критичної інфраструктури. Унаслідок цього недостатньо розкрито питання управління системними ризиками на рівні державної політики.

По-третє, попри наявність порівняльних оглядів, залишається обмеженою типологізація принципів побудови державної політики у сфері критичної інфраструктури. Ці принципи часто декларуються, але не пов'язуються з конкретними рішеннями щодо інституційної архітектури, моделей координації та механізмів відповідальності.

По-четверте, недостатньо систематизовано механізми підтримки державної політики розвитку критичної інфраструктури. У літературі переважає опис окремих фінансових або регуляторних інструментів, тоді як потребує поглиблення комплексне групування механізмів за їх функціональним призначенням та умовами результативності у різних країнах світу.

По-п'яте, у низці досліджень основна увага приділяється нормативно-правовим аспектам, тоді як питання практичної реалізації державної політики, міжвідомчої координації, моніторингу та оцінювання результативності залишаються менш розкритими.

По-шосте, з урахуванням зростання кіберризиків і гібридних загроз актуальною залишається прогалина щодо інтеграції кіберстійкості та кліматичної адаптації в політику розвитку критичної інфраструктури, яка часто розглядається фрагментарно.

Отже, попри значний науковий доробок, зберігається потреба у системному порівняльному аналізі державної політики розвитку критичної інфраструктури через призму принципів її побудови, механізмів підтримки та практик реалізації у країнах світу, що зумовлює актуальність подальших досліджень у цьому напрямі.

З огляду на виявлені наукові прогалини та актуальність проблематики у міжнародному вимірі, **метою цього** дослідження є обґрунтування й систематизація принципів формування державної політики розвитку критичної інфраструктури у країнах світу, а також виокремлення та узагальнення механізмів її підтримки й реалізації на основі порівняльного аналізу зарубіжних практик.

Методологічну основу дослідження становить комплексний міждисциплінарний підхід, який інтегрує інструментарій публічного управління, економічного аналізу та інституційної теорії. Для досягнення мети використано методи аналізу й синтезу, порівняльного та структурно-функціонального аналізу, класифікації, логіко-аналітичний метод, а також інституційний підхід.

Інформаційну базу сформовано на основі аналітичних матеріалів і звітів міжнародних організацій (OECD, World Bank, European Commission, ENISA), результатів міжнародних емпіричних досліджень, нормативно-правових документів Європейського Союзу, а також наукових публікацій вітчизняних і зарубіжних учених з проблематики державної політики та розвитку критичної інфраструктури в умовах багатокомпонентних загроз.

Застосування зазначеного методичного інструментарію дало змогу сформувати цілісну аналітичну рамку, у межах якої принципи побудови державної політики розвитку критичної інфраструктури, механізми її підтримки та практики реалізації розглядаються як взаємопов'язані елементи єдиного управлінського процесу в різних країнах світу.

Викладення основного матеріалу дослідження. В умовах зростання різноманітних (природних, техногенних, інформаційних, кібернетичних, гібридних) загроз державна політика у сфері критичної інфраструктури (KI) еволюціонує від об'єктно-орієнтованої логіки «захисту активів» до сервісної логіки забезпечення безперервності життєво важливих послуг та управління міжсекторальними взаємозалежностями [3; 4]. Така трансформація зумовлена тим, що сучасні інфраструктури функціонують як мережеві системи (енергетика, транспорт, зв'язок, водопостачання, фінансові послуги, цифрові сервіси тощо), де збій у критичному вузлі здатний спричиняти каскадні відмови, масштабуватися у просторі й часі та переходити у площину макроекономічних втрат [3; 4].

З позицій публічного управління це означає, що політика розвитку критичної інфраструктури має поєднувати щонайменше чотири взаємопов'язані блоки: (1) нормативне визначення критичності, (2) ризик-орієнтоване планування; (3) механізми підтримки (інституційні / регуляторні / фінансові / партнерські); (4) модель реалізації та нагляду (координаційна архітектура, вимоги до операторів, інформаційний обмін, стрес-тести, безперервність бізнес/послуг тощо) [3; 14]. Отже, доказовість такого підходу доцільно розкривати через: (а) емпіричні інциденти та їхні наслідки; (б) рамкові регуляторні вимоги (насамперед CER-логіку в Європі); (в) порівняння національних моделей; (г) зіставлення інструментів розвитку та резильєнтності.

Емпіричні приклади (табл. 1) переконливо демонструють, що порушення функціонування критично важливих об'єктів інфраструктури спричиняють не лише прямі руйнування, а й значні непрямі збитки через зупинку виробництва, логістики, сервісів і «ефект доміно» у суміжних секторах [3; 4]. Зокрема, узагальнення OECP щодо блекауту США–Канада (2003 р.) підкреслює масштаб впливу на населення та економіку, тоді як офіційний звіт Task Force документує причини, перебіг інциденту та управлінські рекомендації для запобігання повторенням [3; 15].

