МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІННИЦЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ МИХАЙЛА КОЦЮБИНСЬКОГО

Кваліфікаційна наукова
праця на правах рукопису

СТРАХНІЦЬКИЙ ЯРОСЛАВ ОЛЕКСАНДРОВИЧ

УДК 351.862.2: [351.778+351.824.11] (477) (043.5)

ДИСЕРТАЦІЯ
ОСОБЛИВОСТІ ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

281 – публічне управління та адміністрування

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Я. О. Страхніцький

Науковий керівник: Яременко Олександр Іванович, кандидат наук з державного управління, доцент

Вінниця – 2024

АНОТАЦІЯ

Страхніцький Я.О. **Особливості формування та реалізації державної політики у сфері захисту критичної інфраструктури.** – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 281 – Публічне управління та адміністрування. – Вінницький державний педагогічний університет імені Михайла Коцюбинського, Вінниця, 2024.

У дисертаційній роботі запропоновано вирішення авантажної наукової квестії сфокусованої на узагальненні теоретико-методологічних особливостей сучасної державної політики у сфері захисту критичної інфраструктури та теоретичного обґрунтування доктринальних поглядів у фокусі вдосконалення механізмів державного управління забезпеченням безпеки об’єктів критичної інфраструктури та генерування відповідних науково-практичних рекомендацій.

Проведено аналіз теоретичних підходів до сутності критичної інфраструктури як об’єкту державного управління та описано спектр ключових атрибутів сучасного безпекового середовища, що закладють фундамент цілепокладання державної політики у сфері її захисту. Визначено поняття та ознаки державної політики у сфері захисту критичної інфраструктури. Обґрунтовано горизонт опису критичної інфраструктури у якості складової національної безпеки України, та зафіксовано приналежність її об’єктів до національної інфраструктури.

Здійснено аналітико-бібліографічний огляд наукових праць вітчизняних учених, а також іноземних наукових доробків присвячених питанням обгрунтування дефініції «критична інфраструктура», що дало підстави генерувати авторське бачення змістовного наповнення даного терміну. Авторська інтерпретація підкреслює приналежність об’єктів критичної інфраструктури до сфери національної безпеки, що інспірує пріоритетність відповідальності за її збереження саме за державною безпековою політикою,

а також фіксує пріоритетність тріади людина-суспільство-держава, що забезпечить удосконалення державної політики у даному сегменті відповідно до антропоцентричного підходу та концепції сталого розвитку.

Сформовано категорійно-понятійну систему дослідження теоретико-методичних засад забезпечення захисту критичної інфраструктури. Сформульовано авторське формулювання дефініції «захист критичної інфраструктури» як цілеспрямованої синхронізованої спільної діяльності державних інститутів, власників, операторів а також стейкхолдерів об'єктів критичної інфраструктури із застосування комплексу заходів, спрямованих на профілактику, запобігання, своєчасне виявлення потенційних і нейтралізацію реальних загроз, мінімізацію та ліквідацію наслідків і швидке відновлення функціональної спроможності критичної інфраструктури у разі її пошкодження, що реалізовуються з метою уникнення людських жертв, значних матеріальних та екологічних збитків, або інших деструктивних наслідків які можуть призвести до порушення національної безпеки. Даним тлумаченням змінено кут уваги із процесу захисту критичної інфраструктури до превенції кризових ситуацій, диференціювавши відповідальність між державою, власниками, безпосередніми працівниками критичних об'єктів, а також обґрунтовано інтенцію «стейкхолдери об'єктів критичної інфраструктури» та актуалізовано їх роль у сфері захисту.

Проаналізовано сучасні наукові парадигми формування державної політики у сфері захисту критичної інфраструктури з метою наукового переосмислення поглядів на процес формування архітектури ключових постулатів державної політики та чіткої артикуляції ролі держави у сфері захисту критичної інфраструктури. Науково обґрунтовано, що в основу інституційного цілепокладання заходів державної політики у сфері захисту критичної інфраструктури варто закласти парадигму національного безпекознавства, яка несе у собі еклектичний вимір безпекової трансдисциплінарної парадигми.

З'ясовано інституційно-правові особливості здійснення державної

політики у сфері захисту критичної інфраструктури. Екстрапольовано трактування інституційно-правового регулювання реалізації державної політики у сфері захисту критичної інфраструктури як систему організаційно-управлінських і правових заходів, що реалізовують інститути державної влади, за допомогою яких реалізується. цілеспрямований адміністративний вплив на суспільні відносини орієнтовані на запобігання диференційованим ризикам, загрозам і небезпекам об'єктам критичної інфраструктури основані на тріаді людина-суспільство-держава. Як основа механізму державної політики у сфері захисту критичної інфраструктури розглядається сукупність об'єктивних залежностей і зв'язків між явищами і процесами саморозвитку і саморуху інституційних засобів правової дійсності, що здатний динамічно змінюватися, носити адаптивний характер відповідно до безпекової реальності мікро- та макросередовища, а також глобальної геополітичної ситуації. Розкрито основні завдання державної політики захисту критичної інфраструктури. Визначено адміністративно-правові основи формування переліку об'єктів критичної інфраструктури України у формі відповідного реєстру, зафіксовано певні проблеми організаційного характеру, що перешкоджають ефективності його функціонування.

