The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No.4 (2024)

DOI: 10.62524/msj.2024.2.4.15

Роль інфраструктурної безпеки у стратегіях сталого розвитку: політико-правовий аспект

Галина Куспляк
кандидат наук з державного управління, доцент
доцент кафедри місцевого самоврядування та розвитку територій
Інститут публічної служби та управління
Національний університет "Одеська політехніка"
м. Одеса, Україна
e-mail: kusplyak.galina@gmail.com
ORCID: 0000-0002-1414-5484

Оксана Дуліна
кандидат юридичних наук, доцент
доцент кафедри публічного управління та регіоналістики
Інститут публічної служби та управління
Національний університет "Одеська політехніка"
м. Одеса, Україна
e-mail: oksana_dulina@ukr.net
ORCID: 0000-0002-1009-558X

Катерина Ровинська
кандидат наук з державного управління, доцент
доцент кафедри державознавства, права та європейської інтеграції
Навчально-науковий інститут публічної служби та управління
Національний університет "Одеська політехніка"
м. Одеса, Україна
e-mail: rovkateryna@gmail.com
ORCID: 0000-0002-1334-3112

Анотація. Актуальність дослідження зумовлена зростанням загроз і викликів, що постають перед критичною інфраструктурою України, зокрема в умовах широкомасштабної війни, кібератак, техногенних катастроф і природних лих. Недостатня розвиненість нормативно-правового регулювання, фрагментарність державної політики та обмежена координація між суб'єктами управління критичною інфраструктурою створюють ризики для національної безпеки і сталого розвитку країни.

Метою дослідження є всебічний аналіз сучасного стану нормативно-правового регулювання інфраструктурної безпеки, визначення основних загроз і викликів, що впливають на функціонування критичної інфраструктури, а також розроблення рекомендацій щодо вдосконалення політико-правових інструментів для забезпечення її стійкості.

Методи дослідження охоплювали аналіз чинної нормативно-правової бази, порівняння національного й міжнародного досвіду організації захисту критичної інфраструктури, системний підхід до ідентифікації загроз і ризиків, а також використання методів прогнозування для розроблення рекомендацій.

Результати дослідження показали, що в Україні є низка проблем у сфері захисту критичної інфраструктури, зокрема: відсутність чіткого переліку об'єктів стратегічної

інфраструктури, недостатнє нормативне регулювання комунікаційної інфраструктури, обмежена інтеграція сучасних методологій і технологій у процеси управління ризиками. Світовий досвід свідчить про необхідність створення комплексної системи захисту критичної інфраструктури, що базується на чіткій координації між органами державної влади, підготовці фахівців і регулярному оцінюванні ризиків. Наголошено, що для посилення інфраструктурної безпеки в Україні необхідно: створити чітку нормативно-правову базу, яка регулюватиме питання, що стосуються захисту критичної інфраструктури; інтегрувати в державну політику механізми міжнародної співпраці, обміну інформацією та найкращими практиками; вдосконалити підготовку фахівців у сфері захисту критичної інфраструктури; забезпечити чітку регламентацію та координацію між секторами цієї інфраструктури на національному, регіональному та об'єктовому рівнях.

Ключові слова: національна безпека, інфраструктурна безпека, критична інфраструктура, сталий розвиток, концепція сталого розвитку, політико-правовий аспект, нормативно-правове забезпечення, глобальні виклики.

Вступ (Introduction)

У сучасному світі сталий розвиток є основною концепцією, яка визначає довгострокові пріоритети соціально-економічного розвитку країн. Водночас інфраструктурна безпека відіграє ключову роль у забезпеченні стабільності та ефективності впровадження стратегій сталого розвитку. Інфраструктура як комплекс взаємопов'язаних систем, до якого належать, зокрема, транспорт, енергетика, водопостачання, інформаційні мережі, є не лише основою економічної діяльності, а й критично важливим елементом суспільної життєздатності.

Проте сучасні виклики, як-от зміна клімату, збройні конфлікти, технологічні ризики та все більша залежність від цифрових технологій, створюють загрози для інфраструктурної безпеки. У цьому контексті виникає необхідність адаптації політико-правових механізмів, які забезпечуватимуть захист інфраструктури, її стійкість та здатність реагувати на сучасні виклики.

Проблема ускладнюється тим, що в багатьох країнах немає комплексних підходів до інтеграції питань щодо інфраструктурної безпеки у стратегії сталого розвитку. Крім того, нормативно-правова база часто не враховує специфічних потреб захисту критичної інфраструктури та можливостей міжнародної співпраці у цій сфері.

Дослідники акцентують увагу на важливості інтеграції питань щодо безпеки критичної інфраструктури в державні стратегії розвитку. Зокрема, у роботах С. С. Кларк (S. S. Clark), Т. П. Сігер (T. P. Seager), М. В. Честер (M. V. Chester) [1], Ф. Фусо Неріні (F. Fuso Nerini) [2] вивчаються загрози, спричинені змінами клімату, терористичною діяльністю та технологічними збоями.

Низка досліджень містить розробки механізмів забезпечення стійкості інфраструктури до зовнішніх викликів. Такі автори, як Л. О. Зайцева [3], Я. О. Страхніцький [4], аналізують роль міжнародної співпраці в розв'язанні проблем безпеки, наголошуючи на необхідності гармонізації нормативно-правової бази в різних країнах. Інші вчені, зокрема В. Ліпкан [5] та Г. Зубко [6], акцентують увагу на використанні інноваційних технологій для моніторингу та прогнозування ризиків у сфері інфраструктурної безпеки.

