DOI 10.34132/pard2024.23.02

Yaroslav Strahnitskyi

INSTITUTIONAL TRANSFORMATIONS IN THE DIRECTION OF INCREASING THE EFFECTIVENESS OF THE STATE POLICY OF CRITICAL INFRASTRUCTURE PROTECTION

The article analyzes modern features of state policy in the field of critical infrastructure protection. Attention is focused on the need for institutional transformations in the direction of improving efficiency, transparency, responsibility and responding to new security challenges in the conditions of a hybrid war with the Russian Federation.

The practice of protecting critical infrastructure facilities in developed countries has been studied. It was determined that its priority is the actualization of the predicate of stability of critical infrastructure objects. The content of normative and legal acts of Ukraine in this area was analyzed. A number of provisions have been identified that allow the adjustment of the domestic security doctrine to the European vector of stability.

Within the perspective of the development of the concept of sustainability, the intention of "critical infrastructure stakeholders" is substantiated. This opens up the prospects of creating transparent conditions for ensuring the annihilation of state institutions of power, state protection systems, the private sector, educational and scientific institutions and other stakeholders of critical infrastructure to the National System of Critical Infrastructure Protection at the next levels of management. The possible levels of such cooperation are determined.

Modern scientific works were analyzed, which studied the prospects of changing the paradigm of protection and stability to the paradigm of resilience. The complex of institutional transformations is proposed to be expanded due to the application within the framework of the functioning of the National Critical Infrastructure Protection System of the process of determining and analyzing the range of risks that the country faces in the spheres of critical infrastructure functioning. The transformation of institutional protection systems is considered through the prism of

systemic determinants, among which physical protection and defense, cyber protection and defense, preventive measures of protection and defense, and an educational and scientific approach are highlighted.

The system of organization at the state level of conducting regular interdisciplinary trainings on the operational response to emergency situations at facilities has been studied. It is proposed to increase clarity in the delineation of responsibility for project threats and to strengthen control over compliance with the systematicity of interdisciplinary training. On the basis of the extrapolations of scientists' hypotheses and the results of the author's research, a proposal was made to systematize the main proposals for institutional transformations in the direction of increasing the effectiveness of the state policy for the protection of critical infrastructure in the form of a Preventive concept of resilience of critical infrastructure objects.

Key words: *critical infrastructure, state policy, institutional transformations, sustainability, resilience.*

Постановка проблеми у загальному вигляді. Забезпечення життєво важливих функцій, які виконують об'єкти критичної інфраструктури є стратегічним завданням державної політики держави. Відповідна сфера інфраструктури має розглядатися як ключова сфера забезпечення національної безпеки, отже дестабілізацію інфраструктури слід сприймати як загрозу національній безпеці.

Війна в Україні мала значний вплив на безпекову ситуацію на критичних об'єктах, викликавши переоцінку вразливостей та стратегій їх захисту, як в Україні, так і за її межами. Починаючи 2014 р. влада рф почала застосовувати проти України тактику так званої «гібридної війни», що передбачає здійснення воєнних акцій без офіційного проголошення війни. Окрім цього, рф активно застосовує, окрім воєнних, ще й економічні, політичні, правові, релігійні, культурні та інформаційно-пропагандистські засоби [2]. У таких умовах роль держави передбачає впровадження єдиних методологічних прийомів оцінки проєктних та позапроєктних загроз критичній інфраструктурі та їх нейтралізації, а також розробку моделі

прогнозування потенційних загроз на національному рівні. Таким чином, формування системи державної політики у сфері безпеки критичної інфраструктури відбувається у формі комплексних державно-управлінських рішень, що передбачають систематичну адаптацію до динамічних змін мікро- та макросередовища на основі інституційно-правових трансформацій. Кінцевий результат даних трансформації є прикладом дихотомічного поєднання дій організаційного та правового механізмів публічного управління. Таким чином, важливість оновлення сучасної безпекової доктрини та забезпечення інституційних перетворень у напрямку своєчасності виявлення, відвернення і нейтралізації реальних і потенційних загроз для об'єктів критичної інфраструктури, актуалізують наукове завдання теоретичної розробки і наукового обґрунтування напрямів підвищення ефективності державної політики захисту критичної інфраструктури України в умовах гібридних загроз.

Аналіз останніх досліджень і публікацій. Серед наукових доробків вітчизняних учених, які присвячені проблемам захисту критичної інфраструктури в умовах надзвичайних ситуацій варто відзначити С. Азарова, В. Сидоренка, С. Єременка, А. Пруського, А. Демківа. Щодо перспектив удосконалення державної інфраструктурної політики України та напрямків інституційних трансформацій у цьому напрямку значний науковий внесок здійснили Г. Зубко, С. Кондратов, О. Суходоля. Один із магістральних векторів інституційної трансформації вітчизняної політики захисту критичної інфраструктури – концепції її резильєнтності розпочали досліджувати вітчизняні учені О. Резнікова, С. Пирожков, Є. Божок, Н. Хамітов, а також іноземні учені P. Trucco, E. Cagno, M. De Ambroggi, A. Fekete, J. Rhuner та ін..

Незважаючи на значну кількість наукових напрацювань у напрямку удосконалення державної політики захисту критичної інфраструктури та національної безпеки, недостатньо обґрунтованим у сучасних наукових доробках учених вважаємо вектор дослідження системи забезпечення стійкості критичної інфраструктури, зокрема створення транспарентних умов забезпечення анігіляції держаних інститутів влади, державних систем захисту, приватного сектору, освітньо-наукових установ та інших стейкхолдерів критичної

DOI: 10.34132/pard2024.23.02

інфраструктури. Особливої уваги також вимагає вивчення іноземного досвіду інституційних перетворень у секторі захисту критичної інфраструктури в умовах гібридних загроз.

Формулювання цілей статті (постановка завдання). Метою статті є теоретико-методологічне обґрунтування та розробка практичних рекомендацій щодо підвищення ефективності державної політики захисту критичної інфраструктури України в умовах гібридних загроз та забезпечення її стійкості.