Науково обґрунтовано підходи до оцінки інституційної спроможності національної системи захисту критичної інфраструктури, що дозволило проаналізувати її рівень у розрізі спроможностей структурних, організаційних, технічних систем та окремих індивідів, що включає розвиток навичок і компетенцій на всіх рівнях провадження державної політики у сфері захисту критичної інфраструктури крізь діоптрій процесних інституцій – правил, процедур, засобів, інструментів, методів, організацій і ресурсів. Інституційна спроможність національної системи захисту критичної інфраструктури ідентифікована як комплементарність внутрішньої системи профільних інститутів та відповідних інституцій, що детермінує їх здатність синхронно забезпечувати захист об'єктів

критичної інфраструктури з метою безперебійності їх функціонування.

Проведено аналіз чинного законодавства України та міжнародно-правових актів, ґенези доктринальних поглядів на проблему, стану та перспектив розвитку державної політики у сфері захисту критичної інфраструктури. Розкрито особливості інституційної архітектури національної системи захисту критичної інфраструктури в розрізі сил забезпечення безпеки й оборони об'єктів критичної інфраструктури, які імплікують реалізацію механізмів державної політики у сфері захисту критичної інфраструктури. Проведений аналіз показників інституційної спроможності національної системи захисту критичної інфраструктури в Україні дозволив виявити ряд проблемних питань, серед яких особливу увагу привертає обмеженість наукових досліджень за участю органів публічного управління і стейкхолдерів, відповідальних за політику захисту критичної інфраструктури, а також відсутність у складі освітніх програм управлінських спеціальностей в закладах вищої освіти та установах підвищення кваліфікації фахових компетентностей, орієнтованих на управління у сфері захисту об'єктів критичної інфраструктури.

Проаналізовано дієвість сучасної парадигми державної політики у сфері захисту критичної інфраструктури в умовах воєнного стану, що дало підстави констатувати адаптивність національної архітектури державної політики у сфері захисту критичної інфраструктури до умов масштабних змін геополітичних інтересів, що призвело до безпрецедентних фактів порушення територіальної цілісності країн із слабкою системою державної політики захисту та обороноздатності. Доведено факти безпрецедентного порушення на території України міжнародних конвенцій які забороняють піддавати ударам, знищувати чи виводити з робочого стану об'єкти критичної інфраструктури міст України. У таких умовах аналіз дієвості сучасної парадигми державної політики у сфері захисту критичної інфраструктури в умовах воєнного стану в Україні продемонстрував створення унікальної ситеми протидії дестабілізуючим

впливам на об’єкти критичної інфраструктури. Архітектура даної системи побудована на основі ідентифікації секторів та укомплектуванні реєстру об’єктів критичної інфраструктури, ідентифікації релевантних загроз для об’єктів критичної інфраструктури, організації інституційної ієрархії суб’єктів державної політики у сфері захисту критичної інфраструктури, удосконаленні інституційного забезпечення державної політики у цій сфері, компонування складових системи захисту критичної інфраструктури, вжиття необхідних заходів із подолання наслідків руйнувань об’єктів. Встановлено, що до даної системи обов’язково слід включити вектор превентивного та антикризового управління загрозами та ризиками, який відповідатиме пріоритезації предикату стійкості відносно захисту, що пропагує сучасна парадигма безпекознавства у країнах ЄС. Узагальнено методичний підхід до розробки концептуальних засад захисту критичної інфраструктури на основі забезпечення стійкості у штатному режимі, режимі готовності та запобігання, режимі реагування та режимі відновлення. Структуровано формат інтегрованої безпекової моделі критичної інфраструктури, що передбачає в межах чинної нормативної бази, формувати безпеково-ситуаційні моделі у якості фідбеку до моделі проєктної загрози.

Здійснено інтерпретацію іноземної практики реалізації ефективної державної політики у сфері захисту критичної інфраструктури, зокрема крізь призму положень нової Директиви ЄС 255, що сфокусовані на забезпеченні стійкості, а не захисту об’єктів критичної інфраструктури. Зміна акценту пояснюється неможливістю досягнути бездоганної захищеності інфраструктури в умовах активної фази війни, тобто пропонується сфокусувати зусилля на забезпеченні можливостей швидкої регенерації втрачених потужностей у разі надзвичайної деструктивної ситуації. Із проведеного аналізу закордонного досвіду визначено, що спільним знаменником державної політики у даному напрямку є вектор орієнтований на забезпечення стійкості критичної інфраструктури, орієнтованої на превентивність дій із забезпечення тріади соціальної, організаційної та

технологічної стійкості.

Запропоновано напрями інституційних перетворень у напрямку підвищення ефективності державної політики захисту критичної інфраструктури, основоположними із яких вбачається розвиток її поліінституціональності, що передбачає залучення до її реалізації стейкхолдерів об'єктів критичної інфраструктури. У напрямку забезпечення захисту критичної інфраструктури з позиції сучасної міжнародної практики, пропонується у якості розширеної альтернативи предикату «стійкість критичної інфраструктури» інтегрувати у сферу державної політики термін «резильєнтність критичної інфраструктури», що трактується як здатність об'єктів критичної інфраструктури протидіяти гібридним загрозам, за рахунок забезпечення посилення здатності країни, суспільства, органів державної влади та об'єктів критичної інфраструктури реалізувати 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. Приділяється увага перспективам розробки моделі вимірності резильєнтності критичної інфраструктури.

Розроблено та впроваджено комплексні заходи у напрямку посилення резильєнтності критичної інфраструктури на основі розмежування відповідальності за проєктні загрози. Пропонується сфокусувати інституційні перетворення у точці забезпечення її резильєнтності на основі існуючих національних систем безпеки, захисту та антикризового реагування за умов гарантування якісно нового рівня синхронізації дій та інтеракції між ними, із залученням до даного процесу науково-дослідних установ та стейкхолдерів критичної інфраструктури.

