УДК 621.039.7:352.07(477)
DOI: https://doi.org/10.30838/EP.195.47-54

Плахотнюк Р.В.
Університет митної справи та фінансів
Plakhotniuk Ruslan
University of Customs and Finance
https://orcid.org/0009-0006-6157-1028

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ

Стійкість критичної інфраструктури є важливою складовою національної безпеки та розвитку держави. Залежність сучасних суспільств від ефективного функціонування таких об'єктів, як енергетичні системи, транспортування, зв'язок, водопостачання та інші важливі обєкти, створює необхідність забезпечення їх стійкості до різноманітних загроз. Виділені рівні критичності та запропоновано розподіл об'єктів за інфраструктури за критерієм його критичності. У статті визначено основні фактори, які впливають на стійкість критичної інфраструктури, серед яких вразливість, ризики, механізми відновлення, адаптивність, безпека, соціальні та економічні аспекти, а також роль міжсекторальної координації. Зазначено важливість гнучкості та адаптивності при кризових ситуаціях для швидкого відновлення функціонування інфраструктури після катастрофічних подій, як природних, техногенних так і терористичних дій. Одним із ключових напрямків визначено вивчення оцінки стійкості критичної інфраструктури, які ґрунтуються на багатофакторному підході та включають аналіз як технічних, так і соціальних аспектів. Серед найбільш важливих складових, що впливають на стійкість інфраструктури, є розвиток технологій кібербезпеки, адекватність правових норм та здатність до адаптації інфраструктури до нових загроз. Врахування цих факторів дає змогу не тільки оцінити поточний рівень стійкості інфраструктури, але й визначити найбільш уразливі ділянки, що потребують посилення захисту та його своєчасності. Визначення механізмів відновлення та адаптації є важливим аспектом для забезпечення безперервного функціонування критичних систем під час надзвичайних ситуацій. У статті також представлено можливі напрями оцінки стійкості, що сприяє точнішому прогнозуванню наслідків можливих ризиків і розробленню ефективних стратегій забезпечення стабільності об'єктів критичної інфраструктури. Обгрунтовано висновок про важливість диференційованого підходу до розроблення заходів забезпечення стійкості залежно від критеріїв критичності відповідних об'єктів інфраструктури.

***Ключові слова**: критична інфраструктура, стійкість, оцінка ризиків, механізми відновлення, кібербезпека, адаптивність, міжсекторальна координація, публічне управління.*

SECURING THE RESILIENCE OF CRITICAL INFRASTRUCTURE IN UKRAINE AMIDST CONTEMPORARY CHALLENGES

The resilience of critical infrastructure is a crucial component of national security and state development. The dependence of modern societies on the effective functioning of such objects as energy systems, transportation, communications, water supply, and other vital infrastructure necessitates ensuring their resilience to various threats. The levels of criticality have been identified, and a distribution of infrastructure objects based on their criticality criteria has been proposed. The article defines the main factors that influence the resilience of critical infrastructure, including vulnerability, risks, recovery mechanisms, adaptability, security, social and economic aspects, as well as the role of intersectoral coordination. The importance of flexibility and adaptability in crisis situations is highlighted for the rapid restoration of infrastructure functioning after catastrophic events, whether natural, technological, or terrorist attacks. One of the key areas identified is the study of critical infrastructure resilience assessment, based on a multi-factor approach that includes the analysis of both technical and social aspects. Among the most important factors influencing infrastructure resilience are the development of cybersecurity technologies, the adequacy of legal norms, and the capacity for infrastructure to adapt to new threats. Taking these factors into account not only allows for assessing the current level of infrastructure resilience but also helps identify the most vulnerable areas that require enhanced protection and timely intervention. The identification of recovery and adaptation mechanisms is a critical aspect for ensuring the continuous functioning of critical systems during emergencies. The article also presents possible directions for resilience assessment that contribute to more accurate forecasting of potential risks and the development of effective strategies to ensure the stability of critical infrastructure objects. The conclusion emphasizes the importance of a differentiated approach to developing resilience measures based on the criticality criteria of the respective infrastructure objects.