Виклад основного матеріалу дослідження. Захист критичної інфраструктури є важливим аспектом національної безпеки і вимагає комплексного і багатовимірного підходу до питань інституційних трансформацій. Інституційні перетворення державної політики передбачають процес зміни політичних інститутів – правил, процедур, структур та організацій. Цей процес включає диференційовані варіанти законодавчих змін, реформування урядових агенцій, внесення змін у правову систему тощо. Інституційні перетворення в умовах гібридної війни з рф необхідні з метою покращення ефективності, прозорості, відповідальності та реагування на нові безпекові виклики. Гібридна війна, на переконання А. Г. Гольцова передбачає «використання воєнних і невоєнних інструментів в інтегрованій кампанії, спрямованій на досягнення раптовості, захоплення ініціативи та отримання психологічних переваг для використання в дипломатичних діях; масштабні і стрімкі інформаційні, електронні і кібернетичні операції; прикриття воєнних і розвідувальних дій у поєднанні з економічним тиском» [2]. Тобто, гібридна війна означає підкорення однією державою іншої за допомогою комбінованого впливу фізичних, ідеологічних, електронних, кібернетичних засобів у комбінації з бойовими діями та економічним тиском, що може доповнюватись також психологічним тиском на цивільне населення у вигляді позбавлення їх життєво-важливих послуг чи товарів. Останній пункт яскраво прослідковується у стратегії рф, що підтверджується цілеспрямованим руйнуванням об’єктів критичної інфраструктури, особливо енергетичної. Серед головних цілей мотивації ворога знищити критично важливу інфраструктуру учені розцінюють наступні:

1) послаблення соціальної стійкості серед українців шляхом спричинення або помноження гуманітарних криз , що також призведе до нових хвиль біженців або внутрішньо переміщених осіб;

2) збільшення матеріальних витрат України на ремонт та відновлення електропостачання;

3) збільшення потреби у зовнішній допомозі;

4) ускладнення умов для Збройних Сил України.

Практика захисту об'єктів критичної інфраструктури розвинених країн передбачає актуалізацію предикату стійкості критичної інфраструктури. У світлі глобалізаційних процесів у безпековому середовищі світу та євроінтеграційного курсу нашої держави, вважаємо дифузію даного феномену до вектору державної політики основоположним тригером у сфері посилення захищеності об'єктів критичної інфраструктури в Україні. Етимологічно дефініція «стійкість» походить від латинського «resilio, resilire», що означає «повернення» та «здатність до відновлення» [17]. Таким чином, можемо зробити висновок, що пріоритетними об'єктами для реалізації державної політики у напрямку забезпечення стійкості є пошкоджені, дестабілізовані або зруйновані об'єкти критичної інфраструктури. Стійкість критичної інфраструктури детермінує здатність операторів критичних об'єктів бути готовими та адаптивними до безпекових умов, що змінюються, а також швидко регенрувати порушену функціональну спроможність. При цьому, питанням забезпечення стійкості науковцями приділяється дедалі більше уваги у порівнянні з питаннями захисту [12]. Таке зміщення акценту проблематики обумовлене тим, «що в умовах війни, жодна створена система захисту не може у повній мірі забезпечити захист від усіх загроз і небезпек, що є особливо актуальним у сучасних умовах України» [5]. Дану тезу підтверджують і закордонні дослідники, наголошуючи, що колективне опікування національною стратегією оборони та безпеки є обов'язковою умовою стійкості нації.

Відповідно до пункту 23 частини першої статті 1 Закону України «Про критичну інфраструктуру» стійкість критичної інфраструктури – «стан критичної інфраструктури, за якого

DOI: 10.34132/pard2024.23.02

забезпечується її спроможність функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після впливу загроз будь-якого виду [4]. Також Закон встановлює, що «державна політика у сфері захисту критичної інфраструктури ґрунтується на засадах визнання необхідності забезпечення безпеки та стійкості критичної інфраструктури» [4]. Зазвичай аспект стійкості урегульовується низкою механізмів та інструментів забезпечення їх захисту, зокрема до них варто віднести плани захисту, плани міжсекторальної взаємодії залучених суб'єктів у процесі виконання завдань із захисту об'єктів. Аспект забезпечення захисту критичної інфраструктури слід вважати складовою частиною стратегічного кола завдань національної безпеки, а саме забезпечення стійкості в усьому ланцюжку життєзабезпечення населення. Питання стійкості у даному трактуванні детермінує виведення компетенції захисту таких критичних об'єктів за межі відповідальності лише їх операторів та вимагає розширення кола учасників. У даній пропозиції вважаємо доцільним інтегрувати у інституційно-правову систему захисту категорію «стейкхолдерів критичної інфраструктури».

Дефініцію «стейкхолдер» вперше обґрунтував у монографії «Стратегічне управління: роль зацікавлених сторін» (1984 р.), Р. Е. Фріман [12]. Ідея його «теорії управління стейкхолдерами» заснована на тому, що організація разом зі своїм зовнішнім і внутрішнім середовищем утворює поєднання зацікавлених сторін (стейкхолдерів). Учений довів, що більшість проблем організації можливо вирішити при грамотній взаємодії зі стейкхолдерами. Інтерпретуючи крізь призму концепції стійкості трактування Е. Фріманом сутності інтенції «стейкхолдер», можемо дійти висновку, що «стейкхолдери критичної інфраструктури» – це спектр зацікавлених результатами роботи окремих об'єктів критичної інфраструктури суб'єктів, які є складовою його внутрішнього або зовнішнього середовища і здійснюють свій внесок у поліпшення роботи та його захист, що сприяє підвищенню стійкості даних об'єктів.

Закон «Про критичну інфраструктуру» визначає низку конкретних завдань щодо забезпечення стійкості критичної інфраструктури. Наприклад, п. 4 ст.19 визначає, що секторальні органи вла-

ди розробляють та затверджують плани взаємодії та підтримання життєво важливих функцій на випадок порушення функціонування об'єктів критичної інфраструктури; ст. 20 «зобов'язує місцеві органи виконавчої влади до розробки та затвердження програм підвищення стійкості територіальних громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг чи для здійснення життєво важливих функцій, а також місцевих планів взаємодії залучених суб'єктів у кризовій ситуації з метою підтримання життєво важливих функцій та надання життєво важливих послуг; планів відновлення функціонування критичної інфраструктури» [4].