У дисертаційній роботі уперше обґрунтовано науково-методичний апарат комплексного застосування механізмів та процедур розробки і здійснення стратегії забезпечення рівня захисту критичної інфраструктури в

умовах сучасної геополітичної та воєнної обстановки на основі кластерного підходу.

Наукова новизна і теоретичне значення дослідження буде полягати в тому, що: у*перше:*

– обґрунтовано науково-методичний апарат комплексного застосування механізмів та процедур розробки і здійснення стратегії забезпечення рівня захисту критичної інфраструктури в умовах сучасної геополітичної та воєнної обстановки на основі кластерного підходу;

– введено в науковий обіг дефінітивну експозицію «кластер резильєнтності критичної інфраструктури»;

удосконалено:

– сутнісні характеристики понять «критична інфраструктура», «захист критичної інфраструктури», «стейкхолдери об'єктів критичної інфраструктури» і наведено аргументацію щодо їх застосування;

– напрями інституційних перетворень у векторі підвищення ефективності державної політики захисту критичної інфраструктури;

дістали подальшого розвитку:

– перспективи інтегрування у сферу державної політики терміну «резильєнтність критичної інфраструктури»;

– перспективи внесення змін до чинного Класифікатора професій та Стандарту вищої освіти України спеціальності 281 Публічне управління та адміністрування в частині доповнення фахових компетентностей орієнтованих на управлінське забезпечення національної системи захисту об'єктів критичної інфраструктури, що дозволить посилити інституційну спроможність у цій сфері.

Практичне значення дослідження полягає у тому, що теоретико-методичні положення, викладені у дисертації доведено до рівня чітких концептуальних і науково-методичних пропозицій та рекомендацій щодо стратегування державної політики у сфері захисту критичної інфраструктури.

Зокрема, в процесі роботи розроблено та впроваджено в управлінський процес на об’єктах критичної енергетичної інфраструктури алгоритм ризик-менеджменту та превентивного управління безпекою на принципах стійкості. Окремі елементи наукових результатів у вигляді моделі «кластеру резильєнтності критичної інфраструктури» враховано у процесі реалізації державної політики у сфері електроенергетики та теплопостачання при організації роботи комісій з перевірки знань працівників об’єктів критичної інфраструктури, під час планових перевірок готовності електричних мереж до роботи в кризових умовах та плануванні роботи. Застосовано УСБУ у Вінницькій області окремі результати досліджень дисертаційної роботи при погодженні планів захисту об’єктів критичної інфраструктури I-IV категорії критичності за проектними загрозами національного рівня «Терористичний акт або диверсія». Окремі висновки дисертаційного дослідження використано Департаментом цивільного захисту Вінницької міської ради при розробці програм та планів заходів у сфері цивільного захисту, зокрема спрямованих на захист населення і територій від надзвичайних ситуацій, пов’язаних із об’єктами критичної інфраструктури та запобігання їх виникненню. Пропозиції щодо забезпечення відповідних компетентностей із забезпечення захисту об’єктів критичної інфраструткри у фахівців управлінських спеціальностей впроваджено в освітіній процес Вінницького державного педагогічного університету імені Михайла Коцюбинського.

Ключові слова: *державна політика, захист критичної інфраструктури, об’єкти критичної інфраструктури, національна безпека, стійкість критичної інфраструктури, державно-приватне партнерство.*

ABSTRACT

Strahnytskyi J.O. **Peculiarities of the formation and implementation of state policy in the field of critical infrastructure protection. – Qualifying scientific work on manuscript rights.**

Dissertation for obtaining the scientific degree of Doctor of Philosophy in specialty 281 - Public management and administration. Vinnytsia State Pedagogical University named after Mykhailo Kotsyubynskyi. Vinnytsia, 2024.

The dissertation offers a solution to a burdensome scientific issue focused on summarizing the theoretical and methodological features of modern state policy in the field of critical infrastructure protection and theoretical substantiation of doctrinal views with a focus on improving state management mechanisms for ensuring the safety of critical infrastructure objects and generating relevant scientific and practical recommendations.

An analysis of theoretical approaches to the essence of critical infrastructure as an object of state administration is carried out, and a range of key attributes of the modern security environment, which lay the foundation for the goal-setting of state policy in the sphere of its protection, is described. Concepts and signs of state policy in the field of critical infrastructure protection are defined. The horizon of the description of critical infrastructure as a component of the national security of Ukraine is substantiated, and the belonging of its objects to the national infrastructure is recorded.

An analytical and bibliographic review of the scientific works of domestic scientists, as well as foreign scientific works devoted to the issue of substantiating the definition of "critical infrastructure", was carried out, which gave grounds to generate the author's vision of the meaningful content of this term. The author's interpretation emphasizes the belonging of critical infrastructure objects to the sphere of national security, which inspires the priority of responsibility for its preservation according to the state security policy, and also fixes the priority of the triad of man-society-state, which will ensure the improvement of state policy in this segment in accordance with the anthropocentric approach and concepts of

sustainable development.