Аналогічно японські урядові матеріали щодо тайфунів 2019 року (зокрема Гахаі) фіксують тривалі відключення та проблеми відновлення життєво важливих інфраструктурних послуг (електроенергія, зв'язок), що вимагає удосконалення державних механізмів реагування й відбудови [16]. Для Балтійського регіону (з огляду на гібридні ризики) вагомою є кіберскладова: Estonian Information System Authority (RIA) [17] офіційно повідомляє про 2672 кіберінциденти у 2022 р., які зачіпали людей, бізнес і послуги, що підсилює аргумент про включення кіберстійкості до ядра політики резильєнтності критичної інфраструктури. Додатково OECP у контексті ризику повеней для Паризького мегарегіону наводить оцінки вагомої частки збитків критичної інфраструктури у структурі прямих втрат та домінування непрямих втрат бізнесу, що демонструє, чому сервісний вимір є економічно визначальним [3].

Наведені у табл. 1 кейси демонструють три методологічно важливі висновки для державної політики розвитку критичної інфраструктури.

Таблиця 1

Приклади масштабу наслідків інцидентів критичної інфраструктури

Подія / тип порушення	Ключовий вимір наслідків	Оціночні показники / акценти джерел
Блекаут США–Канада (2003)	каскадні збої багатьох секторів; економічні втрати	узагальнення OECP щодо масштабу впливу та економічних втрат; офіційний звіт причин і рекомендацій
Ризик повені (Паризький мегарегіон)	висока частка збитків KI у прямих втратах, домінування непрямих бізнес-втрат	35-55% прямих збитків і до 85% втрат бізнесу (оцінки OECP)
Тайфун Гахаі (Японія, 2019)	порушення «lifelines» (електрика, зв'язок), ускладнення відновлення	урядовий White Paper акцентує тривалі відключення / збої та потребу вдосконалення механізмів реагування й відновлення
Кіберінциденти (Естонія, 2022)	вплив на людей / бізнес / сервіси, зростання ролі кіберстійкості	2672 кіберінциденти у 2022 р. (RIA), серед яких фішинг, збої сервісів, захоплення акаунтів тощо

Джерело: складено авторами на основі опрацювання й узагальнення [3; 15; 16; 17]

По-перше, економічна значущість критичної інфраструктури визначається не «фактом існування об'єкта», а безперервністю послуг і здатністю системи швидко повертатися до прийнятного рівня функціонування [3; 4].

По-друге, наслідки мають каскадний характер: критичні вузли (енергопостачання, зв'язок, цифрові сервіси) запускають мультисекторальні втрати [3; 15; 16].

По-третє, поряд із фізичними загрозами зростає роль кіберплощини, де інциденти без матеріальних руйнувань здатні порушувати життєво важливі сервіси та довіру до державних / приватних операторів [17; 18].

Саме тому порівняльний аналіз національних моделей доцільно будувати навколо того, як країни інституціоналізують сервісність, ризик-орієнтованість і кіберстійкість у принципах, механізмах підтримки та практиках реалізації. Для європейського контуру вихідною точкою порівняння виступає Директива (ЄС) 2022/2557 (CER) [14] (табл. 2), яка:

- закріплює орієнтацію на забезпечення життєво важливих (необхідних) послуг;
- трактує резильєнтність як повний цикл спроможностей (запобігання – захист – реагування – відновлення – адаптація);
- вимагає державних оцінок ризиків з урахуванням міжсекторальних і транскордонних залежностей;
- підсилює наглядову складову через вимоги до національних стратегій, ідентифікації критичних суб'єктів та контролю виконання.

Водночас CER не вирівнює автоматично практики розвитку критичної інфраструктури. Результативність залежить від того, як країни поєднують регуляторні вимоги з фінансуванням, партнерствами та управлінням взаємозалежностями [3; 14]. Перехід до сервісно-резильєнтної парадигми змінює набір принципів, які фактично виконують роль фільтра для вибору інструментів розвитку критичної інфраструктури (табл. 3). Якщо домінує принцип безперервності послуг, пріоритетними стають вимоги до планування / тестування. Якщо домінує принцип партнерства, то ключовими стають PPP-платформи (публічно-приватні партнерські платформи) й режим обміну інформацією. Якщо домінує кіберпріоритет, то посилюються нормативні вимоги до кіберзахисту критичних провайдерів [3].

При цьому важливо, що ефективність державної політики розвитку критичної інфраструктури визначається не окремим заходом, а узгодженою комбінацією принципів і набору інструментів. OECP акцентує на пріоритеті на-

Таблиця 2

CER-рамка як база для порівняння національних політик європейських країн

Елемент політики	Вимоги / логіка CER	Параметри порівняльного аналізу
Дефініції та фокус	Критичні суб'єкти як основа надання essential services; резильєнтність як здатність запобігати / захищати / реагувати / відновлюватися / адаптуватися	«сервісність» визначень, фокус на послугах і об'єктах, повнота циклу резильєнтності
Оцінювання ризиків	Державні оцінки ризиків, у т.ч. міжсекторальних і транскордонних	методики, частота оновлення, наявність аналізу залежностей і сценаріїв
Стратегування і нагляд	Стратегії, визначення компетентних органів, ідентифікація критичних суб'єктів, контроль виконання	архітектура управління, інструменти нагляду, механізми примусу / підтримки
Підтримка імплементації	можливість застосування інструментів/ресурсів для впровадження	стимули для операторів, стандарти, PPP, страхові / гарантійні механізми

Джерело: складено авторами на основі опрацювання й узагальнення [3; 14]

Таблиця 3

Принципи побудови державної політики розвитку критичної інфраструктури у міжнародних практиках