***Keywords**: critical infrastructure, resilience, risk assessment, recovery mechanisms, cybersecurity, adaptability, intersectoral coordination, public administration.*

***JEL classification**: H54, O10, Q54, D74, L9.*

Постановка проблеми. Критична інфраструктура є основою функціонування сучасного суспільства та економіки. Вона включає всі ключові об'єкти та системи, від яких залежить життєдіяльність населення, ефективність державного управління та стабільність економічної діяльності. Стійкість таких систем визначає здатність держави підтримувати основні соціальні функції навіть в умовах надзвичайних ситуацій, таких як природні катастрофи, техногенні аварії, або кібератаки. У зв'язку з підвищенням кількості глобальних загроз, необхідність забезпечення стійкості інфраструктур стає дедалі більш актуальною. Зокрема, важливими є питання стійкості до технологічних, екологічних та соціальних загроз, а також готовність до швидкого відновлення після криз та катастроф. Для України, яка стикається з численними внутрішніми та зовнішніми загрозами, забезпечення стійкості критичної інфраструктури набуває особливого значення. Збройні конфлікти, кіберзагрози, природні катастрофи, техногенні аварії та економічні виклики створюють серйозні ризики для безпеки та функціонування критичних об'єктів.

Аналіз останніх досліджень і публікацій. Наукові погляди з теми забезпечення стійкості критичної інфраструктури в Україні зосереджується на вивченні різних підходів до оцінки та підвищення стійкості інфраструктурних об'єктів, що мають значення для національної безпеки, економіки, і соціального благополуччя. Законодавчі ініціативи України, як Закон "Про основи національної безпеки України" [1] та "Про основні засади забезпечення кібербезпеки України" [2], окреслюють основні напрями захисту об'єктів критичної інфраструктури від загроз, зокрема, кіберзагроз. Стратегія забезпечення державної безпеки, затверджена Указом Президента України [3] також підкреслює необхідність інтегрованого підходу, який поєднує правові, технічні, економічні та соціальні аспекти. Дослідження авторів Національного інституту стратегічних досліджень [4; 5] акцентують увагу на важливості енергетичної безпеки як одного з ключових елементів критичної інфраструктури. Експерти зазначають, що забезпечення стійкості енергетичних мереж потребує диверсифікації джерел енергії та впровадження резервних систем для швидкого реагування у випадках надзвичайних ситуацій.

Міжнародний досвід, наприклад, практика НАТО в області захисту критичної інфраструктури та кібербезпеки [6], показує ефективність взаємодії різних державних і приватних структур для покращення безпеки та швидкого реагування на катастрофи.

Стійкість критичної інфраструктури в Україні стала об’єктом численних досліджень у зв'язку з новими викликами, пов’язаними з військовими загрозами, кіберзагрозами та природними катастрофами. Серед українських науковців, які досліджували питання національної безпеки та захисту інфраструктури, слід виділити таких авторів, як: Гордієнко С.Г., Доронін І.М., які досліджували багатофакторний підхід до аналізу Інформаційно-правові аспекти захисту критичної інфраструктури [7]; Яременко О.І., Страхніцький Я.І. [8] вивчають важливість визначення дефініції критичної інфраструктури як об’єкту державного управління в контексті забезпечення її стійкості. Крім українських дослідників, важливий внесок у питання захисту критичної інфраструктури зробили і міжнародні дослідники. Серед впливових досліджень є праці: Боіна А. та МакКонела А. [9], які досліджують питання стійкості критичної інфраструктури, акцентуючи увагу на її вразливості до різних загроз. Автори аналізують, чому традиційне кризове управління може виявитися недостатнім і пропонують стратегії для підвищення стійкості. Гвідотті, Р., Хмелевський, Г., Уннікрішнан, В., Гардоні, П., Макалістер, Т., та ван де Ліндт, Дж. [10] досліджують роль залежностей між різними інфраструктурними мережами та їх вплив на загальну стійкість критичної інфраструктури. Автори пропонують модель для оцінки стійкості, яка враховує взаємозв'язки між різними компонентами інфраструктури, демонструють, як порушення в одній частині інфраструктури може призвести до негативного впливу на інші частини через їхню взаємозалежність, і розглядають підходи до мінімізації цих ризиків для підвищення стійкості всієї системи. У статті [11] Селлевог Стіг Руне пропонує концепцію абстракційно-декомпозиційного простору, зосереджується розробці політики стійкості, яка враховує складні залежності між різними компонентами інфраструктури, пропонує методологічні підходи до вдосконалення політик у сфері стійкості, які можуть допомогти оптимізувати управління критичною інфраструктурою для підвищення її надійності.