Однак, попри значний прогрес, є й певні прогалини. По-перше, недостатньо уваги приділено політико-правовим аспектам інтеграції інфраструктурної безпеки у стратегії сталого розвитку. По-друге, дослідження, які аналізують досвід конкретних країн у цьому напрямі, часто є фрагментарними. Нарешті, бракує міждисциплінарного підходу, який поєднував би політико-правові, економічні та технологічні аспекти проблеми. З огляду на

наведене, виникає необхідність наукового аналізу ролі інфраструктурної безпеки у стратегіях сталого розвитку, а також розроблення ефективних політико-правових інструментів, які сприятимуть забезпеченню стійкості та безпеки інфраструктури.

Метою дослідження є аналіз політико-правових аспектів забезпечення інфраструктурної безпеки у стратегіях сталого розвитку, виявлення ключових викликів та розроблення рекомендацій щодо їх подолання.

Відповідно до поставленої мети визначено такі завдання:

– дослідити сучасний стан нормативно-правового регулювання інфраструктурної безпеки в контексті сталого розвитку;

– проаналізувати ключові загрози та виклики, що впливають на інфраструктурну безпеку;

– оцінити досвід окремих країн у впровадженні стратегій сталого розвитку з урахуванням безпеки критичної інфраструктури.

Матеріали та методи (Materials and Methods)

Матеріалами для дослідження є нормативно-правові акти, зокрема міжнародні договори, національні закони та підзаконні акти, які регулюють питання щодо інфраструктурної безпеки. Крім того, використовувалися аналітичні звіти таких міжнародних організацій, як ООН, Світовий банк і Європейська комісія, що містять актуальну інформацію про впровадження стратегій сталого розвитку. Значну частину даних було отримано з наукових публікацій із баз даних Scopus, Web of Science та Google Scholar, які висвітлюють ключові аспекти інфраструктурної безпеки. Досліджувалися дані з відкритих джерел, зокрема офіційних сайтів урядових органів і міжнародних установ.

Методологічно дослідження базувалося на комплексному підході. Метод аналізу та синтезу дозволив систематизувати нормативно-правові акти й наукові праці, виокремлюючи ключові аспекти політико-правового регулювання інфраструктурної безпеки. Порівняльно-правовий метод застосовувався для аналізу підходів до такого регулювання в різних країнах, що дало змогу виявити найкращі практики та наявні прогалини. Метод контент-аналізу допоміг глибоко дослідити тексти нормативно-правових актів і стратегічних документів для визначення їх відповідності цілям сталого розвитку. Емпіричний метод використовувався для аналізу конкретних випадків загроз інфраструктурній безпеці, як-от кібератаки, техногенні аварії та терористичні акти, що дозволило розробити рекомендації щодо їх попередження. Міждисциплінарний підхід об’єднав правові, економічні та соціальні аспекти, створюючи цілісну концепцію інтеграції безпекових компонентів у стратегії сталого розвитку.

Перебіг дослідження складався із трьох основних етапів. На підготовчому етапі було зібрано та систематизовано матеріали, відібрано релевантні джерела та сформовано аналітичну базу даних. Основний етап включав проведення порівняльного аналізу політико-правового регулювання, детальне дослідження прикладів загроз інфраструктурній безпеці та розроблення теоретичної моделі інтеграції безпекових аспектів у стратегії сталого розвитку. На завершальному етапі узагальнено отримані результати, сформульовано рекомендації та висновки, а також підготовлено пропозиції для вдосконалення нормативно-правової бази.

Запропонований методологічний підхід забезпечив глибоке розуміння досліджуваної проблеми, дозволивши досягти поставленої мети.

Результати (Results)

Сучасний розвиток демократичного суспільства неможливий без гармонійного функціонування базових секторів, які забезпечують життєдіяльність населення. Енергетика, транспорт, телекомунікації, водо- та газопостачання, медицина й інші подібні сфери

становлять основу критичної інфраструктури, від якої залежить нормальне життєзабезпечення. Дисфункція будь-якого із цих секторів загрожує серйозними наслідками: порушенням суспільного порядку, значними економічними втратами, техногенними катастрофами та руйнуванням життєво важливих об'єктів.

Особливої гостроти питання щодо інфраструктурної безпеки набуло в умовах сучасної ситуації в Україні. Широкомасштабна війна спричинила безпрецедентний рівень загроз для об'єктів критичної інфраструктури, які стали ціллю для диверсій, терористичних атак та несанкціонованих втручань [4, с. 115]. Такі дії не лише завдають матеріальних збитків, а й використовуються агресором як зброя морально-психологічного терору проти мирного населення, що має на меті внутрішню дестабілізацію країни.

Інфраструктурна безпека є невід'ємною складовою частиною сталого розвитку. Її забезпечення передбачає стійкість і надійність базових секторів, без яких неможливе досягнення цілей сталого розвитку – економічної стабільності, соціальної справедливості та екологічної рівноваги.

Безпека критичної інфраструктури є не лише національним, а й міжнародним викликом, адже руйнування ключових об'єктів може мати значний вплив за межами однієї країни. Наприклад, загрози для енергетичної безпеки України вже стали проблемою для Європейського Союзу, що свідчить про необхідність узгоджених дій у формуванні комплексної системи захисту. У таких умовах особливо важливими стають загальнодержавні заходи, які передбачають координацію між безпековими, правоохоронними органами та міжнародними партнерами для протидії сучасним гібридним загрозам.

В Україні питання щодо інфраструктурної безпеки вперше отримало нормативне закріплення на державному рівні у 2015 році зі схваленням Стратегії національної безпеки України [7]. У документі серед загроз національній безпеці було виділено безпеку критичної інфраструктури, кібербезпеку та безпеку інформаційних ресурсів. Такий підхід став визнанням того, що вразливість стратегічних об'єктів може мати далекосяжні наслідки для життєздатності держави та суспільства.