Принцип	Зміст принципу	Репрезентативні практики / документи
Системності та взаємозалежностей	КІ як мережа взаємопов'язаних секторів, управління каскадністю	OECP (governance/resilience), CER-логіка оцінки залежностей, США (секторизація)
Резильєнтності повного циклу	Запобігання – захист – реагування – відновлення – адаптація	CER, World Bank «Lifelines» як фокус на функціях
Ризик-орієнтованості (all-hazards)	Пріоритизація за ризиками і наслідками, сценарне планування	OECP, Канада (strategy/action plan)
Безперервності послуг	Безперервність надання послуг як критерій критичності та ефективності державної політики	World Bank Lifelines, Японія (disaster management)
Партнерськості	Включення приватних операторів у спільне управління ризиками	Німеччина (UP KRITIS), Канада (cross-sector forum)
Кіберпріоритету	Кіберстійкість критичних провайдерів як елемент нац. безпеки	Японія CIP policy, Естонія (RIA: статистика інцидентів), ENISA ETL
Інституційної визначеності	Визначення відповідального та координаторів, механізми виконання	CER (competent authorities) США (PPD-21)

Джерело: складено авторами на основі опрацювання й узагальнення [3; 4; 14; 16–23]

лежного врядування як основи резильєнтності, що включає координацію, стимулювання операторів, вимірювання прогресу та підтримку рішень на основі ризиків [3]. У практичному вимірі це може бути показано через матрицю відповідності (табл. 4).

Слід зазначити, що для порівняльного аналізу доцільно уніфікувати розуміння «механізмів підтримки» як інструментального ядра політики (тобто чим саме держава забезпечує розвиток і резильєнтність критичної інфраструктури) (табл. 5).

Для посилення доказовості та аналітичної узгодженості дослідження застосовано матричний підхід, який дозволяє зіставляти державну політику розвитку критичної інфраструктури за трьома взаємопов'язаними вимірами: (1) принципи формування політики; (2) механізми підтримки; (3) реалізація та управління [3].

Вибір країн і практик здійснено за логікою «порівняльних полюсів», що відображають різні інституційні традиції та моделі публічного врядування [7; 14; 17; 19; 23]:

- європейський CER-контур (у межах Директиви (ЄС) 2022/2557) з різними адміністративними моделями імплементації;
- північноамериканська секторизована модель врядування ризиками, яку засновано на розподілі ролей між секторами та рівнями влади;
- балтійський підхід до забезпечення кіберорієнтованої резильєнтності в умовах підвищених гібридних загроз;

Таблиця 4

Матриця відповідності принципів і інструментів державної політики розвитку критичної інфраструктури

Принцип	Регуляторні інструменти	Фінансові / ресурсні інструменти	Інституційні інструменти
Системність / залежності	вимоги до оцінки залежностей, стандарти взаємодії	фінансування модернізації критичних вузлів	міжсекторальні координаційні органи / платформи
Резильєнтність повного циклу	вимоги до планів реагування / відновлення, стрес-тести	фонди відновлення / адаптації, співфінансування	центри / штаби реагування, механізми навчання та постійного вдосконалення
Ризик-орієнтованість	національні оцінки ризиків, обов'язковість оновлень	страхові / гарантійні механізми	аналітичні підрозділи, процедури ризик-орієнтованого врядування
Партнерські взаємовідносини	PPP-режими, правила інформаційного обміну	спільні інвестиції, програми підтримки операторів	PPP-платформи (наприклад, UP KRITIS)
Кіберпріоритет	вимоги до кіберзахисту критичних провайдерів, звітність про інциденти	інвестиції у кіберзахист / підготовку кадрів	національні кіберцентри / CSIRT, крос-секторні вправи

Джерело: складено авторами на основі опрацювання [3; 4; 18; 23; 24–26]

Таблиця 5

Класифікація механізмів підтримки державної політики розвитку критичної інфраструктури

Група механізмів	Характеристика	Типові приклади (міжнародні практики)
Інституційні	організація управління, компетенції, координація	компетентні органи/нагляд (CER), секторальне врядування (PPD-21)
Регуляторні	нормативні вимоги до операторів, стандарти, контроль	CER-вимоги, Німеччина (CIP strategy/KRITIS)
Партнерські	інституціоналізована співпраця держави й операторів	UP KRITIS (кооперація держави та економіки), Канада (cross-sector forum)
Фінансово-ресурсні	забезпечення ресурсів розвитку/модернізації/захисту	державні програми / співфінансування, інвестиційна пріоритизація (логіка OECP/Світового банку)
Інформаційно-аналітичні	моніторинг, оцінка ризиків, обмін інформацією, навчання	RIA (інциденти/аналітика), ENISA (threat landscape)
Планувально-тестові	планування безперервності діяльності / надання послуг (BCP/continuity), вправи, стрес-тести, оцінювання готовності	управлінські рекомендації після блекауту, крос-секторні підходи до CIP

Джерело: складено авторами на основі опрацювання [3; 4; 14; 17–19; 21–23; 24–26; 27]

- азійська техно-кібермодель (Японія та Республіка Корея), де кіберстійкість критичних провайдерів та ІКТ-інфраструктури є ядром державної політики.

Результати такого зіставлення узагальнено в табл. 6, яка дозволяє виявити не лише формальні відмінності між країнами, а й глибинну логіку побудови державної політики розвитку критичної інфраструктури.