Такі плани забезпечення стійкості можна розглядати у якості формалізованої рамкової угоди між стейкхолдерами критичної інфраструктури, котрі залучаються до цього процесу та державою. Закон окреслює загальні горизонти інституційних змін, зокрема в межах визначеного терміну «стійкість критичної інфраструктури» наголошується на взаємодії залучених суб'єктів у межах Національної системи захисту критичної інфраструктури на наступних рівнях управління:

1) національний рівень – відповідальний Кабінет Міністрі України, уповноважений орган у сфері захисту критичної інфраструктури України, інститути державної та публічної влади, Національним банком України та іншими державними й центральними органами виконавчої влади;

2) регіональний та галузевий рівні – провадиться органами виконавчої влади центрального та місцевого рангу, котрі законом (в межах окремого сектору) наділені повноваженнями формування та реалізації заходів у сфері захисту об'єктів критичної інфраструктури та призначені підзвітними за функціонування окремих державних систем захисту та сил реагування;

3) локальний рівень – відповідають місцеві органи виконавчої влади (військово-цивільні адміністрації за умов їх створення), а також органи місцевого самоврядування;

4) об'єктовий рівень – реалізується оператором або власником об'єктів критичної інфраструктури на основі нормативних та регуляторних актів, діючих у сфері захисту критичної інфраструктури.

DOI: 10.34132/pard2024.23.02

Захист та стійкість критичної інфраструктури відповідно до визначених рівнів управління забезпечується квадро комплексом відповідних режимів її функціонування та захисту: звичного функціонування, превентивності , рефлексії та регенерації (рис. 1).

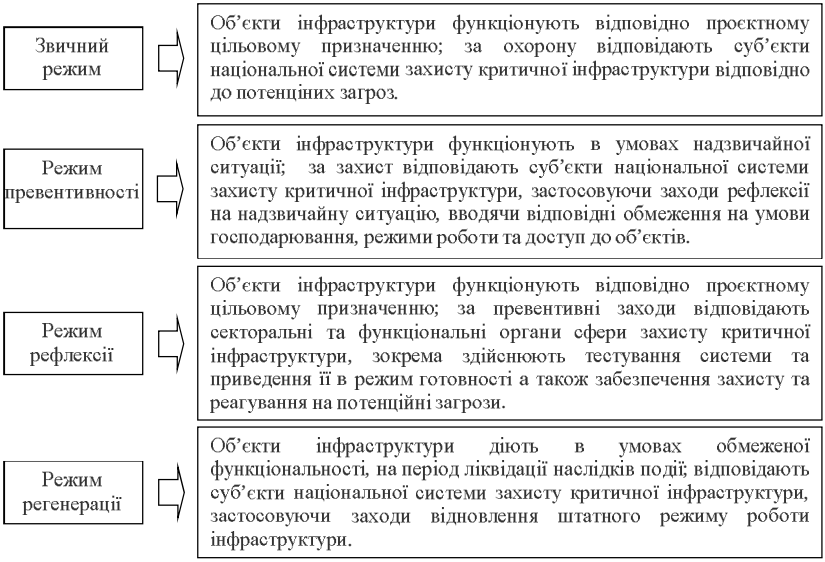

Рис. 1. Режими забезпечення захисту та стійкості критичної інфраструктури в Україні.

Джерело: узагальнено автором на основі [4]

Основоположним напрямком інституційних перетворень вважаємо слушними пропозиції вчених окрім відповідних міністерств, залучати до реалізації стратегії стійкості критичної інфраструктури інших учасників, без яких неможливо уявити врегулювання кризових ситуацій [1; 5]. Із цих слів, можемо зробити висновок, що на всіх рівнях формування та реалізації державної політики захисту критичної інфраструктури державні органи влади зобов'язані співпрацювати щодо аналізу ризиків та загроз із розширеним колом інститутів, відповідальних за вивчення, аналіз, пильнування, запобігання і захист під час кризових та надзвичайних ситуаціях на об'єктах критичної інфраструктури, а також розвивати практику евентуального дорадчого залучення стейкхолдерів.

Зазначимо, що кожний державний інститут або відомство, забезпечуючи розробку та реалізацію політики захисту критичної інфраструктури, має чітко визначити спектр потенційних загроз для підпорядкованих йому критичних об'єктів, оперуючи відповідним набором інструментів та ресурсів. Звернемось до досвіду США, де у National Infrastructure Protection Plan (NIPP) 2013 зазначається, що «національні зусилля щодо зміцнення безпеки та стійкості критичної інфраструктури залежать від здатності власників і операторів критичної інфраструктури державного та приватного секторів приймати рішення щодо найбільш ефективних доступних рішень з урахуванням ризиків при розподілі обмежених ресурсів у обох стабільних умовах – державні та кризові операції». Тобто, аналізуючи напрям інституційних перетворень державної політики США у сфері захисту критичної інфраструктури, відзначимо ключову особливість – її поліінституціональність. Даний феномен можемо пояснити активною участю у формуванні й реалізації державної політики та безпекових заходів у сфері захисту критичної інфраструктури приватного сектору, власників і операторів об'єктів, державних урядових установ, місцевого самоврядування, неурядових організацій, секторальних агентств, федеральних департаментів та наукових установ [18]. Метою даного тренду вважаємо посилення інноваційності у розробках безпечних і стійких технологій, а також ефективізацію та скоординованість програм на всіх рівнях управління, що допомагає зменшити ризики та загрози для критичної інфраструктури, а також збільшити кількість приватних інвестицій у даний сектор. Даний напрям інституційних перетворень також актуалізують умови сучасної глобальної геополітичної та безпекової політики, у яких продовжують розвиватися ризики та загрози, зростаючи у складності, виразності, масштабності та потенційності наслідків.