A categorical and conceptual system of research on the theoretical and methodological foundations of ensuring the protection of critical infrastructure has been formed. The author's formulation of the definition of "critical infrastructure protection" as a purposeful synchronized joint activity of state institutions, owners, operators, as well as stakeholders of critical infrastructure objects with the application of a set of measures aimed at prevention, prevention, timely detection of potential and neutralization of real threats, minimization and elimination consequences and rapid restoration of the functional capacity of critical infrastructure in the event of its damage, which are implemented with the aim of avoiding human casualties, significant material and environmental damage, or other destructive consequences that may lead to a violation of national security. This interpretation changed the focus from the process of critical infrastructure protection to the prevention of crisis situations, differentiating responsibility between the state, owners, and direct employees of critical facilities, as well as justifying the intention of "stakeholders of critical infrastructure facilities" and updating their role in the field of protection.

Modern scientific paradigms of state policy formation in the field of critical infrastructure protection are analyzed with the aim of scientifically rethinking views on the process of forming the architecture of key postulates of state policy and clearly articulating the role of the state in the field of critical infrastructure protection. It is scientifically proven that the basis of institutional goal-setting of state policy measures in the field of critical infrastructure protection should be the paradigm of national security science. As a result of the analysis, we came to the conclusion that each of the analyzed paradigmatic postulates carries an eclectic dimension of the security transdisciplinary paradigm, which is proposed to be the basis of the scientific justification of the main basis of state policy in the field of critical infrastructure protection.

The institutional and legal peculiarities of the implementation of state policy in the field of critical infrastructure protection have been clarified. The

interpretation of the institutional and legal regulation of the implementation of state policy in the field of critical infrastructure protection as a system of organizational, managerial and legal measures implemented by the institutions of state power through which it is implemented is extrapolated. targeted (for the purpose of maximizing the safety of critical infrastructure objects) administrative influence on social relations is focused on the prevention of differentiated risks, threats and dangers to critical infrastructure objects based on the triad of man-society-state. As the basis of the mechanism of state policy in the field of critical infrastructure protection, a set of objective dependencies and connections between phenomena and processes of self-development and self-movement of institutional means of legal reality, which is capable of dynamic change and adaptive character in accordance with the security reality of the micro and macro environment, as well as global geopolitical situation. The main tasks of the state policy of critical infrastructure protection are disclosed. The administrative and legal basis for the formation of the list of critical infrastructure objects of Ukraine in the form of a corresponding register was defined, certain difficulties and problems of an organizational nature were recorded, which hinder the effectiveness of its functioning.

Approaches to the assessment of the institutional capacity of the national critical infrastructure protection system have been scientifically substantiated, which made it possible to analyze its level in terms of the capabilities of structural, organizational, technical systems and individual individuals, which includes the development of skills and competencies at all levels of the implementation of state policy in the field of critical infrastructure protection through a diopter process institutions - rules, procedures, means, tools, methods, organizations and resources. The institutional capacity of the national critical infrastructure protection system is identified as the complementarity of the internal system of specialized institutes and relevant institutions, which determines their ability to synchronously ensure the protection of critical infrastructure objects with the aim of uninterrupted operation.

An analysis of the current legislation of Ukraine and international legal acts, the genesis of doctrinal views on the problem, the state and prospects for the development of state policy in the field of critical infrastructure protection was carried out. The peculiarities of the institutional architecture of the national critical infrastructure protection system in terms of security and defense forces of critical infrastructure objects, which imply the implementation of state policy mechanisms in the field of critical infrastructure protection, are revealed. The analysis of indicators of the institutional capacity of the national system of critical infrastructure protection in Ukraine allowed us to identify a number of problematic issues, among which the limitation of scientific research with the participation of public administration bodies and stakeholders responsible for the policy of critical infrastructure protection, as well as the absence of management specialties in educational programs, draws special attention. in institutions of higher education and specialized institutions for the improvement of professional competences, oriented to management in the field of protection of critical infrastructure objects.

The effectiveness of the modern paradigm of state policy in the field of critical infrastructure protection under martial law conditions was analyzed, which gave grounds to state the adaptability of the national architecture of state policy in the field of critical infrastructure protection to the conditions of large-scale changes in geopolitical interests in the field of redistribution of territories and world resources, which in turn determines the struggle for centers of influence on the most important objects of critical infrastructure, which led to unprecedented violations of the territorial integrity of countries with a weak system of state protection policy and defense capability. The facts of an unprecedented violation on the territory of Ukraine of international conventions that prohibit striking, destroying or decommissioning objects necessary for the survival of the civilian population have been proven. Indisputable arguments have been established that one of the strategic goals of the army of the aggressor country was to choose the critical infrastructure facilities of the cities of Ukraine, located in the deep rear. In such conditions, the analysis of the effectiveness of the modern paradigm of state

policy in the field of protection of critical infrastructure in the conditions of martial law in Ukraine demonstrated the creation of a unique system of counteraction to destabilizing influences on critical infrastructure objects, which led to the damage and complete destruction of about a thousand such objects. The architecture of this system is built on the basis of the identification of sectors and the completion of the registry of critical infrastructure objects, the identification of relevant threats to critical infrastructure objects, the organization of the institutional hierarchy of state policy subjects in the field of critical infrastructure protection, the improvement of the institutional support of state policy in this area, layout of the components of the critical infrastructure protection system, taking the necessary measures to overcome the consequences of destruction of objects. It was established that this system must include a vector of preventive and anti-crisis management of threats and risks, which will correspond to the prioritization of the predicate of stability in relation to protection, which is promoted by the modern paradigm of security science in EU countries. The methodical approach to the development of conceptual principles of critical infrastructure protection based on ensuring stability in regular mode, readiness and prevention mode, response mode and recovery mode is summarized. In addition to this, the format of the integrated security model of critical infrastructure is structured, which provides for the formation of security-situational models as feedback to the project threat model within the limits of the current regulatory framework.