Серед основних чинників, які актуалізували проблему інфраструктурної безпеки, були критична зношеність основних фондів об'єктів, недостатній рівень їх захищеності та відсутність розроблених основ політики безпеки інфраструктури. Зрештою, ці фактори стали основою для прийняття більш цілісного підходу, який знайшов своє відображення в новій редакції Стратегії національної безпеки і оборони України у 2020 році [8].

Закон України "Про критичну інфраструктуру" визначає її захист як один із ключових складників забезпечення національної безпеки держави [9]. У цьому контексті формування державної політики щодо захисту критичних об'єктів має базуватися на врахуванні переліку загроз, визначених у Стратегії національної безпеки України.

Серед ключових викликів, які постають перед сучасним світом, важливе місце посідають кліматичні зміни. Вони провокують ризики, що можуть спричинити надзвичайні ситуації як природного, так і техногенного характеру, а також сприяють поширенню інфекційних захворювань. Крім того, актуальними є загрози, пов'язані з гонитвою озброєнь, зокрема на основі новітніх фізичних принципів, що формує небезпеки у воєнній і технологічній сферах.

Значну увагу слід приділити загрозам міжнародного масштабу, як-от тероризм, кіберзлочинність, нелегальний обіг наркотиків, торгівля людьми, сепаратизм і розповсюдження зброї. До цього додаються наслідки пандемії COVID-19, яка викликала численні кризи – від проблем у сфері охорони здоров'я та соціального захисту до нестабільності в економіці та продовольчій безпеці.

Окремо варто відзначити посилення глобальної конкуренції, яка часто супроводжується демонстрацією "національної сили". Для України ця проблема є особливо

значущою в умовах широкомасштабного вторгнення російської федерації. Відсутність належного фінансування для модернізації озброєння радянського виробництва, яке вже віджило свій ресурс, стає додатковим бар'єром у забезпеченні національної безпеки.

Серед інших викликів слід виділити недостатню ефективність державних органів, високий рівень корупції, що знижує довіру до інституцій, а також низький рівень добробуту населення, який підсилює соціальну напругу. Недосконаліть правової системи та проблеми у ключових секторах, зокрема енергетичному, стримують інвестиційну активність, а значна частка державного сектору в економіці гальмує її розвиток.

Екологічні питання, як-от зниження якості повітря, води, продуктів харчування та нераціональне використання природних ресурсів, значно впливають на стійкий розвиток держави. До цього додаються демографічні виклики, зокрема еміграція кваліфікованих кадрів, що ставить під загрозу стабільність у соціально-економічній сфері.

Особливу увагу необхідно приділити питанням, що стосуються захисту критичної інфраструктури. Серед основних проблем – поганий технічний стан об'єктів, нестача інвестицій в їхню модернізацію, а також фізичні та кіберзагрози, що посилюються у зв'язку з бойовими діями та окупацією частини території країни. Усі ці аспекти підкреслюють нагальність розроблення комплексного підходу до захисту критичної інфраструктури, який має стати основою для гарантування національної безпеки України. Одним із важливих кроків на шляху розв'язання проблем стало ухвалення Концепції створення державної системи захисту критичної інфраструктури [10]. Документ заклав основи для формування ефективної системи безпеки, яка базується на чіткому розподілі відповідальності між суб'єктами управління та партнерській співпраці з іншими органами влади. Основна мета Концепції полягає у створенні дієвих механізмів захисту, здатних забезпечити стійкість інфраструктури перед обличчям сучасних викликів.

Стаття 7 Закону України "Про критичну інфраструктуру" визначила багаторівневу структуру державного управління у цій сфері (табл. 1).

Таблиця 1. Рівні управління критичною інфраструктурою України

Назва	Характеристика
Загальнодержавний рівень	Управління здійснюють Кабінет Міністрів України, уповноважений орган у сфері захисту критичної інфраструктури, а також органи державної влади, центральні виконавчі органи, державні установи та Національний банк України, відповідно до їхніх повноважень
Регіональний і галузевий рівні	Управління реалізується через центральні та місцеві органи виконавчої влади, які відповідають за розроблення і виконання державної політики у відповідних секторах
Місцевий рівень	Управління здійснюють військово-цивільні адміністрації, що діють під час воєнного стану, а також органи місцевого самоврядування, які забезпечують виконання своїх завдань у межах наданих їм повноважень
Об'єктовий рівень	Передбачає управління операторами критичної інфраструктури, які діють на підставі нормативно-правових і регуляторних актів, що регулюють сферу захисту об'єктів критичної інфраструктури

Джерело: складено автором на основі [9].

Державна політика у сфері захисту критичної інфраструктури України формується та реалізується за участю кількох ключових органів влади, кожен з яких виконує свої специфічні функції, забезпечуючи ефективність і комплексність цього процесу [4, с. 136].

Кабінет Міністрів України відіграє центральну роль у впровадженні державної політики. Він організовує та забезпечує функціонування національної системи захисту критичної інфраструктури (далі – КІ), надаючи необхідні ресурси, сили та засоби для її безперебійної роботи. Крім того, уряд визначає уповноважений орган, відповідальний за питання захисту КІ, та затверджує регламент обміну інформацією між суб'єктами національної системи, що дозволяє забезпечити належну взаємодію, оперативність та координацію у розв'язанні завдань захисту.