Варто звернути увагу на дослідження учених Мохори В.В., Коробейнікової Ф.О. [10], які акцентують увагу на досвіді країн ЄС, де на зміну парадигми захисту та стійкості приходить парадигма резильєнтності. На загальному рівні це також знаходить своє відображення в останніх директивах Ради ЄС, що визначають нові пріоритети в забезпеченні безпеки об'єктів критичної

DOI: 10.34132/pard2024.23.02

інфраструктури. Пирожков С. І., Хамітов Н. В., аналізуючи семантичний зміст терміну «резильєнтність» ототожнюють його із життєстійкістю та здатністю відновлюватися [8]. Науковці Кондратов С. І. та Суходоля О. М. трактують даний предикат як здатність протидіяти гібридним загрозам [7], тому у напрямку забезпечення захисту критичної інфраструктури з позиції сучасної міжнародної практики, вважаємо доцільним вживати саме термін «резильєнтність критичної інфраструктури». Предикат «резильєнтність критичної інфраструктури» можемо визначити як готовність і здатність країни, суспільства та органів державної влади забезпечити ефективний комплекс заходів, націлених на забезпечення готовності, запобігання, протистояння ризикам та загрозам надзвичайних ситуацій, швидкого відновлення нормального функціонування об'єктів від їх наслідків, а також постійного удосконалення компетентностей персоналу, засвоєння досвіду та залучення приватних інвестицій. Це питання стосується не тільки урядових органів, але й стейкхолдерів критичної інфраструктури загалом.

Ще одним із напрямків інституційних перетворень для забезпечення резильєнтності критичної інфраструктури з метою розвитку можливостей ефективно протистояти ризикам, варто розглянути перспективи проведення комплексного їх аналізу. Відзначимо, що ризик-аналіз в окремих країнах став важливим складником системи забезпечення національної безпеки та публікується у формі окремого документа – «Національної оцінки ризиків» (National Risk Assessment – NRA). Починаючи з першого десятиліття 2000-х років, уряди окремих країн, що входять до Організації економічного співробітництва та розвитку (OECD), почали розробляти портфельний аналіз «всіх небезпек», з якими стикається їхня національна безпека, які, врешті-решт, можуть призвести до масштабних надзвичайних ситуацій, у тому числі і на об'єктах критичної інфраструктури [19]. В межах інституційної трансформації в Україні вважаємо доцільним забезпечити процес визначення і аналізу спектру ризиків, з якими стикається країна у сферах функціонування критичної інфраструктури. Прикладом застосування такого інструменту є ризик-аналіз, який проводиться

у Великій Британії, де Уряд щорічно готує «Національну оцінку ризиків». В межах даної ініціативи забезпечується реалізація важливих елементів системи стійкості: прогнозування (готовність); формування реєстру ризиків (протистояння); оцінка ризиків (запобігання) [6]. Подібний підхід використовується й у США. Він базується на аналізі загроз (Threat), вразливостей (Vulnerability) та наслідків (Consequence). При цьому ризики критичній інфраструктурі оцінюються на основі експертних оцінок за п'ятибальною шкалою (інколи за трибальною) – від низького рівня до катастрофічного [16]. Важливим кроком у запровадженні подібної ініціативи став затверджений Постановою Кабінету Міністрів України 22 липня 2022 р. № 821 «Порядок проведення моніторингу рівня безпеки об'єктів критичної інфраструктури» [11], який визначає механізм проведення моніторингу із встановлення відповідності стану захищеності об'єкта критичної інфраструктури вимогам законодавства, достовірності наданої інформації визначеним суб'єктам національної системи захисту критичної інфраструктури, надання методичної допомоги операторам об'єктів критичної інфраструктури в удосконаленні системи захисту критичної інфраструктури. Порядок містить чіткий алгоритм дій: здійснюється раз на три роки секторальними та функціональними органами; оцінка стану захищеності враховує специфіку функціонування об'єкта; за результатом моніторингу складається акт, де вказують одну з трьох оцінок забезпечення захищеності: «забезпечує», «обмежено забезпечує», «не забезпечує»; обов'язково надаються пропозиції про вдосконалення системи захисту об'єкта; оператор критичної інфраструктури отримує акт перевірки і зобов'язаний вжити заходів щодо усунення виявлених порушень. Таким чином, це дає можливість відповідним державним органам постійно моніторити стан критичної інфраструктури та мати у розпорядженні необхідні механізми впливу задля забезпечення безперебійної роботи [11].

Актуальним заходом державної політики у сфері захисту критичної інфраструктури в умовах воєнного стану сьогодні вважаємо Постанову Кабінету Міністрів України «Деякі питання паспортизації об'єктів критичної інфраструктури» № 818 від 04.08.2023 р., якою затверджено «Порядок розроблення та

DOI: 10.34132/pard2024.23.02

погодження паспорта безпеки на об'єкт критичної інфраструктури». Паспорт безпеки став одним із ключових інституцій у сфері забезпечення резильєнтності критичної інфраструктури, яким регламентуються заходи, що вживатимуться у разі виникнення загроз для функціонування інфраструктури. Дана ініціатива забезпечить раннє попередження осіб, що приймають управлінські рішення, про нові потенційні загрози та ризики, з метою їх об'єктивної та всебічної оцінки, підготовлення та здійснення відповідного рішення та реагування. Тобто розробка паспорта для об'єкту критичної інфраструктури надасть можливість переорієнтувати існуючі можливості цільового моніторингу у необхідне русло в межах функціонування системи раннього виявлення та попередження загроз критичним об'єктам.

Виходячи із описаних вище ключових атрибутів резильєнтності об'єктів критичних інфраструктур, трансформування інституційних систем їх захисту варто розглядати крізь призму ресурсних системних детермінант, серед яких можемо виділити фізичний захист і оборону, кіберзахист і оборону, превентивні заходи захисту й оборони та освітньо-науковий підхід (рис.2).

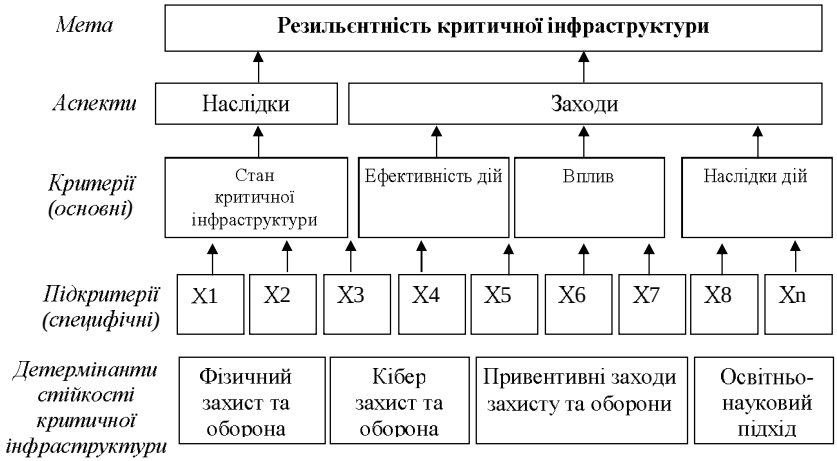

Рис. 2. Структурно-логічна схема забезпечення стійкості критичної інфраструктури в межах реалізації державої політики.