The foreign practice of implementing an effective state policy in the field of critical infrastructure protection was interpreted, in particular through the prism of the provisions of the new EU Directive 2557 (CER Directive), which are focused on ensuring stability, rather than protecting critical infrastructure objects. The change in emphasis is explained by the impossibility of achieving perfect security of the infrastructure in the conditions of the active phase of the war, that is, it is necessary to focus efforts on ensuring the possibility of rapid regeneration of lost capacities in the event of an extraordinary destructive situation. Based on the analysis of foreign experience, it was determined that the common denominator of

state policy in this direction is a vector focused on ensuring the stability of critical infrastructure, which is interpreted as a three-stage process of anti-crisis management, focused on preventive actions to ensure the triad of stability options: social, organizational and technological.

The directions of institutional transformations in the direction of increasing the efficiency of the state policy of protection of critical infrastructure are proposed, the fundamental of which is the development of its poly-institutionality, which involves the involvement of stakeholders of critical infrastructure objects in its implementation. In the direction of ensuring the protection of critical infrastructure from the standpoint of modern international practice, it is proposed as an extended alternative to the predicate "sustainability of critical infrastructure" to integrate the term "resilience of critical infrastructure" into the sphere of state policy, which is interpreted as the ability of critical infrastructure objects to counteract hybrid threats, due to ensuring the strengthening of the ability of the country, society, state authorities and critical infrastructure objects to implement an effective set of measures aimed at ensuring readiness, prevention, resistance to risks and threats of emergency situations, rapid restoration of the normal functioning of objects from their consequences, as well as constant improvement personnel competencies, learning experience and attracting private investments. Attention is paid to the prospects of developing a model for measuring the resilience of critical infrastructure.

Developed and implemented in the direction of strengthening the resilience of critical infrastructure based on the separation of responsibility for project threats, it is proposed to focus institutional transformations at the point of ensuring its resilience on the basis of existing national systems of security, protection and anti-crisis response under the conditions of guaranteeing a qualitatively new level of synchronization of actions and interaction between them, with the involvement of research institutions and critical infrastructure stakeholders in this process.

In the dissertation, for the first time, the scientific and methodological apparatus of the complex application of mechanisms and procedures for the

development and implementation of a strategy for ensuring the level of protection of critical infrastructure in the conditions of the modern geopolitical and military situation based on the cluster approach is substantiated.

The scientific novelty and theoretical significance of the research will be that: *for the first time:*

– the scientific and methodological apparatus of the complex application of mechanisms and procedures for the development and implementation of a strategy for ensuring the level of protection of critical infrastructure in the conditions of the modern geopolitical and military situation based on the cluster approach is substantiated.

– the definitive exposition "resilience cluster of critical infrastructure"

was introduced into scientific circulation improved:

– the essential characteristics of the concepts of "critical infrastructure", "protection of critical infrastructure" and the reasoning for their application are given.

– directions of institutional transformations in the vector of increasing the efficiency of the state policy of critical infrastructure protection

received further development:

– prospects of integrating the term "resilience of critical infrastructure" into the sphere of state policy;

– prospects for making changes to the current Classifier of Professions and the Standard of Higher Education of Ukraine, specialty 281 Public management and administration in terms of supplementing professional competencies focused on the management support of the national system for the protection of critical infrastructure objects, which will allow strengthening the institutional capacity in this area.

The practical significance of the research is that the theoretical and methodological provisions outlined in the dissertation have been brought to the level of clear conceptual and scientific-methodical proposals and recommendations

for strategizing state policy in the field of critical infrastructure protection. In particular, in the process of work, an algorithm of risk management and preventive safety management based on the principles of sustainability was developed and implemented into the management process at critical energy infrastructure facilities. Individual elements of scientific results in the form of a "cluster of resilience of critical infrastructure" model are taken into account in the process of implementing state policy in the field of electricity and heat supply when organizing the work of commissions for checking the knowledge of employees of critical infrastructure facilities, during scheduled checks of the readiness of electric networks to work in crisis conditions and work planning. Some research results of the dissertation were applied by the Ukrainian Security Service in the Vinnytsia region when approving plans for the protection of critical infrastructure objects of the I-IV criticality category according to the project threats of the national level "Terrorist act or sabotage". Separate conclusions of the dissertation research were used by the Department of Civil Protection of the Vinnytsia City Council in the development of programs and plans of measures in the field of civil protection, in particular aimed at protecting the population and territories from emergency situations related to critical infrastructure objects and preventing their occurrence. Proposals for ensuring the appropriate competences for ensuring the protection of critical infrastructure objects among specialists in management specialties have been introduced into the educational process of Mykhailo Kotsiubynskyi Vinnytsia State Pedagogical University.