Як видно з табл. 6, сервісна орієнтація та резильєнтність повного циклу виступають спільною методологічною основою для всіх розглянутих моделей, однак інструментальні рішення суттєво різняться залежно від інституційного контексту.

Зокрема, європейський CER-контур інституціоналізує розвиток критичної інфраструктури через поєднання стратегування, державного нагляду та ідентифікації критичних суб'єктів, формуючи уніфіковану регуляторну рамку з національною імплементацією [14]. США, навпаки, реалізують політику розвитку критичної інфраструктури через секторне врядування, що базується на чіткій секторизації, розподілі відповідальності та міжвідомчій координації [15; 28]. Канада доповнює подібну логіку врядування ризиками розвинутими партнерськими та кооперативними механізмами взаємодії між федеральним, субнаціональними рівнями влади та операторами критичної інфраструктури [15; 19; 20].

Особливу увагу в межах порівняльного аналізу привертає балтійський підхід, представлений моделлю Естонії, де кіберстійкість розглядається як ключова умова забезпечення безперервності життєво важливих послуг. Посилення кіберінституцій, моніторингу та реагування на інциденти формує специфічну «фронтову» модель резильєнтності, актуальну для держав із підвищеним рівнем гібридних загроз [17; 18]. Водночас Японія та Республіка Корея демонструють техно-орієнтовані підходи, у яких кіберполітики та спеціалізоване законодавство щодо захисту критичної ІКТ-інфраструктури інтегруються в ширшу систему забезпечення гарантованої безперервності виконання критичних функцій (mission assurance) [21; 23].

Таким чином, табл. 6 підтверджує, що розвиток критичної інфраструктури в сучасних державах постає не як сукупність ізольованих заходів, а як політика системної резильєнтності, спрямована на управління ризиками та забезпечення безперервності життєво важливих послуг, а не лише на фізичний захист об'єктів інфраструктури [3; 4].

Водночас повноцінна оцінка результативності державної політики розвитку критичної інфраструктури потребує врахування не лише її структурних характеристик, а й управлінських переваг та обмежень, які супроводжують кожну модель. З цією метою у дослідженні здійснено порівняльний аналіз сильних сторін і ризиків різних підходів (табл. 7).

Як свідчать дані табл. 7, ключовою перевагою CER-орієнтованої європейської моделі є уніфікація мінімальних вимог і посилення нагляду, проте її обмеженням залишається ризик формальної комплаєнс-орієнтації без належного фінансового та інституційного підкріплення [3; 14]. Північноамериканські моделі (США, Канада) забезпечують гнучкість і адаптивність завдяки секторизації та партнерствам, однак стикаються з проблемами міжрівневої координації та нерівномірної спроможності субнаціональних акторів [15; 19; 20; 28].

Балтійська кібер-орієнтована модель вирізняється високою готовністю до реагування на кіберінциденти та наявністю доказової аналітики, проте несе ризик надмірної концентрації на кіберкомпоненті за недостатньої уваги до фізичної стійкості інфраструктурних мереж [17; 18]. Азійські техно-кібермоделі (Японія, Республіка Корея) демонструють ефективність у нормативному закріпленні кіберстійкості, але потребують постійного оновлення політик і балансування між цифровими та територіально-фізичними аспектами розвитку критичної інфраструктури [21; 23].

Узагальнення результатів, наведених у табл. 6 і табл. 7, дозволяє виокремити типологію державної політики розвитку критичної інфраструктури та сформулювати ключові критерії її результативності: сервісна

Таблиця 6

Порівняльний аналіз державної політики розвитку критичної інфраструктури

Країна / регіон	Принципи формування	Механізми підтримки	Реалізація та управління
ЄС	сервісна орієнтація, резильєнтність повного циклу, урахування міжсекторальних залежностей	стратегічне планування, державний нагляд, ідентифікація критичних суб'єктів	регуляторно-наглядова модель з національною імплементацією
Німеччина	критичність як суспільно-економічна важливість, партнерська взаємодія	національна стратегія захисту КІ, стандарти безпеки, платформи співпраці держави та операторів	координаційно-мережева модель
Польща	критична інфраструктура як основа безпеки та функціонування держави	державна координація, інтеграція з кризовим управлінням	державоцентрична координаційна модель
Чехія	формалізоване визначення критичної інформаційної інфраструктури	нормативні процедури ідентифікації, спеціалізований державний орган	інституційно-процедурна модель
Велика Британія	оцінка критичності через рівень суспільного впливу, ризик орієнтований підхід	партнерські механізми, планування стійкості, управління ризиками	децентралізована партнерська модель
США	секторний підхід, узгодження дій між органами влади	визначення секторів, розподіл ролей, міжвідомча координація	федеративна модель врядування ризиками
Канада	управління всіма видами загроз, партнерська взаємодія, міжрівнева координація	національна стратегія, спільні плани дій, кооперація з операторами	кооперативна модель
Естонія	пріоритет кіберстійкості життєво важливих послуг	національна система кібербезпеки, моніторинг, реагування на інциденти	кіберорієнтована модель
Японія	забезпечення безперервності критичних функцій, інтеграція кіберполітики	державна кіберполітика для критичної інфраструктури	координаційно-секторна модель
Республіка Корея	технологічна та кіберорієнтація критичної інфраструктури	спеціальне законодавство щодо захисту ІКТ-інфраструктури	нормативно координаційна модель