Джерело: розроблено автором

Структурно-логічну схему забезпечення резильєнтності критичної інфраструктури в межах реалізації державної політики варто деталізувати у наступних етапах:

1. Етап оцінки можливих подій: передбачає аналіз ризиків і загроз (дії із посилення готовності).

2. Етап перед подією: триває від моменту виникнення загрози до початку надзвичайної ситуації – деструкції (дії із передбачення, підготовки та запобігання).

3. Етап протягом події: триває від початку деструкції до максимального її впливу на об'єкт критичної інфраструктури (дії із проходження події, забезпечення витримки та протистояння).

4. Етап після події: триває від максимального погіршення функціональності об'єкта до її повного або часткового повернення (дії з реагування на подію та відновлення)

5. Етап підготовки до наступної події: триває від моменту повного або часткового повернення функціональності об'єкта критичної інфраструктури до виникнення наступної надзвичайної ситуації (дії з адаптації та навчання). Цей етап підкреслює здатність вчитися та вдосконалюватися на основі набутого досвіду.

Ефективний захист критичної інфраструктури в Україні у світлі запропонованих концептуальних сценаріїв в умовах надзвичайних ситуацій та терористичних актів неможливий без реалізації суб'єктами у сфері формування та реалізації державної політики їх специфічних функцій які повинні реалізовуватися державними управлінськими інститутами. Опираючись на проведений аналіз даного вектору у попередніх розділах роботи, погодимось із вченими Кондратовим С. І. та Суходолею О. М. [5], які вбачають проблему у тому, що відповідальність за безпеку критичних об'єктів інфраструктури покладено на різні міністерства і відомства, які забезпечують функціонування відповідних систем. При цьому кожна система має «власні» набори загроз та ризиків, якими вона опікується, «власні» режими функціонування у різних безпекових умовах, «власні» плани і процедури реагування, викладені із застосуванням відомчої термінології і понятійного апарату. До того ж, «визначені у положеннях і планах механізми і процедури взаємодії між існуючими національними системами безпеки і

DOI: 10.34132/pard2024.23.02

кризового реагування здебільшого є недостатньо відпрацьованими та апробованими для випадків масштабних кризових ситуацій, оскільки в країні до цього часу практика міжвідомчих навчань і тренувань на рівнях, вищих ніж об'єктовий, була розвинута слабко» [13]. Отже, дана проблема потребує адекватної відповіді у вигляді управлінського рішення по створенню певних міжсекторальних осередків захисту, які б опікувалися безпекою конкретних об'єктів критичної інфраструктури. Для цього важливо регламентувати градацію розподілу відповідальності за типами проєктних загроз

В межах інституційних перетворень у напрямку посилення резильєнтності критичної інфраструктури на основі розмежування відповідальності за проєктні загрози, вважаємо за доцільне, посилити на державному рівні активність у забезпеченні проведення регулярних міжсекторальних навчань із оперативного реагування на надзвичайні ситуації на об'єктах з метою підвищення рівня міжвідомчої взаємодії для попередження загроз. Такі заходи доречно проводити спільними зусиллями із об'єднанням представників державних систем захисту та реагування обов'язковим залученням представників Служби Безпеки України, Міністерства внутрішніх справ, Антитерористичного Центру, Державної інспекції ядерного регулювання України, Держслужби з надзвичайних ситуацій, Державної прикордонної служби, Збройних Сил України, Національної гвардії, Департаментів цивільного захисту, а також органів виконавчої влади та місцевого самоврядування і власників (операторів) об'єктів критичної інфраструктури. Такий механізм у складі державної політики варто розглядати у якості складової превентивного комплексу заходів сфери захисту об'єктів критичної інфраструктури в умовах воєнного стану в Україні.

Дану пропозицію підтримує Зубко Г. І. [3], пропонуючи деталізацію описаного навчального сценарію та включити до нього:

– диференціацію навчальних заходів, інструментів та інформації за основними модулями: універсальним (базові знання для усіх секторів критичної інфраструктури), спеціальним (профільне навчання для кожного сектора або об'єкта) та цифровізованого;

– загальний модуль необхідно наповнити курсами націленими на навчання громадськості, суспільства та відповідних стейкхолдерів

з метою підвищення рівня їх компетентностей із основних питань цивільного захисту та превентивних дій стосовно загроз та ризиків критичній інфраструктурі загального характеру;

– спеціальний модуль для кожного сегменту критичної інфраструктури направлено на структурування навчальних заходів із підвищення кваліфікації основних суб'єктів процесу захисту критичної інфраструктури, відповідних державних службовців, секторальних та функціональних органів, власників та операторів критичної інфраструктури;

– модуль цифровізованого навчання, передбачає формування компетенцій у суб'єктів захисту критичної інфраструктури у кіберпросторі на основі посилення ролі ІТ-технологій та штучного інтелекту для забезпечення резильєнтності критичної інфраструктури.

Одними із організаційних заходів, у межах зазначеної ініціативи, спрямованих на захист і забезпечення превентивних заходів з метою посилення резильєнтності критичної інфраструктури, є періодичний скринінг готовності сил реагування та операторів до протидії кризовій ситуації, що здійснюються під час проведення різного роду навчань та тренінгів. При цьому у вітчизняній практиці варто розрізняти різні види даних заходів, зокрема:

– орієнтовані на здобуття й закріплення теоретичних знань

– націлені на здобуття та закріплення практичних навичок, а також відпрацювання сценаріїв злагодженості дій у імітованій ситуації.