Keywords: *public policy, critical infrastructure protection, critical infrastructure facilities, national security, critical infrastructure sustainability, public-private partnership*

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Основні результати дослідження відображено в публікаціях:

1. Яременко О. І., **Страхніцький Я. О.** Теоретичні підходи до визначення дефініції критичної інфраструктури як об'єкту державного управління. *Публічне управління та митне адміністрування.* 2022. №1 (32). С. 76-82. DOI: https://doi.org/10.32836/2310-9653-2022-1.13

2. Яременко О. І., **Страхніцький Я. О.** Теоретико-методичні основи забезпечення системи захисту критичної інфраструктури держави. *Державне управління: удосконалення та розвиток.* 2022. № 1. URL: http://www.dy.nayka.com.ua/?op=1&z=2610. DOI: https://doi.org/10.32702/2307-2156-2022.1.38

3. Яременко О. І., **Страхніцький Я. О.** Визначення та управління загрозами у структурі державної політики захисту критичної інфраструктури. *Університетські наукові записки*. 2022. № 3 (87). С. 73-82. DOI https://doi.org/10.37491/UNZ.87.6

4. **Страхніцький Я. О.** Структурно-функціональна характеристика системи захисту критичної інфраструктури в Україні. *Публічне управління та митне адміністрування.* 2022. № 4. (35). С.112-117. DOI https://doi.org/10.32782/2310-9653-2022-4.17

5. **Страхніцький Я. О.** Кластерний підхід до забезпечення захисту критичної інфраструктури в умовах воєнного стану в Україні. *Інвестиції: практика та досвід*. 2023. № 23. С.163-169. URL: https://www.nayka.com.ua/index.php/investplan/article/view/2610
DOI: https://doi.org/10.32702/2306-6814.2023.23.163

6. **Страхніцький Я. О.** Інституційні перетворення у напрямку підвищення ефективності державної політики захисту критичної інфраструктури. *Публічне управління та регіональний розвиток.* 2024. №1 (23). С. 28-52. DOI https://doi.org/10.34132/pard2024.23.02

7. Modernization of the system of public management and administration in Ukraine: the experience of the Republic of Latvia: SECTION 5. Features of the

current state policy in the sphere of protection of critical infrastructure in the conditions of war in Ukraine (**Strahnitskyi Ya. O.**). Scientific monograph. Riga, Latvia: “Baltija Publishing”, 2023, p. 115-143. DOI https://doi.org/10.30525/978-9934-26-279-1-5

Наукові праці, які засвідчують апробацію матеріалів дисертації

8. Яременко О. І., **Страхніцький Я. О.** Сучасні проблеми державної політики України у сфері захисту критичної інфраструктури. *Публічне управління в Україні: виклики сьогодення та глобальні імперативи»:* матеріали Міжнар. наук-практ. конф., м. Хмельницький, 11 лют. 2022 р. / Хмельницький: Хмельницький університет управління та права імені Леоніда Юзькова. Хмельницький, 2022. С. 126-129.

9. **Страхніцький Я. О.** Формування наукової парадигми державної політики у сфері захисту критичної інфраструктури. *Управління інноваційним процесом в Україні: напрями розвитку:* матеріали IX Міжнар. наук-практ. конф., м. Львів, 19-21 трав. 2022 р. Львівська політехніка. Львів, 2022. С. 176-178.

10. **Страхніцький Я. О.** Особливості сучасної системи захисту критичної інфраструктури в Україні. *Наука, освіта, технології та суспільство: актуальні проблеми теорії та практики*: матеріали Міжнар. наук-практ. конф., м. Полтава, 25 трав. 2022 р. Полтава, 2022. Ч. 1. С. 58-60.

11. **Strahnitskyi Ya. O.** Institutional aspects of state policy implementation in the sphere of critical infrastructure protection in Ukraine. *International Scientific Conference Development of Scientific Space in the Context of Global Changes: Conference Proceedings*, November 25-26, 2022. Riga, Latvia: «Baltija Publishing», P. 26-30.

12. **Strahnitskyi Ya. O.** Organizational and legal mechanisms of modern state policy in the field of critical infrastructure protection in Ukraine. *International scientific conference «Influence of Europeanization on public management and administration in Ukraine» : conference proceedings* (October 5–6, 2022. Riga, the Republic of Latvia). Riga, Latvia: “Baltija Publishing”. 2022. P. 91-95.

13. **Страхніцький Я. О.** Державна політика у сфері захисту критичної інфраструктури в умовах військового стану в Україні. *Сучасна парадигма публічного управління:* збірник тез IV Міжнар. наук.-практ. конф. м. Львів 10-12 листоп. 2022р. / За наук. ред. к.е.н., доцента Стасишина А.В.. ЛНУ імені Івана Франка, Львів, 2022. С. 376-381.

14. **Страхніцький Я. О.** Концептуальні засади забезпечення резильєнтності об'єктів критичної інфраструктури в умовах гібридних загроз. *Глобальні тенденції та національні особливості публічного управління та адміністрування*: матер. круглого столу, м. Вінниця 22 груд. 2023 р. Вінниця: Вінницький державний педагогічний університет імені Михайла Коцюбинського, ТОВ «Друк», 2023. С. 42-44.

Наукові праці, які додатково відображають наукові результати дисертації

15. **Страхніцький Я. О.** Особливості державної політики захисту критичної інфраструктури в Україні та напрями її удосконалення в умовах війни. *Knowledge, Education, Law, Management*. 2022. № 7. (51). С. 104-111. DOI https://doi.org/10.51647/kelm.2022.7.15