Джерело: складено авторами на основі опрацювання [3; 4; 14–23; 27–31]

Таблиця 7

Переваги та обмеження державної політики розвитку критичної інфраструктури: порівняльне узагальнення

Країна / регіон	Переваги	Обмеження та ризики
ЄС	уніфікація базових вимог, посилення державного нагляду, орієнтація на життєво важливі послуги	ризик формального виконання вимог, недостатнє фінансове та інституційне забезпечення
Німеччина	інституціоналізована взаємодія держави та операторів, узгодження стандартів і підходів	висока складність координації, потреба зрілих управлінських спроможностей
США	чітка секторна структура, розподіл відповідальності між органами влади	складність міжрівневої та міжсекторальної координації, ризик фрагментації реалізації
Канада	партнерський і кооперативний підхід, узгодження дій між рівнями влади	нерівномірна спроможність субнаціональних рівнів у фінансуванні та впровадженні
Естонія	висока готовність до кіберінцидентів, системний моніторинг і реагування	ризик надмірної концентрації на кіберскладовій, недостатня увага до фізичної стійкості мереж
Японія	комплексна державна кіберполітика, орієнтація на безперервність критичних функцій	потреба постійного оновлення політик у відповідь на зміну загроз
Республіка Корея	чітке законодавче регулювання захисту ІКТ-інфраструктури	необхідність балансування цифрових і територіально-фізичних аспектів розвитку

Примітка: переваги та обмеження подано з позицій результативності державної політики розвитку критичної інфраструктури та її спроможності забезпечувати безперервність життєво важливих послуг.

Джерело: складено авторами на основі опрацювання [3; 4; 14–23; 24–26; 27–31]

орієнтація; урахування міжсекторальних і транскордонних взаємозалежностей; інституційна визначеність відповідальності; інструментальна узгодженість механізмів підтримки та доказовість рішень на основі оцінок ризиків і втрат [3; 4; 14].

Отже, розширене міжрегіональне порівняння (Європа – Північна Америка – Балтія – Азія) підтверджує, що розвиток критичної інфраструктури в сучасних умовах виступає ключовою складовою державної політики резильєнтності, яка реалізується через різні інституційні моделі, але має спільну методологічну основу – управління ризиками та забезпечення безперервності життєво важливих послуг.

Висновки. Результати проведеного дослідження свідчать, що сучасна державна політика розвитку критичної інфраструктури дедалі більше відходить від об'єктно-орієнтованої логіки захисту та формується у межах сервісної парадигми резильєнтності. У цій парадигмі ключовим критерієм критичності та ефективності політики виступає безперервність надання життєво важливих послуг, а також спроможність держави управляти міжсекторальними та транскордонними залежностями.

Узагальнення емпіричних кейсів із країн Європи, Північної Америки та Азії підтверджує мультиплікативний характер економічних і соціальних втрат у разі порушення функціонування критичної інфраструктури. Масштабні техногенні аварії, природні катастрофи та кіберінциденти спричиняють каскадні ефекти, що одночасно охоплюють кілька секторів економіки й істотно посилюють системні ризики для суспільства, державних фінансів і національної безпеки.

Порівняльний аналіз регуляторних рамок засвідчив, що європейська CER-модель формує спільний мінімальний стандарт сервісного підходу, ризик-орієнтованого планування та державного нагляду у сфері критичної інфраструктури. Водночас її практична результативність значною мірою визначається інституційною спроможністю країн-членів, наявністю фінансових інструментів підтримки та ступенем інтеграції регуляторних вимог у повсякденну діяльність операторів.

Важливим результатом дослідження є встановлення того, що найбільш стійкими виявляються моделі державної політики, у яких принципи формування розвитку критичної інфраструктури підкріплюються узгодженим поєднанням механізмів підтримки. Йдеться про одночасне застосування регуляторних вимог, інституцій координації, фінансових стимулів та партнерських форматів взаємодії між державою і операторами, а не про ізольоване використання окремих інструментів.

Аналіз північноамериканського досвіду демонструє ефективність секторного врядування та чіткого розподілу відповідальності між органами влади й операторами критичної інфраструктури, що підвищує керованість ризиків і сприяє інтеграції фізичної та кіберстійкості. Водночас така модель потребує високого рівня міжрівневої координації та сталих механізмів узгодження інтересів між секторами.

Канадська практика додатково підкреслює цінність підходу спільної відповідальності, реалізованого через крос-секторні плани дій і кооперативні механізми взаємодії між федеральним та субнаціональними рівнями. Це забезпечує гнучкість і адаптивність політики розвитку критичної інфраструктури, проте водночас вимагає вирівнювання інституційної та фінансової спроможності на різних рівнях управління.

Досвід Японії та балтійських країн акцентує увагу на ролі життєво важливих інфраструктурних ліній і кіберстійкості як ключових чинників забезпечення безперервності критичних сервісів. Балтійський кейс, зокрема на прикладі Естонії, переконливо демонструє, що інституційна спроможність до моніторингу, аналізу та реагування на кіберінциденти стає визначальною умовою резильєнтності в умовах гібридного безпекового середовища.

Південнокорейська модель, своєю чергою, ілюструє техно-державний підхід, у межах якого правове регулювання захисту критичної ІКТ-інфраструктури інтегрується зі стратегічним баченням розвитку цифрових сервісів і посилює їхню стійкість до зовнішніх збурень.