Варто акцентувати увагу, що в Україні здійснення навчальних заходів передбачено в межах підвищення кваліфікації окремих державних системи захисту та реагування, наприклад у ст. 92 Кодексу цивільного захисту регламентовано підготовку до дій за призначенням органів управління цивільного захисту, що здійснюється під час проведення командно-штабних та інших навчань і тренувань. Найбільш детально методичні аспекти підготовки та проведення навчань висвітлені у п.4 «Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків», де регламентовано співпрацю у вигляді спільних тактико-спеціальних та командно-штабних тренувань і

DOI: 10.34132/pard2024.23.02

навчань зі спільного використання суб'єктами сил і засобів в умовах боротьби з тероризмом. Відповідно до Закону України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» (ст. 16, 17, 22) у рамках Державного плану взаємодії центральних та місцевих органів виконавчої влади на випадок вчинення диверсій передбачені тренування, підготовка та перепідготовка персоналу. У Законі «Про критичну інфраструктуру (ст.19) згадується, що до компетенції секторальних органів у сфері захисту критичної інфраструктури включено «організацію системи підготовки персоналу, навчання та тренувань щодо забезпечення стійкості та захисту секторів критичної інфраструктури». Окрім цього, Закон регламентує процес розробки та затвердження місцевими органами виконавчої влади та військово-цивільними адміністраціями програм навчання населення у напрямку забезпечення посилення захисту в умовах виникнення кризової ситуації та введення режиму реагування та відновлення функціональності об'єктів критичної інфраструктури. Оператори об'єктів критичної інфраструктури також «зобов'язані проводити навчання та тренінги для підготовки та перевірки персоналу, який відповідає за охорону, безпеку та захист об'єктів критичної інфраструктури» [4].

У ст.22 Закону передбачено. що на секторальному (галузевому) та регіональному рівнях органи державної влади розробляють і затверджують галузеві, регіональні плани та програми з протидії загрозам критичній інфраструктурі, включаючи аварійні плани, плани реагування на кризові ситуації, плани взаємодії, плани відновлення об'єктів критичної інфраструктури, плани проведення навчань та тренувань. З метою організації взаємодії між суб'єктами національної системи захисту критичної інфраструктури передбачено проведення спільних командно-штабних, тактико-спеціальних навчань, спільних тренувань та занять із захисту, охорони, оборони, припинення злочинних дій, інцидентів та кібератак проти об'єктів критичної інформаційної інфраструктури (п.3 ст.24). Також у ст. 31 передбачено, що Україна, відповідно до міжнародних договорів, може брати участь у спільних заходах із забезпечення захисту критичної інфраструктури, зокрема у проведенні спільних навчань суб'єктів

сектору безпеки і оборони в рамках заходів колективної оборони [4]. Отже, із проаналізованих нормативних положень, можемо зробити висновок, що система регламентування процесу навчань та тренувань сил реагування на надзвичайні ситуації у секторі критичної інфраструктури має комплексний характер, проте відсутній механізм контролю за дотриманням системності даного процесу.

Опираючись на теорії сучасних публікацій з державного управління, щодо складних соціально-економічних систем, можна стверджувати, що напрям посилення резильєнтності критичної інфраструктури варто розглядати з двох базових позицій:

– як стан захищеності макросистеми від внутрішніх та зовнішніх загроз або ризиків;

– як сукупність елементів (адміністративних, технічних, інформаційних і т.д.), які задіяні для подальшого підтримання стану захищеності на рівні мікросистеми [21; 22].

Ґрунтуючись на результатах проведених досліджень, сфокусуємо увагу на застарілості безпекової парадигми, котра орієнтована здебільшого на урахуванні внутрішніх детермінант порушення безпеки критичної інфраструктури. При цьому переважна більшість науковців залишають поза увагою важливий сегмент державної політики, що лежить у площині стійкості і забезпечення комплексності інституційної складової розбудови макросистеми захисту критичної інфраструктури. Визначальним стрижнем інституційної трансформації державної політики захисту у цьому напрямку варто розглядати новітні ризики та загрози, які породжені вторгненням військ рф, адже саме вони на сьогодні чинять найбільш суттєвий та відчутний вплив на систему захисту критичної інфраструктури України. Вважаємо доцільним ключові постулати інституційних трансформацій на основі результатів оцінки ризиків та загроз скомпонувати у формі Превентивної концепції резильєнтності об’єктів критичної інфраструктури. Дану пропозицію підтримує і О. М. Суходоля, відзначаючи, що забезпечення стійкості потребує уваги чинної системи кризового управління в країні, формування заходів реагування, виділення ресурсів, проведення моніторингу за досягненням цієї цілі. Учений також наголошує на необхідності запровадження Концепції резильєнтно-

DOI: 10.34132/pard2024.23.02

сті, спрямованої на побудову спроможностей реагування на випередження, а не на ліквідацію наслідків основаної на теорії кризового реагування [14]. Також вчений підкреслює необхідність методологічного поєднання зусиль різних державних систем захисту та реагування на кризові ситуації у різних секторах критичної інфраструктури, що забезпечують існування суспільства та держави [15]. Екстраполюючи гіпотези учених, висловимо пропозицію щодо основних положень Превентивної концепції резильєнтності об'єктів критичної інфраструктури:

1. Встановлення відповідальності за порушення, що призвели до погіршення безпеки критичної інфраструктури, як засобу адміністративно-правового забезпечення такої безпеки та визначення механізмів притягнення до відповідальності.

2. Законодавче врегулювати питання щодо проведення комплексної національної оцінки ризиків і загроз у сфері безпеки критичної інфраструктури.

3. Сформувати Національний реєстр загроз критичній інфраструктурі та визначити інститут державної влади, який забезпечуватиме його формування та ведення.

4. Сформувати єдину нормативно-правову базу у сфері планування та реагування на кризові ситуації та загрози для скоординованих дій державних органів.

5. Створити двосторонні канали комунікацій органів державної і місцевої влади з населенням утворити постійно діючі механізми взаємодії органів державної і місцевої влади, неурядових організацій, приватного бізнесу та міжнародних партнерів з питань забезпечення національної стійкості.

6. Загальну схему розподілу відповідальності та повноваження органів державної влади за визначеними напрямами забезпечення національної стійкості.

7. Формування національної мережі наукових установ з питань стратегічного аналізу.

8. Розробка діючих механізмів взаємодії органів державної та місцевої влади, неурядових організацій, приватного бізнесу та міжнародних партнерів з питань забезпечення резильєнтності критичної інфраструктури.

9. Обов'язковість проведення періодичних міжвідомчих навчань і тренувань за участю населення з метою підвищення рівня обізнаності та готовності до реагування на широкий спектр загроз, удосконалення кризового менеджменту, стійкість громад, економічна стійкість, суспільна стійкість [9].