16. Kaminska V., Namazova Yu., **Strakhnitskyi Y.** Mehanisms of formation and implementation of state policy in the field of youth protection. *Modern Science.* 2022. №1. P. 41-49.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Сучасний розвиток світового суспільства базується на функціонуванні найважливіших секторів забезпечення життєдіяльності країн, серед яких учені виділяють енергетику, транспорт, телекомунікації та ін. Розлагодженість у роботі будь-якого із секторів загрожує суспільству глобальним дисбалансом та навіть руйнуваннями. Варто також відзначити, що разом із розвитком цивілізації у світі почастішали факти негативних явищ у вигляді природних катаклізмів, техногенних аварій, екологічних катастроф, терористичних актів, диверсій, військових конфліктів, кібератак, що загострює ризики дестабілізації функціонування світових держав. З огляду на ці факти та нинішню ситуацію військового вторгнення в Україні, питання безпеки та захисту об’єктів критичної інфраструктури стають все більш актуальними. По-перше, наслідки стихійних лих, аварій, катастроф та інших надзвичайних ситуацій набувають все більш масштабних і небезпечних наслідків для суспільства та стабільності функціонування економіки. По-друге, кризові явища, з якими стикнулося наше суспільство у період військової агресії, продемонструвало значимість об’єктів критичної інфраструктури та необхідність кардинальної зміни системи її захисту. По-третє, питання забезпечення організаційної структури, адміністративних функцій, напрямів розвитку та основ функціонування системи захисту критичної інфраструктури детермінує необхідність чіткої детекції місця та ролі держави. Це, у свою чергу, актуалізує необхідність вирішення проблем у модернізації державної безпекової політики у сфері забезпечення захисту критичних об’єктів в умовах воєнного стану в Україні**.**

Аналіз сучасних наукових доробків, засвідчив посилену увагу дослідників до питань захисту критичної інфраструктури, особливо удосконалення державної політики в умовах зростання військових загроз. Значний внесок у дослідження зазначеного вектора проблем зробили такі науковці, як: О. Я. Лазор, О. Д. Лазор, С. І. Азаров, В. Л. Сидоренко,

С. А. Єременко, А. В. Пруський, О. П. Єрменчук, Г. Ю. Зубко, С. І. Кондратов, О. М. Суходоля, А.В. Заболотний, І. Г. Юник, О. П. Єрменчук, М. Б. Домарацький, Д. С. Бірюков, С. В. Бєлай та інші. Аналізу наукових джерел із проблематики державного управління у сфері національної безпеки, у тому числі − захисту критичної інфраструктури присвячено вагомий теоретичний доробок як українських, так і зарубіжних учених таких як: М. Ф. Криштанович, Я. Я. Пушак, М. І. Флейчук, В. І. Франчук, С. І. Крук, В. А. Ліпкан, Д. Г. Бобро, С. П. Іванюта, С. І. Кондратов, О. М. Суходоля, Д. М. Павлов, М. А. Микитюк та ін.

Водночас, недостатньо вивченими залишаються окремі аспекти специфіки державної політики у сфері захисту критичної інфраструктури, складової її теоретичного обгрунтування та практичних дієвих напрямів державного управління критично важливими об’єктами в умовах військового стану. Це зумовлює актуальність обраної теми дослідження.

Зв’язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано у Вінницькому державному педагогічному університеті відповідно до тематики науково-дослідної роботи «Теоретико-методологічні та практичні аспекти публічного управління суспільними процесами в Україні», державний реєстраційний номер: 0122U000282.

Тема дисертаційного дослідження затверджена Вченою радою Вінницького державного педагогічного університету імені Михайла Коцюбинського (витяг з протоколу № 4 від 20 жовтня 2021 року).

Об’єкт дослідження – державна політика у сфері захисту критичної інфраструктури.

Предмет дослідження – сукупність теоретичних, методичних та прикладних аспектів формування та реалізації державної політики у сфері забезпечення безпеки об’єктів критичної інфраструктури в Україні.

Мета дослідження полягає в обґрунтуванні теоретичних засад та розробці практичних рекомендацій щодо удосконалення державної політики у сфері захисту об’єктів критичної інфраструктури.

Задля досягнення поставленої мети визначено наступні **завдання:**

1. Розкрити теоретичні підходи до сутності критичної інфраструктури як об'єкту державного управління.

2. Дослідити теоретико-методичні засади забезпечення захисту критичної інфраструктури.

3. Проаналізувати сучасні наукові парадигми формування державної політики у сфері захисту критичної інфраструктури.

4. Здійснити оцінку інституційно-правових аспектів реалізації державної політики у сфері захисту критичної інфраструктури.

5. Оцінити інституційну спроможність національної системи захисту критичної інфраструктури.

6. Проаналізувати дієвість сучасної парадигми державної політики у сфері захисту критичної інфраструктури в умовах воєнного стану.

7. Визначити особливості іноземної практики реалізації ефективної державної політики у сфері захисту критичної інфраструктури.

8. Запропонувати напрями інституційних перетворень у напрямку підвищення ефективності державної політики захисту критичної інфраструктури.

9. Запропонувати шляхи удосконалення державних механізмів реалізації політики захисту критичної інфраструктури України в умовах воєнного стану.

Методи дослідження. З метою вирішення поставлених у дисертації завдань було використано наступні наукові методи:

– аналіз і синтез, індукція та дедукція – для деталізації предмета дослідження;

– ретроспективний аналіз – для оцінки кількості надзвичайних ситуацій на критично важливих об'єктах України;

– структурний підхід – для визначення взаємозв'язків між елементами державної системи захисту критичної інфраструктури;

– логіко-дескриптивний аналіз – для визначення напрямів

трансформації державної системи моніторингу стану критичної інфраструктури;

Наукова новизна і теоретичне значення одержаних результатів полягає у принципово та якісно новому узагальненні засад формування та реалізації державної політики у сфері захисту критичної інфраструктури та обґрунтування у формотворчому вимірі науково-практичних рекомендацій щодо комплексу заходів з її удосконалення.