Разом з тим, окремі питання дослідження стійкості критичної інфраструктури потребують додаткового дослідження особливо в умовах сучасних викликів в країні.

Метою цієї статті є аналіз стійкості критичної інфраструктури в Україні та пропозиція заходів, які сприятимуть її підвищенню в умовах сучасних викликів.

Виклад основних результатів дослідження. Вивчення основних факторів, які визначають стійкість критичної інфраструктури, а також розробка підходів до її посилення стають сьогодні для країни надзвичайно актуальною проблемою. Практично щоденно населення країни відчуває негативні наслідки обстрілів, зокрема й внаслідок руйнування об’єктів критичної інфраструктури.

Загалом, згідно з міжнародними стандартами, національними нормативно-правовими актами та науковими узагальненнями дослідників, критична інфраструктура охоплює об'єкти, системи та мережі, що забезпечують функціонування економіки, безпеку

суспільства та держави. Це важливі елементи, без яких неможливо забезпечити нормальне життя населення та підтримку базових державних функцій [1; 5; 8].

До ключових складових критичної інфраструктури за законодавством України відноситься:

- енергетична інфраструктура (енергетичні мережі, енергоблоки, системи електропостачання та газопостачання, електростанції, мережі енергопостачання, газові та нафтові магістралі, які забезпечують країну енергоресурсами для промисловості, транспорту та побутових потреб);
- транспортна інфраструктура (автомобільні, залізничні, авіаційні й водні шляхи, а також логістичні хаби, які гарантують переміщення товарів і людей по території країни та за її межами);
- інформаційно-комунікаційна інфраструктура (телекомунікаційні мережі, Інтернет, бази даних, мобільний зв'язок, інформаційні платформи, сервісні мережі та інші технології передачі даних, які забезпечують цифрову взаємодію та передачу даних);
- водопостачання та каналізація (системи постачання питної води, водовідведення та очистки стічних вод);
- охорона здоров'я (лікарні, медичні заклади, системи швидкої допомоги);
- фінансова інфраструктура (банки, платіжні системи, фондові ринки, які гарантують фінансову стабільність та безперервність економічних операцій);
- захист від надзвичайних ситуацій (служби порятунку, цивільного захисту, пожежні частини та інші органи, які займаються реагуванням на надзвичайні ситуації) [8].

Тобто, критична інфраструктура – це сукупність об'єктів і систем, що забезпечують безперебійне функціонування суспільства і економіки, а також забезпечують національну безпеку та добробут громадян. Оскільки не всі об'єкти мають однакову важливість для функціонування суспільства, їх можна класифікувати за критерієм критичності. Критичність визначається залежно від того, як швидко та якою мірою порушення їхньої роботи може вплинути на суспільні процеси, економіку, безпеку, здоров'я людей і довкілля.

Критичність об'єктів інфраструктури можна оцінити за основними критеріями, які представлені на рисунку 1.

Рис. 1. Критерії визначення критичності об’єктів інфраструктури
Джерело: складено автором

Значення для національної безпеки передбачає визначення впливу функціонування об'єкта на стабільність і захист держави.

Вплив на суспільство означає оцінку наслідків нестабільної роботи для життєдіяльності населення, добробуту громадян, доступу до основних послуг (наприклад, водопостачання, охорона здоров'я).

Економічний вплив характеризує оцінку важливості об’єкту з позицій того, як відсутність чи порушення його роботи позначиться на перебігу економічних процесів (виробництво, торгівля, фінансова стабільність).

Швидкість відновлення визначає час, необхідний для відновлення функціонування після надзвичайної ситуації.

Міжсекторальна залежність характеризує наявність залежностей від інших інфраструктур, які можуть погіршити ситуацію при їх збоях.

Отже, критичність інфраструктури визначається її здатністю забезпечувати життєво важливі функції, від яких залежить безпека, стабільність та добробут суспільства. Об'єкти критичної інфраструктури є важливими не лише з економічної, але й з соціальної та національної точки зору. Порушення їхньої роботи може спричинити серйозні економічні, соціальні, екологічні та політичні наслідки, що безпосередньо впливають на здатність держави і суспільства до нормального

функціонування. Слід акцентувати, що визначення критичності того чи іншого об'єкту залежить від відповідності всім критеріям одночасно (рис. 2).