Секторальні та функціональні органи відіграють важливу роль у формуванні й реалізації політики в окремих секторах критичної інфраструктури. Вони несуть відповідальність за розроблення та впровадження заходів, спрямованих на підвищення рівня захисту об'єктів, що належать до їхньої компетенції.

Координаційну функцію в національній системі захисту критичної інфраструктури виконує уповноважений орган. Він забезпечує узгодженість діяльності всіх суб'єктів системи, сприяючи ефективному функціонуванню механізмів захисту на всіх рівнях.

Г. Ю. Зубко слушно звертає увагу на інституційну недосконаліть державної політики у сфері захисту КІ в умовах воєнного стану в Україні, акцентуючи на стратегічній випадковості, розпорошеності й подекуди фрагментарності політики, що суттєво ускладнює формування цілісної та ефективної стратегії національної безпеки. Такий стан справ створює значні бар'єри для реалізації узгоджених заходів, спрямованих на захист КІ [6, с. 167]. Особливо актуальним є питання щодо забезпечення ефективної взаємодії між усіма суб'єктами, які беруть участь у формуванні та реалізації державної політики. Необхідність належної координації дій різних органів влади, підвищення рівня комунікації та створення єдиного підходу до управління системою захисту критичної інфраструктури є важливими для забезпечення національної безпеки. Без чіткої взаємодії та скоординованих зусиль формування надійної системи захисту стає практично неможливим, що лише підсилює виклики й загрози в умовах широкомасштабної війни.

Для ефективного формування та реалізації державної політики у сфері захисту критичної інфраструктури необхідно врахувати низку проблемних аспектів, зокрема питання стосовно комунікаційної політики держави, яке потребує не лише наукового осмислення, а й концептуального визначення на державному рівні. Натепер комунікаційна політика залишається недостатньо регульованою, а її стратегічна складова частина лише частково представлена в нормативно-правовій базі [11, с. 80].

Єдиним нормативним документом, який прямо регулює напрям, є Концепція Закону України "Про основні засади державної комунікативної політики" [12]. У ній передбачено окремі аспекти налагодження комунікацій між органами влади, місцевого самоврядування, засобами масової інформації та громадськістю. Однак документ має обмежену правову силу, не відповідає сучасним викликам українського суспільства та не враховує глобальні тенденції у сфері стратегічних комунікацій.

Для ефективного формування та реалізації державної політики у сфері безпеки стратегічної інфраструктури необхідно визначити та законодавчо закріпити чіткий перелік її секторів і об'єктів, а також установити порядок їхньої паспортизації. Натепер на законодавчому рівні в Україні немає офіційного переліку таких об'єктів, що створює суттєві перешкоди для розроблення системної політики у цій сфері.

У Законі України "Про критичну інфраструктуру" зазначено лише загальні життєво важливі функції та послуги, зокрема: урядування, енергозабезпечення, водопостачання, охорона здоров'я, інформаційні послуги, транспорт, оборона, правопорядок тощо [9]. Однак у переліку не враховані важливі об'єкти, які широко визнані в міжнародній практиці, як-от хімічний сектор, дамби, гідротехнічні споруди, комерційні об'єкти, ядерні реактори, служби екстреної допомоги тощо.

Залишається нерозв'язаним питання щодо формування національного та секторального переліків об'єктів стратегічної інфраструктури. На законодавчому рівні цей процес регламентовано лише частково, переважно для інформаційної інфраструктури. Наприклад, постановою Кабінету Міністрів України від 9 жовтня 2020 року № 943 визначено порядок формування переліку об'єктів критичної інформаційної інфраструктури [13]. Для банківської системи аналогічний порядок установлено постановою Правління Національного банку України від 30 листопада 2020 року № 151 [14].

Однак в інших секторах стратегічної інфраструктури подібних механізмів немає, що ускладнює координацію та взаємодію між суб'єктами публічного управління у сфері безпеки КІ, а також перешкоджає їхній інтеграції в єдину систему. Для подолання проблем необхідно розробити комплексний підхід до нормативно-правового забезпечення, який включатиме всі ключові сектори стратегічної інфраструктури та чітко визначатиме їхню роль у національній безпеці.

Наступним важливим аспектом, який потребує чіткого визначення та закріплення в нормативно-правових актах, є суб'єкти державної системи безпеки критичної інфраструктури, котрі формують організаційно-інституційну структуру системи, визначають її функціональність та ефективність. Для забезпечення її належного функціонування необхідно реалізувати низку заходів на різних рівнях: загальнодержавному, галузевому, місцевому та об'єктовому.

Наразі у відповідних документах, зокрема Концепції [10] та Законі України "Про критичну інфраструктуру" [9], лише окреслено загальні завдання, які мають виконуватися на кожному рівні. Проте немає конкретних визначень органів державного управління, установ, організацій та інших суб'єктів, відповідальних за забезпечення безпеки стратегічної інфраструктури, її стійкості та протидії загрозам. Зазначене створює невизначеність у реалізації державної політики, особливо в розподілі повноважень і відповідальності між суб'єктами.

У наукових дослідженнях запропоновано лише загальний перелік секторів стратегічної інфраструктури та відповідних відомств [15]. Однак окреслені пропозиції потребують значного доопрацювання, зокрема в аспектах нормативно-правового закріплення, організаційного та методологічного забезпечення. Крім того, необхідно провести додатковий науковий аналіз для вдосконалення процесу ідентифікації об'єктів стратегічної інфраструктури та уточнення переліку суб'єктів, які мають відповідні повноваження.