У сучасному суспільстві система інфраструктури та її компоненти не існують ізольовано, а функціональні або фізичні зв'язки між ними є динамічними та складними. Через взаємозалежність всередині інфраструктури або між інфраструктурами збій у будь-якій частині системи вплине на інші частини або навіть пошириться та спричинить порушення в інших інфраструктурах через функціональне чи фізичне підключення [20]. Таким чином, небезпека або збій можуть призвести до непередбачуваних каскадних наслідків. Це також стосується і наднаціональних загроз та ризиків, до детермінує посилення міжнародного співробітництва. Співробітництво України з ЄС у напрямку посилення захисту об'єктів критичної інфраструктури повинно сфокусуватись у напрямках

Висновки. Отже, на сучасному етапі удосконалення державної політики у сфері захисту критичної інфраструктури варто сфокусувати інституційні перетворення у точці забезпечення її резильєнтності на основі існуючих національних систем захисту, безпеки та кризового реагування за умов досягнення якісно нового рівня координації дій та взаємодії між ними. Вкрай важливим питанням є врегулювання публічно-приватної взаємодії у межах Національної системи захисту критичної інфраструктури диференційовано за відповідними сферами. При чому із обов'язковим залученням представників СБУ, Збройних Сил України, Державної прикордонної служби, Національної гвардії, Держслужби з надзвичайних ситуацій, Національної поліції, а також Департаментів цивільного захисту, представників органів виконавчої влади та місцевого самоврядування і операторів об'єктів критичної інфраструктури. Одними із організаційних заходів, у межах зазначеної ініціативи, є періодичний скринінг готовності сил реагування та операторів до протидії кризовій ситуації, що здійснюються під час проведення різного роду навчань та тренінгів. Дану пропозицію можна віднести до категорії превентивних та антикризових заходів державного управління у сфері захисту

DOI: 10.34132/pard2024.23.02

найважливіших об'єктів критичної інфраструктури. Виходячи із описаних вище ключових атрибутів резильєнтності об'єктів критичних інфраструктур, трансформування інституційних систем їх захисту варто розглядати крізь призму ресурсних системних детермінант, серед яких можемо виділити фізичний захист і оборону, кіберзахист і оборону, превентивні заходи захисту й оборони та освітньо-науковий підхід Екстраполюючи гіпотези учених та результати авторських досліджень висловлено пропозицію узагальнити основні пропозиції у формі Превентивної концепції резильєнтності об'єктів критичної інфраструктури.

Стаття надійшла до редакції: 20.09.2023

ІНСТИТУЦІЙНІ ПЕРЕТВОРЕННЯ У НАПРЯМКУ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У статті аналізуються сучасні особливості державної політики у сфері захисту критичної інфраструктури. Акцентовано увагу на необхідності інституційних перетворень у напрямку покращення ефективності, прозорості, відповідальності та реагування на нові безпекові виклики в умовах гібридної війни з рф.

Вивчено практику захисту об'єктів критичної інфраструктури розвинених країн та визначено, що її пріоритетом є актуалізація предикату стійкості об'єктів критичної інфраструктури. Проаналізовано зміст нормативно-правових актів України у даній сфері та визначено ряд положень, які допускають перелаштування вітчизняної безпекової доктрини на європейський вектор стійкості. Обґрунтовано інтенцію «стейкхолдери критичної інфраструктури», що відкриває перспективи розширення Національної системи захисту критичної інфраструктури.

Проаналізовано сучасні наукові праці, у яких вивчено перспективи зміни парадигми захисту та стійкості на парадигму резильєнтності, як здатності протидіяти гібридним загрозам. Трансформування інституційних систем захисту розглянуто крізь призму системних детермінант, серед яких виділено фізичний

захист і оборону, кіберзахист і оборону, превентивні заходи захисту й оборони та освітньо-науковий підхід.

На основі екстраполяцій гіпотез учених та результатів авторських досліджень висловлено пропозицію щодо систематизації основних пропозицій інституційних трансформацій у напрямку підвищення ефективності державної політики захисту критичної інфраструктури у формі Превентивної концепції резильєнтності об'єктів критичної інфраструктури.

Ключові слова: *критична інфраструктура, державна політика, інституційні перетворення, стійкість, резильєнтність.*

Received: 20.09.2023

References

1. Azarov, S.I., Sydorenko, V.L., Yeremenko, S.A., Pruskyi, A.V. & Demkiv, A.M. (2021). *Zakhyst krytychnoi infrastruktury v umovakh nadzvychainykh sytuatsii [Protection of critical infrastructure in emergency situations]*. Kyiv [in Ukrainian].

2. Holtsov, A.H. (2023). Heostratehiia Ukrainy shchodo Rosiiskoi Federatsii [Geostrategy of Ukraine in relation to the Russian Federation]. *Visnyk NTUU «KPI». Politolohiia. Sotsiolohiia. Pravo – National Technical University of Ukraine Journal. Political science. Sociology. Law,* 1 (57), (pp. 71-77) [in Ukrainian].

3. Zubko, H.Yu. (2020). *Derzhavna infrastrukturna polityka Ukrainy: administratyvno-pravovi zasady rehuliuvannia [State infrastructure policy of Ukraine: administrative and legal principles of regulation].* Kherson: Vydavnychyi dim «Helvetyka» [in Ukrainian].

4. Zakon Ukrainy Pro krytychnu infrastrukturu: pryiniatyi 16 list 2021 roku No. 1882-IX [Law of Ukraine On Critical Infrastructure from 16 November 2021, No. 1882-IX]. (n.d.). *zakon.rada.gov.ua.* Retrieved from: https://zakon.rada.gov.ua/laws/show/1882-20 [in Ukrainian].

5. Kondratov, S.I., & Sukhodolia, O.M. (2020). *Derzhavna systema zakhystu krytychnoi infrastruktury v systemi zabezpechennia natsionalnoi bezpeky [State system of protection of critical infrastructure in the system of ensuring national security]*. Kyiv: NISD [in Ukrainian].