Узагальнюючи отримані результати, резильєнтність критичної інфраструктури доцільно трактувати як керовану багатовимірну систему, ефективність якої визначається не кількістю нормативних документів, а вимірюваними параметрами стійкості сервісів, швидкості відновлення, готовності операторів до реагування та здатності системи адаптуватися до економічних шоків і зовнішніх загроз.

На основі проведеного аналізу для досліджених країн доцільно рекомендувати подальше посилення інтеграції регуляторних і фінансових інструментів, зокрема шляхом поєднання вимог до резильєнтності з інвестиційними стимулами для операторів критичної інфраструктури. Важливим напрямом є розвиток інституційних платформ співпраці держави й приватного сектору, здатних забезпечувати регулярний обмін інформацією, спільні оцінки ризиків і навчання. Окремої уваги потребує балансування кіберорієнтованих підходів із фізичною стійкістю мереж, що є критичним для зменшення системних ризиків у довгостроковій перспективі.

Для України в умовах воєнного та повоєнного відновлення обґрунтованим є поетапне впровадження сервісної логіки розвитку критичної інфраструктури з фокусом на безперервність життєво важливих послуг. Практично значущими кроками є гармонізація національної термінології та критеріїв критичності з європейською CER-рамкою, впровадження секторної моделі відповідальності, інституціоналізація публічно-приватних платформ співпраці та посилення національного кіберконтуру для критичних сервісів.

Важливим напрямом має стати стандартизація державної оцінки ризиків з урахуванням міжсекторальних залежностей, запровадження диференційованих вимог до резервування і часу відновлення, а також розвиток фінансових інструментів підтримки модернізації та відновлення критичної інфраструктури. Реалізація таких підходів дозволить перейти від реактивного відновлення до проактивного розвитку резильєнтності як основи національної стійкості та економічної безпеки у повоєнний період.

Подальші наукові дослідження доцільно спрямувати на кількісну оцінку ефективності механізмів розвитку критичної інфраструктури, розроблення системи індикаторів

резильєнтності життєво важливих послуг, а також на моделювання економічних ефектів інвестування у резильєнтність критичної інфраструктури в умовах повоєнної відбудови України.

ЛІТЕРАТУРА

1. The Global Risks Report 2023. 18th ed. Geneva : World Economic Forum, 2023. 98 p. URL: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

2. 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

3. Good Governance for Critical Infrastructure Resilience. Paris: OECD Publishing, 2019. 118 p. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/good-governance-for-critical-infrastructure-resilience_7d5a9993/02f0e5a0-en.pdf (oecd.org in Bing)

4. Hallegatte S., Rentschler J., Rozenberg J. Lifelines: The Resilient Infrastructure Opportunity. Sustainable Infrastructure. Washington, DC : The World Bank, 2019. 224 p.

DOI: https://doi.org/10.1596/978-1-4648-1430-3

5. Bevere L., Fan I., Gillespie F. et al. Resilience Index 2021: a cyclical growth recovery, but less resilient world economy. Zurich : Swiss Re Institute, 2021. URL: https://www.swissre.com/dam/jcr:ca784019-cd41-45fb-81ed-9379f2cd91e3/swiss-re-institute-sigma-resilience-index-update-june-2021.pdf

6. Pörtner H.-O., Roberts D. C., Tignor M. et al. Climate Change 2022: Impacts, Adaptation and Vulnerability. Geneva : IPCC; Cambridge : Cambridge University Press, 2022. 3056 p.

DOI: https://doi.org/10.1017/9781009325844

7. ENISA Threat Landscape 2023. Brussels : European Union Agency for Cybersecurity, 2023. 161 p. URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

8. Anglmayer I. European critical infrastructure: Revision of Directive 2008/114/EC. Brussels : European Parliamentary Research Service, 2021. 12 p. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf

9. Wells E. M., Boden M., Tseytlin I., Linkov I. Modeling critical infrastructure resilience under compounding threats: A systematic literature review. *Progress in Disaster Science*. 2022. Vol. 15. Art. 100244.

DOI: https://doi.org/10.1016/j.pdisas.2022.100244

10. Бірюков Д. С., Кондратов С. І., Насвіт О. І., Суходоля О. М. Зелена книга з питань захисту критичної інфраструктури в Україні. Київ : Національний інститут стратегічних досліджень, 2015. 35 с.

11. Арсенович Л. А. Парадигма захисту критичної інфраструктури в системі національної безпеки України. *Державне управління: удосконалення та розвиток*. 2024. № 8.

DOI: https://doi.org/10.32702/2307-2156.2024.8.7

12. Єрменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монографія. Дніпро : ДДУВС, 2018. 180 с.

13. Shkuropadska D., Lebedeva L., Gonçalves J. Institutional Framework for the Resilience of Critical Infrastructure of EU, NATO Countries and Ukraine. *Scientia Fructuosa*. 2025. No. 1. P. 45–60.