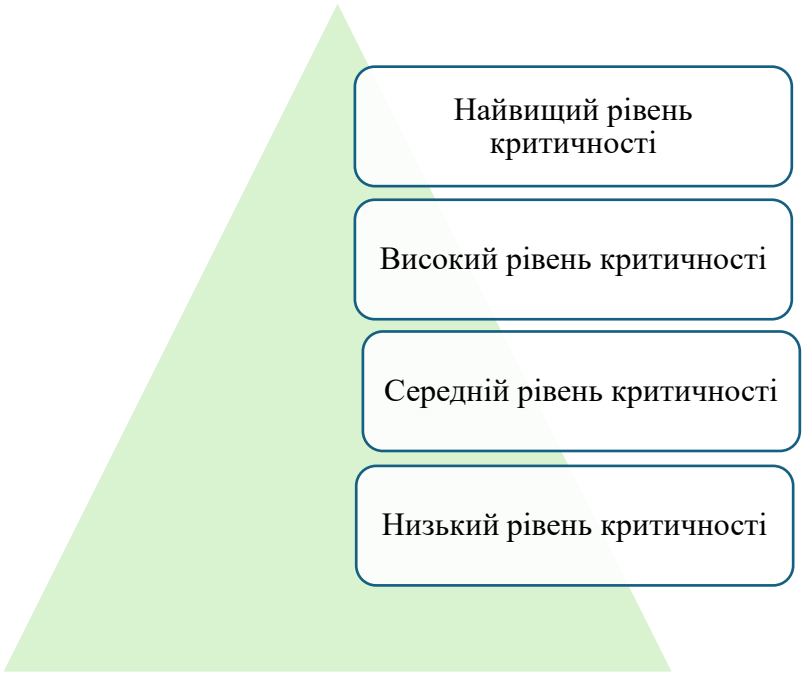

Рис. 2. Ієрархія критичності інфраструктури
Джерело: розроблено автором

У контексті розгляду критичної інфраструктури, її стійкість характеризується кількома основними аспектами, а саме [5; 9]:

По перше. Здатність до безперервності функціонування. Цей аспект передбачає, що стійка критична інфраструктура повинна забезпечувати безперервне надання основних послуг, таких як енергопостачання, водопостачання, транспорт, зв'язок, охорона здоров'я, навіть у випадку виникнення надзвичайних ситуацій або зовнішніх загроз. Наприклад, енергетична мережа повинна залишатися функціональною під час техногенних аварій, природних катастроф або навіть воєнних конфліктів.

По друге. Здатність до адаптації та гнучкості, яка визначає, що стійкість також передбачає здатність інфраструктури адаптуватися до змінних умов або нових загроз. Це може включати впровадження нових технологій, оновлення систем безпеки, а також зміни в управлінні чи організаційній структурі. Наприклад, у випадку зміни кліматичних умов чи збільшення кількості кіберзагроз, інфраструктура повинна бути здатною швидко адаптуватися до нових реалій.

По третє. Відновлювальна здатність. Цей аспект важливий до врахування, коли інфраструктура піддається руйнуванню через надзвичайні ситуації (природні катастрофи, терористичні акти, кібератаки чи інші фактори), стійкість визначається здатністю швидко відновлюватися і повернутися до нормального функціонування. Це включає наявність резервних систем, швидку реакцію на надзвичайні події та чітко налагоджені процеси відновлення.

По четверте. Захист від загроз та забезпечення безпеки, що означає здатність системи запобігати або мінімізувати вплив зовнішніх і внутрішніх загроз. Стійкість критичної інфраструктури у цьому разі включає в себе заходи щодо кібербезпеки, захисту фізичних об'єктів, а також управління ризиками, що можуть виникнути внаслідок природних або техногенних катастроф.

По п'яте. Міцність до зовнішніх і внутрішніх шоків, тобто здатність витримувати зовнішні шоки, такі як військові загрози, природні катастрофи, економічні кризи, а також внутрішні стреси, пов'язані з технічними неполадками чи людським фактором. Важливою складовою є також мінімізація ефектів від цих шоків, щоб не допустити великомасштабних руйнувань і порушень.

По шосте. Інтеграція з іншими системами, що часто визначається також здатністю критичної інфраструктури інтегруватися в загальну екосистему, включаючи взаємодію з іншими інфраструктурами та державними системами управління, що сприяє ефективному реагуванню на надзвичайні ситуації на всіх рівнях – від місцевого до національного.