6. Sait Uriadu Velykobrytanii [Site of UK Government]. *www.gov.uk.* Retrieved from https://www.gov.uk [in Ukrainian].

 DOI: 10.34132/pard2024.23.02

7. Pyrozhkov, S.I., Bozhok, Ye.V. & Khamitov, N.V. (2021). Natsionalna stiikist (rezylientnist) krainy: stratehiia i taktyka vyperedzhennia hibrydnykh zahroz [National stability (resilience) of the country: strategy and tactics of anticipating hybrid threats]. *Visnyk Natsionalnoi akademii nauk Ukrainy – Visnyk of the National Academy of Sciences of Ukraine,* 8, (pp. 74-82) [in Ukrainian].

8. Pyrozhkov, S.I. & Khamitov, N.V. (2016). Tsyvilizatsiinyi proekt Ukrainy: vid ambitsii do realnykh mozhlyvostei [Civilization project of Ukraine: from ambitions to real possibilities]. *Visnyk Natsionalnoi akademii nauk Ukrainy – Visnyk of the National Academy of Sciences of Ukraine,* 6, (pp. 45-52) [in Ukrainian].

9. Postanova KMU Poriadok provedennia monitorynhu rivnia bezpeky obiektiv krytychnoi infrastruktury pryiniata 22 sich 2022 roku. No. 821 [Resolution of the CMU Procedure for monitoring the security level of critical infrastructure objects from 22 January No. 821]. (n.d.). *zakon.rada.gov.ua.* Retrieved from: https://zakon.rada.gov.ua/laws/show/821-2022-p#Text [in Ukrainian].

10. Reznikova, O.O. (2022). *Natsionalna stiikist v umovakh minlyvoho bezpekovoho seredovyshcha [National stability in the conditions of a changing security environment]*. Kyiv: NISD [in Ukrainian].

11. Mokhor, V.V., & Korobeinikov, F.O. (2023). Vtilennia paradyhmy rezylientnosti v zabezpechennia funktsionuvannia krytychnoi infrastruktury YeS [Implementation of the paradigm of resilience in ensuring the functioning of the critical infrastructure of the EU]. *Rezylientnist krytychnoi infrastruktury – 2023: zbirnyk materialiv naukovo-praktychnoi konferentsii – Critical Infrastructure Resilience – 2023: collection of materials of the scientific and practical conference,* (pp. 48-52). Kyiv: PIMEE of NAS of Ukraine [in Ukrainian].

12. Strakhnitskyi, Ya.O. (2022). Osoblyvosti derzhavnoi polityky zakhystu krytychnoi infrastruktury v Ukraini ta napriamy yii udoskonalennia v umovakh viiny [Peculiarities of the state policy of critical infrastructure protection in Ukraine and directions for its improvement in wartime conditions]. *Knowledge, Education, Law, Management,* 7 (51), (pp. 104-111) [in Ukrainian].

13. Strakhnitskyi, Ya.O. (2022). Strukturno-funktsionalna kharakterystyka derzhavnoi polityky u sferi zakhystu krytychnoi infrastruktury v Ukraini [Structural and functional characteristics of state policy in the sphere of critical infrastructure protection in Ukraine]. *Publichne upravlinnia ta mytne administruvannia – Public administration and customs administration,* 4 (35), (pp. 112-117) [in Ukrainian].

14. Sukhodolia, O.M. (2018). Stiikist enerhetychnoi systemy chy stiikist enerhozabezpechennia spozhyvachiv: postanovka problem [Sustainability of

the energy system or sustainability of energy supply to consumers: problem statement]. *Stratehichni priorytety – Strategic priorities*, 2, (pp. 101-117) [in Ukrainian].

15. Suhodolya, O.M. (2023). *Nova Dyrektyva YeS shchodo stiikosti krytychnoi infrastruktury (CER Directive) [The new EU Directive on the sustainability of critical infrastructure (CER Directive)]*. Kyiv: NISD. Retrieved from https://niss.gov.ua/sites/default/files/2023-04/az_eu-cer_12042023.pdf [in Ukrainian].

16. Sait Electricity Information Sharing and Analysis Center [Site of Electricity Information Sharing and Analysis Center]. *www.eisac.com.* Retrieved from: https://www.eisac.com/ [in English].

17. Josse, E., Dubois, V. (2009). *Interventions humanitaires en santé mentale dans les violences de masse*, (1st edition). Bruxelles: Groupe De Boeck, 301 [in English].

18. National Infrastructure Protection Plan – NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. (n.d.). *www.cisa.gov.* Retrieved from https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf [in English].

19. National Risk Assessments: A Cross Country Perspective The evolving practice of National Risk Assessments in OECD countries. (n.d.). *read.oecd-ilibrary.org.* Retrieved from https://read.oecd-ilibrary.org/governance/national-risk-assessments/the-evolving-practice-of-national-risk-assessments-in-oecd-countries_9789264287532-3-en#page1 [in English].

20. Trucco, P., Cagno, E., & Ambroggi, M.De. (2012). Dynamic functionalmodelling of vulnerability and interoperability of Critical Infrastructures. *Reliability Engineering and System Safety*, 105, (pp. 51-63) [in English].

21. Williamson, R.D., & Morris, J.C. (2021). Lessons from the COVID-19 Pandemic for Federalism and Infrastructure: A Call to Action. *Public Works Management and Policy*, 5, (pp. 6-12) [in English].

22. Fekete, A., Rhuner, J. (2020). Sustainable Digital Transformation of Disaster Risk-Integrating New Types of Digital Social Vulnerability and Interdependencies with Critical Infrastructure. *Sustainability*, 12(22), (pp. 1-18) [in English].

DOI: 10.34132/pard2024.23.02

Відомості про авторів / Information about the Authors

Ярослав Страхніцький, аспірант кафедри публічного управління та адміністрування Вінницького державного педагогічного університету імені Михайла Коцюбинського, м. Вінниця, Україна. E-mail: strahnitskiy@gmail.com, orcid: https://orcid.org/0000-0002-3066-0961

Yaroslav Strahnitskyi, PhD-student of the Department of Public Manage-ment and Administration of Mykhailo Kotsyubynskyi State Pedagogical University of Vinnytsia, Vinnytsia, Ukraine. E-mail: strahnitskiy@gmail.com, orcid: https://orcid.org/0000-0002-3066-0961

Strahnitskyi, Y. (2024). Institutional transformations in the direction of increasing the effectiveness of the state policy of critical infrastructure protection. Public Administration and Regional Development, 23, 28-51. https://doi.org/10.34132/pard2024.23.02