Питання щодо розбудови парадигми державної політики у сфері захисту КІ на основі світового досвіду є надзвичайно актуальним для України в умовах сучасних викликів і загроз. У цьому контексті заслуговують на увагу дослідження вченого Д. Г. Бобро, який виділив ключові кроки, що можуть слугувати орієнтиром для формування ефективної системи захисту критичної інфраструктури [16].

Створення сучасної нормативно-правової основи є першочерговим завданням для забезпечення захисту КІ. Законодавчі акти мають бути адаптовані до сучасних умов, враховувати світові практики та забезпечувати гнучкість у реагуванні на нові загрози. Важливою складовою частиною процесу є регулярна модернізація законодавства, що дозволяє інтегрувати нові технологічні рішення та методології.

Наступним етапом є розроблення чітких методологій для формування переліків об'єктів критичної інфраструктури, а також для оцінювання ризиків та загроз. Підходи мають враховувати специфіку секторів та потенційні загрози. Без належної методологічної бази неможливо забезпечити комплексний підхід до захисту інфраструктури.

Одним із фундаментальних елементів захисту КІ є наявність висококваліфікованих фахівців. Підготовка таких кадрів має здійснюватися в рамках спеціалізованих освітніх

програм, тренінгів та симуляційних вправ. Інвестування в людський капітал є запорукою стабільності системи.

Налагодження взаємодії між суб'єктами КІ, як на національному, так і на міжнародному рівнях, є ключовим фактором успіху. Обмін інформацією, найкращими практиками й технологіями дозволяє підвищити ефективність управління та захисту інфраструктури.

Україна має використовувати найкращі міжнародні практики, адаптуючи їх до власних умов. У цьому контексті на особливу увагу заслуговують США та Польща [17, с. 31–32]. Зазначені країни вибрано як приклад з огляду на їхні здобутки та релевантність досвіду для України.

США є світовим лідером щодо інноваційних підходів, держава володіє розгалуженою та ефективною національною системою безпеки критичної інфраструктури. Їхній досвід у координації, управлінні ризиками та впровадженні сучасних технологій є надзвичайно цінним. Система захисту КІ у США базується на чітко визначених політичних і законодавчих актах, що регламентують основні терміни, концепції та підходи у цій сфері. Президентська директива PPD-21 деталізує підходи до безпеки та стійкості КІ. Зокрема, безпека трактується як зменшення ризиків через фізичні та кіберзахисні заходи, тоді як стійкість розглядається як здатність адаптуватися до змін, протистояти загрозам і швидко відновлюватися після криз [18].

З 2005 року державна політика США у сфері критичної інфраструктури реалізується через плани захисту національної інфраструктури, які регулярно оновлюються. Примітно, що поняття "захист критичної інфраструктури" чітко не визначене в законодавстві, що пояснюється використанням загальних принципів, уже закріплених для інших сфер захисту, як-от ядерна безпека.

США прагнуть посилити безпеку і стійкість КІ шляхом управління ризиками, їхні зусилля спрямовані на зменшення вразливостей, мінімізацію наслідків, ідентифікацію загроз і прискорення реагування. Федеральний уряд активно співпрацює з власниками та операторами об'єктів КІ, місцевими органами влади та міжнародними партнерами. Важливо, що політика США враховує взаємозв'язки між елементами КІ, що дозволяє забезпечувати їхню інтегровану захищеність.

Особливо критичними вважаються енергетичні системи та системи зв'язку, які забезпечують функціонування інших секторів КІ. У PPD-21 визначено три стратегічні імперативи для реалізації державної політики: уточнення та роз'яснення взаємозв'язків між урядовими структурами для забезпечення єдності підходів; забезпечення ефективного обміну інформацією між усіма учасниками процесу; інтеграція та аналіз даних для підтримки планування та ухвалення рішень щодо КІ.

Керівники міністерств та федеральних агентств відповідають за оцінювання загроз, розроблення коригувальних заходів та забезпечення безпеки підпорядкованих їм об'єктів КІ, які мають особливе значення для виконання життєво важливих функцій держави. Зокрема, Велика Британія є однією з європейських лідерів у впровадженні систем захисту критичної інфраструктури, активно розвиває концепцію безпеки КІ та неодноразово висловлювала готовність надавати підтримку Україні. Така взаємодія створює можливості для запозичення найкращих практик.

Польща, як сусід України, має подібні економічні та демографічні характеристики, що робить її досвід релевантним для моделювання української системи захисту критичної інфраструктури. Польща успішно розвиває власну інфраструктуру безпеки, враховуючи регіональні виклики та міжнародні стандарти, що може теж стати орієнтиром для України.

Правові основи функціонування системи захисту КІ в Польщі регламентовані низкою ключових документів, зокрема Законом про кризове управління від 26 квітня 2007 року [19].

Хоча закон прямо не пояснює, чому саме тоді було розпочато роботу із захисту КІ на національному рівні, очевидно, що поштовхом стала активізація діяльності Європейського Союзу в середині 2000-х років. Саме ЄС розробив стратегічні документи з питань захисту КІ, що вплинуло на формування національних систем у країнах Східної Європи, зокрема Польщі, Чехії, Угорщини та Болгарії.

Особливістю Національної програми захисту критичної інфраструктури Польщі є використання безсанкційного підходу, що дозволяє знайти баланс між державним регулюванням і фінансовими витратами операторів КІ на гарантування безпеки. Однак уряд Польщі залишає за собою право змінити цей підхід, якщо він виявиться недостатньо ефективним. Основоположні принципи реалізації Національної програми мають такий зміст: по-перше, захист КІ є спільним завданням державних органів, операторів КІ, суспільства та економіки, тобто цей принцип ураховує критичну важливість безпеки КІ для держави загалом; по-друге, зважаючи на складність і взаємозалежність завдань, забезпечення захисту КІ потребує спільних дій усіх суб'єктів, ефективного використання доступних ресурсів і можливостей [17].