По сьоме. Забезпечення стійкості в умовах цифрової трансформації. Цей аспект набуває особливого значення в умовах поширення цифровізації. У сучасному світі важливим аспектом стійкості є здатність інфраструктури функціонувати в умовах цифрових технологій, що включає в себе захист від кіберзагроз, інтеграцію нових технологій, а також забезпечення стійкості цифрових платформ, які підтримують економічні та соціальні процеси.

По восьме. Стійкість у контексті екологічних і соціальних факторів. Критична інфраструктура також має бути стійкою до екологічних змін, таких як зміна

клімату або природні катастрофи, а також здатною реагувати на соціальні виклики, наприклад, міграційні процеси або соціальні хвилювання. Вона повинна мати ресурси для адаптації і реагування на такі виклики без значного порушення функціонування.

Отже, стійкість – це здатність системи, організації чи інфраструктури ефективно функціонувати і відновлюватися після впливу різноманітних загроз або стресових факторів. Вона включає не лише здатність витримувати критичні навантаження, але й забезпечувати безперервність важливих функцій у довгостроковій перспективі, навіть у випадку серйозних порушень чи катастроф.

Таким чином, критичність об'єкта інфраструктури та першочергова важливість забезпечення його стійкості визначається впливом функціонування такого об'єкту на: *життєдіяльність населення* (доступ до основних послуг, таких як енергетика, водопостачання, охорона здоров'я, безпека), *економічну стабільність* (здатність підтримувати виробничі потужності, торгівлю, фінансову систему), *національну безпеку* (здатність забезпечити функціонування органів влади, оборонні об'єкти, цивільну оборону), *швидкість і можливість відновлення* (швидкість реагування на катастрофи і здатність відновити роботу в разі збоїв).

Кожен об'єкт інфраструктури має свій рівень критичності залежно від того, як його функціонування безпосередньо впливає на основні сфери життя країни та суспільства та наскільки важливий розгляд щодо нього стійкості у функціонуванні. Враховуючи зазначені критерії визначення критичності відповідних об'єктів інфраструктури доцільно врахувати ієрархією рівнів у цілях розроблення заходів захисту та їх імплементації в безпекові питання публічного управління (табл. 1).

Таблиця 1

Різновиди об'єктів інфраструктури за рівнем критичності

Рівень критичності	Характеристика та опис	Можливі різновиди об'єктів інфраструктури
Найвищий рівень критичності	Ці об'єкти мають вирішальне значення для безпеки держави, життєдіяльності населення та економіки. Їхнє порушення роботи може призвести до катастрофічних наслідків	- енергетичні системи (електростанції та мережі, особливо атомні та гідроелектростанції), газопостачальні мережі, нафтохімічні заводи і об'єкти зберігання нафти та газу); - транспортні мережі (міжнародні аеропорти, основні залізничні маршрути, особливо для вантажоперевезень), транспортні вузли та автомагістралі, що забезпечують перевезення вантажів і людей між регіонами та державами); - засоби зв'язку (центри комунікацій, телекомунікаційні мережі, радіо і телемовлення, особливо в умовах кризових ситуацій (наприклад, національні системи оповіщення); - водопостачальні та водовідведення системи (міські та регіональні водоочисні станції, великі водопостачальні магістралі); - системи охорони здоров'я (головні лікарні та медичні установи, лабораторії, що займаються аналізом епідемій та біологічними загрозами, системи постачання лікарських засобів та медичних матеріалів); - системи національної безпеки (об'єкти оборони та розвідки, інфраструктура цивільної оборони (укриття, мобілізаційні пункти).
Високий рівень критичності	Об'єкти, важливість яких не поступається переліку першої категорії, але їхнє пошкодження може призвести до серйозних, але не катастрофічних наслідків	- енергетична інфраструктура другого рівня (електричні підстанції, трансформаторні станції, паливні склади); - транспортні об'єкти другого рівня (міжнародні транспортні шляхи (наземний та водний транспорт), порти і вокзали, що забезпечують основні економічні та торгові зв'язки); - інфраструктура фінансових послуг (центральні банки, фондові біржі та інші фінансові установи, які забезпечують стабільність фінансової системи); - інфраструктура зв'язку другого рівня (регіональні сервери та дата-центри).
Середній рівень критичності	Ці об'єкти менш важливі для безпеки та економіки, але їхній збій може мати значний вплив на певні сфери	- інфраструктура житлово-комунального господарства (газопостачання для населення, місцеві водопостачальні станції); - система опалення та охолодження (теплові електростанції, обласні або регіональні теплоцентралі); - транспортні засоби для масового перевезення (автобуси, метрополітени, трамваї у великих містах).
Низький рівень критичності	Ці об'єкти мають обмежену важливість для функціонування інфраструктури, і їхня відсутність може спричинити лише короткочасні та обмежені наслідки	- системи охорони здоров'я місцевого рівня (лікарні та медпункти не основного призначення); - системи електропостачання для побутових потреб (місцеві електричні мережі та невеликі підстанції); - дрібні комунікаційні системи (телевізійні та радіомережі для місцевого масштабу).