DOI: https://doi.org/10.31617/1.2025(159)03

14. Directive (EU) 2022/2557 … on the resilience of critical entities. *Official Journal of the European Union*. 2022. L 333. P. 164–198. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj

15. Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. Canada : U.S.-Canada Power System Outage Task Force, 2004. 238 p. URL: https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

16. White Paper on Disaster Management 2020 (Chapter 2: Review and Measures on Typhoons Faxai and Hagibis in 2019) // Cabinet Office, Government of Japan. 2020. URL: https://www.bousai.go.jp/en/documentation/white_paper/pdf/2020/SF2.pdf

17. RIA: The number of cyber attacks in 2022 was a hundred times higher than during the April Unrest // Estonian Information System Authority. 2023. 6 February. URL: https://ria.ee/en/news/ria-number-cyber-attacks-2022-was-hundred-times-higher-during-april-unrest

18. Voronova S. Resilience of critical entities // European Parliamentary Research Service (EPRS). 2022. November. URL: https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/738212/EPRS_ATA(2022)738212_EN.pdf

19. National Strategy for Critical Infrastructure // Public Safety Canada. 2009. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf

20. National Cross Sector Forum 2021–2023: Action Plan for Critical Infrastructure // Public Safety Canada. 2021. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/2021-ctn-pln-crtcl-nfrstrctr-en.pdf

21. The Cybersecurity Policy for Critical Infrastructure Protection // Government of Japan, Cybersecurity Strategic Headquarters. 2022. 17 June. URL: https://www.cyber.go.jp/eng/pdf/cip_policy_2024_eng.pdf

22. Die Unabhängige Partnerschaft KRITIS (UP KRITIS). Öffentlich-private Partnerschaft zum Schutz Kritischer Infrastrukturen in Deutschland // Bundesamt für Sicherheit in der Informationstechnik. 2024. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/UPK/upk-flyer.pdf

23. Act on the Protection of Information and Communication Infrastructure // Korean Law Information Center. Republic of Korea. 2022. 10 June. URL: https://www.law.go.kr/lsInfoP.do?chrClsCd=010203&lsiSeq=242915&urlMode=engLsInfoR&viewCls=engLsInfoR#0000

24. Кизим М. О., Хаустова В. Є., Трушкіна Н. В. Фінансове забезпечення розвитку критичної інфраструктури в умовах повоєнної відбудови економіки України. *Бізнес Інформ*. 2023. № 8. С. 263–274.

DOI: https://doi.org/10.32983/2222-4459-2023-8-263-274

25. 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

26. Хаустова В. Є., Трушкіна Н. В. Правові засади регулювання розвитку критичної інфраструктури: міжнародна практика та український досвід. *Бізнес Інформ*. 2025. № 11. С. 6–26.

DOI: https://doi.org/10.32983/2222-4459-2025-11-6-26

27. National Strategy for Critical Infrastructure Protection (CIP Strategy) // Federal Ministry of the Interior, Federal Republic of Germany. 2009. 17 June. URL: https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/civil-protection/kritis_englisch.pdf

28. The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience // Office of the Press

Secretary, The White House. 2013. 12 February. URL: https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf

29. Critical Infrastructure // Government Centre for Security of the Republic of Poland. 2024. URL: https://www.gov.pl/web/rcb-en/critical-infrastructure

30. Critical Information Infrastructure – Decision scheme // National Cyber and Information Security Agency (NCISA) of the Czech Republic. 2018. URL: https://nukib.gov.cz/download/publications_en/support_materials/KII_rozhodovaci_schema_EN_final.pdf

31. Critical National Infrastructure // The National Protective Security Authority (NPSA) of the United Kingdom. 2025. 23 June. URL: https://www.npsa.gov.uk/about-npsa/critical-national-infrastructure

REFERENCES

Anglmayer I. (2021). European critical infrastructure: Revision of Directive 2008/114/EC. *Brussels: European Parliamentary Research Service*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf

Arsenovych L. A. (2024). Paradyhma zakhystu krytychnoi infrastruktury v systemi natsionalnoi bezpeky Ukrainy [Paradigm of critical infrastructure protection in the system of national security of Ukraine]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, *8*. https://doi.org/10.32702/2307-2156.2024.8.7

Bevere L., Fan I. & Gillespie F. (2021). Resilience Index 2021: a cyclical growth recovery, but less resilient world economy. *Zurich: Swiss Re Institute*. https://www.swissre.com/dam/jcr:ca784019-cd41-45fb-81ed-9379f2cd91e3/swiss-re-institute-sigma-resilience-index-update-june-2021.pdf

Biriukov D. S., Kondratov S. I., Nasvit O. I. & Sukhodolia O. M. (2015). *Zelena knyha z pytan zakhystu krytychnoi infrastruktury v Ukraini* [Green Paper on Critical Infrastructure Protection in Ukraine]. Kyiv: Natsionalnyi instytut stratehichnykh doslidzhen.