Отже, правові засади захисту КІ в Польщі базуються на прагненні інтегрувати національні та європейські стандарти, врахувати специфіку регіону та створити ефективну систему співпраці між державою, бізнесом і суспільством для забезпечення сталого функціонування критичної інфраструктури.

Розвиток системи захисту критичної інфраструктури у світі пов'язаний зі швидкими змінами в глобальному, регіональному та національному безпековому середовищі. Зміни знаходять відображення у вдосконаленні законодавчих основ, термінології та структур, що забезпечують діяльність відповідних систем.

Таким чином, реалізація наведених вище кроків може стати основою для формування дієвої системи захисту критичної інфраструктури, що відповідає світовим стандартам. Застосування кращих практик дозволить не лише підвищити стійкість об'єктів до зовнішніх і внутрішніх загроз, а й сприятиме інтеграції України в міжнародні механізми захисту стратегічної інфраструктури.

Обговорення (Discussions)

Аналіз отриманих даних підтвердив положення, висловлені Д. Г. Бобро, щодо необхідності створення чіткої нормативно-правової бази та визначення координуючого органу, відповідального за управління захистом критичної інфраструктури [16]. Результати дослідження узгоджуються з підходами, запропонованими Департаментом внутрішньої безпеки США, де центральний координуючий орган забезпечує ефективну взаємодію між різними секторами критичної інфраструктури.

Водночас у дослідженні було виявлено, що низка аспектів, які у світовій практиці вважаються базовими (наприклад, методологія оцінювання ризиків та загроз, механізми формування переліків критичних об'єктів), в Україні все ще перебувають на етапі концептуалізації. Про це зазначено у висновках Г. Ю. Зубко [6], який наголошує на необхідності адаптації західних підходів до оцінювання ризиків, але вказує на їхню фрагментарність в українському контексті.

Зіставлення отриманих результатів дослідження із працями зарубіжних учених, зокрема Л. А. Арсеновича [15], свідчить про загальну тенденцію до інституційної децентралізації у сфері захисту критичної інфраструктури. Учений акцентує увагу на важливості співпраці між державними та приватними структурами, що забезпечує гнучкість та оперативність системи. У цьому аспекті отримані результати демонструють подібність до висновків Л. А. Арсеновича, хоча в Україні така співпраця потребує додаткового законодавчого унормування.

Окремим питанням є розбудова комунікаційної інфраструктури як складника стратегічної інфраструктури. У рамках нашого дослідження підтверджено, що її роль залишається недооціненою в українському законодавстві, що співзвучно з висновками Л. О. Зайцева [3]. Водночас аналіз європейського досвіду, зокрема моделі ЄС, продемонстрував ефективність інтеграції комунікаційної інфраструктури в загальну систему захисту критичної інфраструктури.

Щодо кадрового забезпечення системи захисту КІ отримані висновки збігаються з дослідженнями М. Ажажа, Я. Пеліова, Т. Несторенко [11], які підкреслюють важливість створення спеціалізованих програм підготовки кадрів. Аналогічні тенденції спостерігаються і в представленому аналізі української системи, де кадровий потенціал поки що не відповідає світовим стандартам.

Отже, результати дослідження демонструють, що основними проблемами залишаються фрагментарність нормативно-правової бази, відсутність чіткої координації між суб'єктами, недосконаліть кадрового забезпечення та недооцінка комунікаційної інфраструктури. Усі аспекти потребують комплексного підходу для вирішення, що стане основою для формування висновків та практичних рекомендацій, які викладено в наступному розділі.

Висновок (Conclusion)

Аналіз сучасного стану нормативно-правового регулювання інфраструктурної безпеки в контексті сталого розвитку показав, що в Україні ця сфера перебуває на етапі формування. Це створює значні виклики для забезпечення стабільності та сталого розвитку. Попри наявність окремих законодавчих ініціатив, як-от Закон України "Про критичну інфраструктуру", нормативно-правова база є фрагментарною та не охоплює всі аспекти захисту критичної інфраструктури. Зокрема, немає чітко визначених функцій та повноважень суб'єктів державного управління, а також механізмів координації їхньої діяльності.

Дослідження виявило основні загрози та виклики, що впливають на інфраструктурну безпеку. Серед них слід виокремити кібератаки, техногенні аварії, природні катастрофи та воєнні дії. Особливу увагу слід приділити забезпеченню стійкості інформаційної та комунікаційної інфраструктури, яка є критично важливою складовою частиною стратегічної безпеки. Недостатність чітких критеріїв для визначення критичних об'єктів і відсутність розроблених планів оперативного реагування на надзвичайні ситуації значно ускладнюють ефективну протидію цим загрозам.

На основі проведеного аналізу запропоновано низку рекомендацій, спрямованих на вдосконалення політико-правових інструментів для забезпечення стійкості критичної інфраструктури. Насамперед необхідно розробити комплексну нормативно-правову базу, яка регламентуватиме діяльність усіх суб'єктів, залучених до захисту критичної інфраструктури, з чітким розмежуванням їхніх функцій і повноважень. Доцільним є впровадження дієвої методології ідентифікації та паспортизації об'єктів КІ з урахуванням світового досвіду, що забезпечить чіткість і системність у цій сфері.

Ключовим напрямом є забезпечення належного функціонування координаційного органу, відповідального за взаємодію між секторами критичної інфраструктури. Важливим є розроблення програм підготовки кадрів у сфері захисту КІ та підвищення їхньої кваліфікації відповідно до міжнародних стандартів. Не менш важливим є інтегрування комунікаційної інфраструктури до переліку об'єктів стратегічної безпеки з подальшим забезпеченням її належного захисту.