Джерело: складено автором

Незважаючи на важливість критичної інфраструктури, вона піддається різноманітним загрозам, які можуть спричинити серйозні наслідки для національної безпеки та стабільності [6; 7; 10].

1. Воєнні загрози. Збройний конфлікт, який триває на сході України, а також зовнішні агресії створюють численні загрози для критичної інфраструктури. Від обстрілів та руйнувань енергетичних та транспортних мереж до блокування важливих постачальних ліній – ці фактори прямо впливають на здатність держави забезпечувати функціонування базових потреб суспільства.

2. Кіберзагрози. Зростання цифровізації та залежність від інформаційних технологій створюють нові ризики. Кібератаки, спрямовані на енергетичні мережі, фінансові установи або державні інформаційні системи, можуть призвести до порушень нормальної роботи економіки та створення паніки серед населення.

3. Природні катастрофи. Україна, як і багато інших країн, піддається ризикам від природних катастроф: повені, землетруси, бури та посухи можуть призвести до серйозних руйнувань в інфраструктурі, зокрема у транспорті та водопостачанні.

4. Техногенні аварії. У зв’язку з високим рівнем індустріалізації країни, аварії на великих промислових об'єктах, атомних станціях чи хімічних підприємствах можуть призвести до катастрофічних наслідків для навколишнього середовища та безпеки громадян.

5. Економічні та соціальні фактори. Недофінансування та зношеність інфраструктури, а також нестабільність у фінансовому секторі можуть істотно знизити рівень стійкості критичних об'єктів. Корупція, неефективне управління та відсутність стратегії розвитку також виступають як серйозні виклики.

Для повнішого розуміння варіантів забезпечення стійкості відповідних об’єктів критичної інфраструктури особливого значення набуває оцінка стійкості критичної інфраструктури. Така оцінка дає змогу за параметрами критичності стстематизувати відповідні об’єкти та розробити уніфіковані та стандартизовані заходи щодо забезпечення їх стійкості. Така оцінка може здійснюватися за використання відповідних кількісних та якісних методів в порядку реалізації основних етапів проведення оцінки. Послідовність етапів оцінки стійкості критичної інфраструктури як неперервність оцінювання уявлена на рисунку 3.

Рис. 3. Основні етапи оцінки стійкості критичної інфраструктури
Джерело: складено автором

Слід акцентувати на наявності успішних прикладів забезпечення стійкості критичної інфраструктури в умовах сьогоднішніх викликів.

Насамперед, міжнародний досвід має низку таких прикладів щодо природних катастроф та подолання їх наслідків. Зокрема, у США внаслідок часних ураганів та природних катастроф були введені нові технології для автоматизації енергомереж, що дозволяє швидше реагувати на аварії та зменшувати наслідки стихійних лих. Окрім того, створення інтегрованих систем реагування на катастрофи дозволяє швидко налагоджувати взаємодію між різними державними та приватними структурами.

Одним із успішних прикладів в Україні є відновлення енергетичної інфраструктури після обстрілів і руйнувань країни. Використання мобільних генераторів, резервних джерел енергії та системи автоматизованого моніторингу дозволяє забезпечувати

постачання електроенергії в регіони з високим рівнем пошкоджень.