Bundesamt für Sicherheit in der Informationstechnik. (2024). Die Unabhängige Partnerschaft KRITIS (UP KRITIS). Öffentlich-private Partnerschaft zum Schutz Kritischer Infrastrukturen in Deutschland. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/UPK/upk-flyer.pdf

Cabinet Office, Government of Japan. (2020). White Paper on Disaster Management 2020 (Chapter 2: Review and Measures on Typhoons Faxai and Hagibis in 2019). https://www.bousai.go.jp/en/documentation/white_paper/pdf/2020/SF2.pdf

U.S.-Canada Power System Outage Task Force (2004). *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. Canada: U.S.-Canada Power System Outage Task Force. https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

Estonian Information System Authority. (2023, February 6). RIA: The number of cyber attacks in 2022 was a hundred times higher than during the April Unrest. https://ria.ee/en/news/ria-number-cyber-attacks-2022-was-hundred-times-higher-during-april-unrest

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

European Union Agency for Cybersecurity (2023). *ENISA Threat Landscape 2023*. Brussels: European Union Agency for Cybersecurity. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

Federal Ministry of the Interior, Federal Republic of Germany. (2009, June 17). National Strategy for Critical Infrastructure Protection (CIP Strategy). https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/civil-protection/kritis_englisch.pdf

Government Centre for Security of the Republic of Poland. (2024). Critical Infrastructure. https://www.gov.pl/web/rcb-en/critical-infrastructure

Government of Japan, Cybersecurity Strategic Headquarters. (2022, June 17). The Cybersecurity Policy for Critical Infrastructure Protection. https://www.cyber.go.jp/eng/pdf/cip_policy_2024_eng.pdf

Hallegatte S., Rentschler J. & Rozenberg J. (2019). *Lifelines: The Resilient Infrastructure Opportunity*. Washington, DC: The World Bank. https://doi.org/10.1596/978-1-4648-1430-3

Khaustova V. Ye. & Trushkina N. V. (2025). Teoretychni pidkhody do sutnosti poniattia «krytychna infrastruktura»: mizhnarodnyi, prostorovyi i rezylientnisnyi 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

Khaustova V. Ye. & Trushkina N. V. (2025). Pravovi zasady rehuliuvannia rozvytku krytychnoi infrastruktury: mizhnarodna praktyka ta ukrainskyi dosvid [Legal principles of regulating the development of critical infrastructure: international practice and Ukrainian experience]. *Biznes Inform*, *11*, 6–26. https://doi.org/10.32983/2222-4459-2025-11-6-26

Korean Law Information Center. Republic of Korea. (2022, June 10). Act on the Protection of Information and Communication Infrastructure. https://www.law.go.kr/lsInfoP.do?chrClsCd=010203&lsiSeq=242915&urlMode=engLsInfoR&viewCls=engLsInfoR#0000

Kyzym M. O., Khaustova V. Ye. & Trushkina N. V. (2023). Finansove zabezpechennia rozvytku krytychnoi infrastruktury v umovakh povoiennoi vidbudovy ekonomiky Ukrainy [Financial support for the development of critical infrastructure in the conditions of post-war reconstruction of the economy of Ukraine]. *Biznes Inform*, *8*, 263–274. https://doi.org/10.32983/2222-4459-2023-8-263-274

National Cyber and Information Security Agency (NCISA) of the Czech Republic. (2018). Critical Information Infrastructure – Decision scheme. https://nukib.gov.cz/download/publications_en/support_materials/KII_rozhodovaci_schema_EN_final.pdf

The National Protective Security Authority (NPSA) of the United Kingdom. (2025, June 23). Critical National Infrastructure. https://www.npsa.gov.uk/about-npsa/critical-national-infrastructure

OECD Publishing (2019). *Good Governance for Critical Infrastructure Resilience*. Paris: OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/good-governance-for-critical-infrastructure-resilience_7d5a9993/02f0e5a0-en.pdf

Office of the Press Secretary, The White House. (2013, February 12). The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience. https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf

Official Journal of the European Union. (2022). Directive (EU) 2022/2557 … on the resilience of critical entities. https://eur-lex.europa.eu/eli/dir/2022/2557/oj

Pörtner H.-O., Roberts D. C. & Tignor M. (2022). *Climate Change 2022: Impacts, Adaptation and Vulnerability*. Geneva:

IPCC; Cambridge: Cambridge University Press. https://doi.org/10.1017/9781009325844

Public Safety Canada. (2009). National Strategy for Critical Infrastructure. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf

Public Safety Canada. (2021). National Cross Sector Forum 2021–2023: Action Plan for Critical Infrastructure. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/2021-ctn-pln-crtcl-nfrstrctr-en.pdf

Shkuropadska D., Lebedeva L. & Gonçalves J. (2025). Institutional Framework for the Resilience of Critical Infrastructure of EU, NATO Countries and Ukraine. *Scientia Fructuosa*, *1*, 45–60. https://doi.org/10.31617/1.2025(159)03

Voronova S. Resilience of critical entities. *European Parliamentary Research Service (EPRS)*. https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/738212/EPRS_ATA(2022)738212_EN.pdf

Wells E. M., Boden M., Tseytlin I. & Linkov I. (2022). Modeling critical infrastructure resilience under compounding threats: A systematic literature review. *Progress in Disaster Science*, *100244*(15). https://doi.org/10.1016/j.pdisas.2022.100244

World Economic Forum (2023). *The Global Risks Report 2023*. (18th ed.). Geneva: World Economic Forum. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

Yermenchuk O. P. (2018). *Osnovni pidkhody do orhanizatsii zakhystu krytychnoi infrastruktury v krainakh Yevropy: dosvid dlia Ukrainy: monohrafiia* [Main approaches to organizing the protection of critical infrastructure in European countries: experience for Ukraine: monograph]. Dnipro: DDUVS.

Стаття надійшла до редакції 18.01.2026 р.
Статтю прийнято до публікації 04.02.2026 р.
Оприлюднено 23.04.2026 р.