Отже, забезпечення стійкості критичної інфраструктури в Україні потребує системного підходу, який включає вдосконалення нормативно-правового регулювання, ефективну координацію між суб'єктами, підготовку кваліфікованих кадрів і впровадження сучасних

технологій для протидії загрозам. Реалізація наведених заходів сприятиме підвищенню рівня національної безпеки та сталого розвитку держави.

Рекомендації (Recommendations)

На сучасному етапі реформування національної системи захисту критичної інфраструктури першочерговим завданням є її подальша розбудова на основі наявних механізмів захисту та кризового реагування. Для досягнення мети необхідно впровадити комплексну "модель взаємодії і координації", яка стане фундаментом для інтеграції зусиль усіх зацікавлених сторін. Така модель має забезпечити ефективну комунікацію, організацію дій і розподіл відповідальності між органами виконавчої влади, реальним сектором економіки та громадськістю, орієнтуючись на єдиний підхід до формування й реалізації державної політики у сфері захисту критичної інфраструктури.

Необхідно забезпечити дієву взаємодію між різними суб'єктами національної безпеки. Така взаємодія передбачає не лише узгодження пріоритетів, а й розроблення конкретних механізмів координації, що сприятимуть спільній підготовці та реалізації стратегічних документів. Зокрема, слід звернути особливу увагу на гармонізацію дій щодо впровадження Стратегії національної безпеки України, Стратегії кібербезпеки України та Стратегії громадської безпеки та цивільного захисту України. Узгодженість зазначених документів із сучасними викликами має сприяти створенню умов для ефективної протидії загрозам, які ставлять під ризик об'єкти критичної інфраструктури.

Крім того, доцільним є створення спеціалізованих міжвідомчих платформ для обміну інформацією, оперативного реагування на кризи та попередження ризиків. Такі платформи мають функціонувати на основі сучасних інформаційних технологій, що забезпечать прозорість процесів та оперативність ухвалення рішень. Важливим аспектом є підвищення рівня взаємодії між державними установами і приватними підприємствами, які володіють або управляють об'єктами критичної інфраструктури. Така взаємодія потребує розроблення нормативно-правових механізмів, які стимулюватимуть співпрацю і створюватимуть сприятливі умови для спільного реагування на загрози.

Значну увагу слід приділити питанням, що стосуються підготовки кваліфікованих кадрів, здатних діяти у сфері захисту критичної інфраструктури, що включає як підвищення кваліфікації спеціалістів державного сектору, так і залучення експертів із приватного сектору та наукових кіл. Формування відповідних освітніх програм, тренінгів і симуляційних заходів сприятиме розвитку необхідних компетенцій та створенню професійної спільноти, здатної реагувати на сучасні виклики.

Необхідним складником є проведення регулярного оцінювання ефективності впроваджених заходів та оновлення підходів відповідно до змін у зовнішньому і внутрішньому середовищах. Такі заходи дозволять уникнути застою в розвитку системи захисту критичної інфраструктури та сприятимуть її адаптивності до нових умов. У цьому контексті слід активізувати міжнародну співпрацю, використовуючи досвід інших країн і запозичуючи найкращі практики.

Реалізація зазначених рекомендацій та пропозицій дозволить забезпечити комплексний підхід до захисту критичної інфраструктури у стратегіях сталого розвитку, підвищити рівень стійкості національної системи безпеки та сприятиме інтеграції політико-правових аспектів України в глобальну систему захисту стратегічної інфраструктури.

Подяки (Acknowledgements)

Автори заявляють, що у них немає конкуруючих інтересів за тематикою статті.

Використані джерела (References)

1. Clark, S. S., Seager, T. P., & Chester, M. V. (2018). A capabilities approach to the prioritization of critical infrastructure. *Environmental Systems and Decisions, 38*, 339–352.