Разом з тим, для підвищення стійкості критичної інфраструктури необхідно впроваджувати сучасні стратегії та технології, які враховують різноманітні загрози та виклики. Такі заходи мають передбачати:

- правові та нормативні ініціативи. В Україні уже активно розвивається нормативно-правова база для забезпечення безпеки критичної інфраструктури, але її потрібно удосконалювати у контексті посилення заходів з кібербезпеки, енергетичної безпеки та захисту державних інформаційних систем;
- впровадження новітніх технологій, таких як системи моніторингу, автоматичного управління та технології «розумних» мереж (smart grids), що дозволять не тільки підвищити ефективність функціонування інфраструктури, а й зменшити її вразливість до різних загроз;
- посилити розвиток кібербезпеки та підготовки кваліфікованих кадрів, зокрема шляхом інвестування в систему захисту національних інформаційних ресурсів;
- забезпечення енергетичної безпеки важливою шляхом диверсифікації джерел енергії та побудови резервних енергетичних систем. В Україні попри воєнні ризики розвиваються відновлювані джерела енергії, а також будуються нові потужності для збереження енергетичної автономії;
- посилення співпраці з міжнародними партнерами, зокрема з Європейським Союзом, що має важливе значення для забезпечення стійкості критичної інфраструктури. Обмін досвідом, технологіями та координація зусиль у разі глобальних криз дозволяють швидше реагувати на загрози.

Висновки. Стійкість критичної інфраструктури є комплексним та багатогранним поняттям, яке включає не тільки фізичний захист інфраструктурних об'єктів, але й адаптацію до змін, здатність відновлюватися після кризових ситуацій та забезпечення безпеки в умовах постійно змінюваних загроз. В умовах глобалізації та технологічних змін для досягнення стійкості критичної інфраструктури важливим є інтегрований підхід, що охоплює правові, технічні, економічні та соціальні аспекти, які містять в основі врахування рівня критичності відповідного об’єкту.

Забезпечення стійкості критичної інфраструктури в Україні є необхідною умовою для збереження національної безпеки та розвитку економіки. Враховуючи багатоаспектні загрози – від воєнних до кібернетичних і природних – Україні необхідно розвивати комплексну стратегію для захисту важливих об'єктів інфраструктури. Це включає наступні адміністративно-правові та інституційні заходи: удосконалення правового та нормативного забезпечення; впровадження новітніх технологій для підвищення ефективності та безпеки; розвиток кібербезпеки та підготовку кваліфікованих кадрів; розвиток міжнародного співробітництва для обміну досвідом та ресурсами.

Список використаних джерел:

1. Закон України "Про основи національної безпеки України" 19 червня 2003 року № 964-IV. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text
2. Закон України "Про основні засади забезпечення кібербезпеки України" 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. Указ Президента України. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про Стратегію забезпечення державної безпеки". 16 лютого 2022 року № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text
4. Суходоля О.М., Харазішвілі Ю.М., Бобро Д.Г., Сменковський А.Ю., Рябцев Г.Л., Завгородня С.П. (2020). Енергетична безпека України: методологія системного аналізу та стратегічного планування. 178 с. URL: https://niss.gov.ua/sites/default/files/2020-12/sukhodolia_energy_security_sayt-1.pdf
5. Суходоля О. (2023). Стійкість критичної інфраструктури ЄС: посилення політики та координації. НІСД, 9 с. URL: https://niss.gov.ua/sites/default/files/2023-02/az_eu-cip-coordinated_24022023.pdf
6. Cyber defence. (30 Jul. 2024). NATO. URL: https://www.nato.int/cps/uk/natohq/topics_78170.htm?selectedLocale=en
7. Гордієнко С.Г., Доронін І.М. (2024). Інформаційно-правові аспекти захисту критичної інфраструктури України. Інформація і Право. № 3(50). С. 115-123. DOI: https://doi.org/10.37750/2616-6798.2024.3(50).311678.
8. Яременко О.І., Страхніцький Я.І. (2022). Теоретичні підходи до визначення дефініції критичної інфраструктури як об’єкту державного управління. Публічне управління та митне адміністрування. № 1. С. 76-82. URL: http://customs-admin.umsf.in.ua/archive/2022/1/13.
9. Boin, A., & McConnell, A. (2007). Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. Journal of Contingencies and Crisis Management, Vol. 15. No. 1. Pp. 50-59. DOI: https://doi.org/10.1111/j.1468-5973.2007.00504.x
10. Guidotti, R., Chmielewski, H., Unnikrishnan, V., Gardoni, P., McAllister, T., & van de Lindt, J. (2016). Modeling the resilience of critical infrastructure: the role of network dependencies. Sustainable and Resilient Infrastructure, Vol. 1. No. 3–4. Pp. 153–168. DOI: https://doi.org/10.1080/23789689.2016.1254999
11. Sellevåg, Stig Rune. (2022). "Abstraction-decomposition space for critical infrastructure systems: A framework for infrastructure planning and resilience policies." Security and Defence Quarterly, Vol. 39. No. 3. Pp. 6-20. DOI: https://doi.org/10.35467/sdq/146789