https://doi.org/10.1007/s10669-018-9691-8
2. Fuso Nerini, F., Tomei, J., & To, L. S. (2018). Mapping synergies and trade-offs between energy and the Sustainable Development Goals. *Nature Energy, 3*, 10–15. https://doi.org/10.1038/s41560-017-0036-5
3. Зайцева, Л. О. (2019). Складові концепції сталого розвитку. *Ефективна економіка, 11*. https://doi.org/10.32702/2307-2105-2019.11.55
4. Страхніцький, Я. О. (2023). Особливості сучасної державної політики у сфері захисту критичної інфраструктури в умовах війни в Україні. In *Modernization of the system of public management and administration in Ukraine: the experience of the Republic of Latvia: Scientific monograph* (pp. 115–141). Riga, Latvia: Baltija Publishing. https://doi.org/10.30525/978-9934-26-279-1-5
5. Ліпкан, В. (2021). Безпека стратегічної інфраструктури та стратегічні комунікації в контексті реалізації геостратегії сучасної України. *Вісник Львівського університету. Серія: Філос.-політолог. студії, 38*, 205–216. https://doi.org/10.30970/PPS.2021.38.27
6. Зубко, Г. Ю. (2020). Система суб'єктів реалізації державної інфраструктурної політики України. *Правові новели, 11*, 166–178. https://doi.org/10.32847/ln.2020.11.22
7. Президент України. (2015, 26 травня). *Про стратегію національної безпеки і оборони України* (287/2015). Retrieved December 21, 2024, from https://www.president.gov.ua/documents/2872015-19070
8. Президент України. (2020, 14 вересня). *Про стратегію національної безпеки України* (392/2020). Retrieved December 21, 2024, from https://www.president.gov.ua/documents/3922020-35037
9. Закон України "*Про критичну інфраструктуру*" № 1882-IX (2021, 16 лист.) Retrieved December 21, 2024, from https://zakon.rada.gov.ua/laws/show/1882-20
10. Кабінет Міністрів України. (2017, 6 груд). *Концепція створення державної системи захисту критичної інфраструктури (1009-р./2017).* Retrieved December 21, 2024, from https://zakon.rada.gov.ua/laws/show/1009-2017-р
11. Ажажа, М., Пеліова, Я., & Несторенко, Т. (2023). Комунікативна політика держави в контексті посилення суспільного впливу. *Modeling the development of the economic systems, 2* (8), 79–88. https://doi.org/10.31891/mdes/2023-8-11
12. Кабінет Міністрів України. (2010, 13 січня). *Концепція проєкту Закону України "Про основні засади державної комунікативної політики" (85-р./2010).* Retrieved December 21, 2024, from https://zakon.rada.gov.ua/laws/show/85-2010-р
13. Кабінет Міністрів України. (2020, 9 жовт.). *Деякі питання об'єктів критичної інформаційної інфраструктури (943/2020).* Retrieved December 21, 2024, from https://zakon.rada.gov.ua/laws/show/943-2020-п
14. Правління НБУ. (2020, 30 лист.) *Про затвердження Положення про визначення об'єктів критичної інфраструктури в банківській системі України* (151/2020). Retrieved December 21, 2024, from https://bank.gov.ua/ua/legislation/Resolution_30112020_151
15. Арсенович, Л. А. (2024). Парадигма захисту критичної інфраструктури в системі національної безпеки України. *Державне управління: удосконалення та розвиток, 8*. http://doi.org/10.32702/2307-2156.2024.8.7
16. Бобро, Д. Г. (2016). *Удосконалення методології ранжування об'єктів критичної інфраструктури та їх віднесення до критичної інфраструктури: аналіт. записка*. Retrieved December 21, 2024, from http://www.niss.gov.ua/content/articles/files/krutuchna_infra-a7636.pdf
17. Бобро, Д. Г., Іванюта, С. П., Кондратов, С. І., & Суходоля, О. М. (2019). *Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури*

України: аналіт. доп. О. М. Суходоля (Ed.). НІСД. Retrieved December 21, 2024, from https://niss.gov.ua/sites/default/files/2019-05/Dopov_Suchodolya_print.pdf
18. Presidential Policy Directive 21 (PPD-21). (2013, Febr. 12). *Critical Infrastructure Security and Resilience*. Retrieved December 20, 2024, from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
19. *The Act of 26 April 2007 on Crisis Management*. Retrieved December 20, 2024, from https://rcb.gov.pl/wp-content/uploads/WERYF_-ACT_Crisis_Management_English-1.pdf

The Role of Infrastructure Security in Sustainable Development Strategies: Political and Legal Aspect

Halyna Kuspliak
PhD in Public Administration, Assistant Professor
Assistant Professor of the Department of Local Self-Government and Territorial Development
Institute of Public Service and Administration
Odesa Polytechnic National University
Odesa, Ukraine
e-mail: kusplyak.galina@gmail.com
ORCID: 0000-0002-1414-5484

Oksana Dulina
Ph.D. in Law, Assistant Professor
Assistant Professor of the Department of Public Administration and Regionalism
Institute of Public Service and Administration
Odesa Polytechnic National University
Odesa, Ukraine
e-mail: oksana_dulina@ukr.net
ORCID: 0000-0002-1009-558X

Kateryna Rovynska
PhD in Public Administration, Assistant Professor
Assistant Professor of the Department of State Studies, Law and European Integration
Institute of Public Service and Administration
Odesa Polytechnic National University
Odesa, Ukraine
e-mail: rovkateryna@gmail.com
ORCID: 0000-0002-1334-3112

Abstract. The relevance of the study is due to the growing threats and challenges facing Ukraine's critical infrastructure, in particular in the context of a full-scale war, cyberattacks, man-made disasters and natural disasters. Insufficient legal and regulatory development, fragmentation of state policy and limited coordination between critical infrastructure management entities pose risks to national security and sustainable development of the country.

The purpose of the study is to comprehensively analyse the current state of legal and regulatory framework for infrastructure security, identify the main threats and challenges affecting the functioning of critical infrastructure, and develop recommendations for improving the political and legal instruments to ensure its sustainability.

The research methods included an analysis of the current regulatory framework, a comparison of national and international experience in organising the protection of critical infrastructure, a systematic approach to identifying threats and risks, and the use of forecasting methods to develop recommendations.

The study results showed that Ukraine has a number of problems in the field of critical infrastructure protection, including the lack of a clear list of strategic infrastructure facilities, insufficient regulatory framework for communications infrastructure, and limited integration of modern methodologies and technologies into risk management processes. Global experience shows the need to create a comprehensive system of critical infrastructure protection based on clear coordination between public authorities, training of specialists and regular risk assessment. It is emphasised that in order to strengthen infrastructure security in Ukraine, it is necessary to create a clear legal framework regulating the protection of critical infrastructure; identify a coordinating body and develop a methodology for identifying critical facilities; integrate into the State policy the mechanisms of international cooperation, exchange of information and best practices; improve the training of specialists in the field of critical infrastructure protection; ensure clear regulation and coordination between the sectors of this infrastructure at the national level.

Keywords: national security, infrastructure security, critical infrastructure, sustainable development, concept of sustainable development, political and legal aspect, regulatory and legal support, global challenges.