References:

1. Zakon Ukrainy "Pro osnovy natsionalnoi bezpeky Ukrainy" vid 19 chervnia 2003 roku № 964-IV [Law of Ukraine "On the Fundamentals of National Security of Ukraine" from June 19. 2003. No. 964-IV]. Verkhovna Rada of Ukraine. Retrieved from: https://zakon.rada.gov.ua/laws/show/964-15#Text. [in Ukrainian].
2. Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy" vid 5 zhovtnia 2017 roku № 2163-VIII [Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" from October 5, 2017, No. 2163-VIII]. Verkhovna Rada of Ukraine. Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19#Text. [in Ukrainian].
3. Ukaz Prezydenta Ukrainy. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 30 hrudnia 2021 roku "Pro Stratehiiu zabezpechennia derzhavnoi bezpeky". 16 liutoho 2022 roku № 56/2022 [Decree of the President of Ukraine. On the Decision of the National Security and Defense Council of Ukraine dated December 30, 2021, "On the Strategy for Ensuring National Security" from February 16, 2022, No. 56/2022]. Verkhovna Rada of Ukraine. Retrieved from: https://zakon.rada.gov.ua/laws/show/56/2022#Text. [in Ukrainian].
4. Sukhodolia, O.M., Kharazishvili, Yu.M., Bobro, D.H., Smenkovskyi, A.Yu., Riabtsev, H.L., & Zavhorodnia, S.P. (2020). Enerhetychna bezpeka Ukrainy: metodolohiia systemnoho analizu ta stratehichnoho planuvannia. [Energy Security of Ukraine: Methodology of System Analysis and Strategic Planning.]. Kyiv: NISD. 175p. Retrieved from: https://niss.gov.ua/sites/default/files/2020-12/sukhodolia_energy_security_sayt-1.pdf. [in Ukrainian].
5. Sukhodolia O. (2023). Stiikist krytychnoi infrastruktury YeS: posylennia polityky ta koordynatsii [Critical Infrastructure Resilience in the EU: Strengthening Policy and Coordination]. Kyiv: NISD, 9 p. Retrieved from: https://niss.gov.ua/sites/default/files/2023-02/az_eu-cip-coordinated_24022023.pdf. [in Ukrainian].
6. NATO. (2024, July 30). Cyber defence. Retrieved from: https://www.nato.int/cps/uk/natohq/topics_78170.htm?selectedLocale=en.
7. Hordiienko, S.H., & Doronin, I.M. (2024). Informatsiino-pravovi aspekty zakhystu krytychnoi infrastruktury Ukrainy [Information and Legal Aspects of Protecting Critical Infrastructure of Ukraine]. Informatsiia i Pravo - Information and Law, No. 3(50). Pp. 115-123. DOI: https://doi.org/10.37750/2616-6798.2024.3(50).311678. [in Ukrainian].
8. Yaremenko, O.I., & Strakhnitskyi, Ya.I. (2022). Teoretychni pidkhody do vyznachennia definitsii krytychnoi infrastruktury yak obiektu derzhavnoho upravlinnia [Theoretical Approaches to Defining the Concept of Critical Infrastructure as an Object of Public Administration]. Publichne upravlinnia ta mytne administruvannia - Public Administration and Customs Administration, No. 1. Pp. 76-82. Retrieved from: http://customs-admin.umsf.in.ua/archive/2022/1/13.pdf. [in Ukrainian].
9. Boin, A., & McConnell, A. (2007). Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. Journal of Contingencies and Crisis Management, Vol. 15. No. 1. Pp. 50-59. DOI: https://doi.org/10.1111/j.1468-5973.2007.00504.x
10. Guidotti, R., Chmielewski, H., Unnikrishnan, V., Gardoni, P., McAllister, T., & van de Lindt, J. (2016). Modeling the resilience of critical infrastructure: the role of network dependencies. Sustainable and Resilient Infrastructure, Vol. 1. No. 3-4. Pp. 153-168. DOI: https://doi.org/10.1080/23789689.2016.1254999
11. Sellevåg, S.R. (2022). Abstraction-decomposition space for critical infrastructure systems: A framework for infrastructure planning and resilience policies. Security and Defence Quarterly, Vol. 39. No. 3. Pp. 6-20. DOI: https://doi.org/10.35467/sdq/146789