Уперше:

– обґрунтовано науково-методичний апарат комплексного застосування механізмів та процедур розробки і здійснення стратегії забезпечення рівня захисту критичної інфраструктури в умовах сучасної геополітичної та воєнної обстановки на основі кластерного підходу;

– уведено в науковий обіг дефінітивну експозицію «кластер резильєнтності критичної інфраструктури»;

удосконалено:

– сутнісні характеристики понять «критична інфраструктура», «захист критичної інфраструктури», «стейкхолдери об'єктів критичної інфраструктури» і наведено аргументацію щодо їх застосування;

– напрями інституційних перетворень у векторі підвищення ефективності державної політики захисту критичної інфраструктури;

подальшого розвитку набули:

– перспективи інтегрування у сферу державної політики терміну «резильєнтність критичної інфраструктури»;

– перспективи внесення змін до чинного Класифікатора професій та Стандарту вищої освіти України спеціальності 281 Публічне управління та адміністрування в частині доповнення фахових компетентностей орієнтованих на управлінське забезпечення національної системи захисту об'єктів критичної інфраструктури, що дозволить посилити інституційну спроможність у цій сфері.

Практичне значення одержаних результатів полягає у тому, що теоретико-методичні положення, викладені у дисертації доведено до рівня чітких концептуальних і науково-методичних пропозицій та рекомендацій щодо стратегування державної політики у сфері захисту критичної інфраструктури. Результати дисертаційної роботи впроваджено у: навчальний процес Вінницького державного педагогічного університету імені Михайла Коцюбинського (довідка від 26.12.2023 р. № 06/39). За результатами дисертаційного дослідження впроваджено використання в управлінському процесі на об'єктах критичної енергетичної інфраструктури (які зазнають найбільшого цілеспрямованого руйнування з боку ворога) запропонованого алгоритму ризик-менеджменту та превентивного управління безпекою на принципах стійкості. Окремі елементи наукових результатів враховано у процесі реалізації державної політики у сфері нагляду (контролю) у галузях електроенергетики та теплопостачання. Зокрема при організації роботи комісій з перевірки знань працівників об’єктів критичної інфраструктури, під час планових перевірок готовності електричних мереж до роботи в кризових умовах та плануванні роботи (довідка від 13.11.2023 р. № 10/14/751-23). Застосовано УСБУ у Вінницькій області окремі результати досліджень дисертаційної роботи при погодженні планів захисту об’єктів критичної інфраструктури I-IV категорії критичності за проектними загрозами національного рівня «Терористичний акт або диверсія» (довідка від 19.03.2024 р. № 53/2/52-21018). Окремі висновки дисертаційного дослідження використано Департаментом цивільного захисту Вінницької міської ради при розробці програм та планів заходів у сфері цивільного захисту, зокрема спрямованих на захист населення і територій від надзвичайних ситуацій, пов’язаних із об’єктами критичної інфраструктури та запобігання їх виникненню (довідка від 10.11.2023 р. № 27/00/014/69236).

Особистий внесок здобувача. Дисертаційна робота є самостійною науково-дослідною роботою автора, яка містить теоретичні обґрунтування, практичні рекомендації, висновки та пропозиції, що були отримані автором

особисто, та в сукупності вирішують важливе наукове завдання щодо розробки та впровадження комплексу заходів щодо підвищення рівня державної безпеки критичної інфраструктури.

Апробація результатів дослідження. Основні положення дисертації доповідалися на:

– *міжнародних науково-практичних конференціях:* «Публічне управління в Україні: виклики сьогодення та глобальні імперативи». (м. Хмельницький, 11 лютого 2022 року); «Управління інноваційним процесом в Україні: напрями розвитку» (м. Львів, 19-21 травня 2022 р.); «Наука, освіта, технології та суспільство: актуальні проблеми теорії та практики» (Полтава, 25 травня 2022 р.); «Influence of Europeanization on public management and administration in Ukraine» (Riga, Latvia 5-6 жовтня 2022 р.); Сучасна парадигма публічного управління (м. Львів, 10-12 листопада 2022 р.); Development of Scientific Space in the Context of Global Changes: Conference Proceedings (Riga, Latvia 25-26 листопада, 2022 р.);

– *круглому столі* «Глобальні тенденції та національні особливості публічного управління та адміністрування» (м. Вінниця 22 грудня 2023 р).

Публікації. Основні положення та результати дослідження за темою дисертації відображено у 16 наукових працях, з яких 6 статей у провідних наукових фахових виданнях, затверджених АК МОН України; 2 статті – у наукових закордонних виданнях; 1 стаття у закордонній монографії та 7 тез – у збірниках матеріалів конференцій.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, висновків, списку використаних джерел і додатків. Повний обсяг дисертації становить 312 сторінок, з них 240 сторінок основного тексту. Робота містить 18 рисунків, 3 таблиці та 5 додатків. Список використаних джерел містить 358 найменувань.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Теоретичні підходи до визначення критичної інфраструктури як об'єкту державного управління.

Валідність непорушності автентичних принципів і фундаментальних засад забезпечення національної безпеки має безумовне значення для будь-якої незалежної країни світу. В сучасних умовах військового стану в Україні це питання є пріоритетним у сфері державного управління, що пояснюється чинним законодавством, зокрема п. 9 ст. 1 Закону України «Про національну безпеку України», яким визначено інтенцію національної безпеки як «захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз» [62]. Згідно п. 10 ст. 1 цього ж Закону, під національними інтереси України пропонується розуміти «життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян» [62]. При цьому зазначені норми роблять акцент саме на стратифікації векторів забезпечення фундаментальних національних інтересів України, до яких включено:

1. Територіальну цілісність та державний суверенітет України, її конституційний лад на принципах демократії і недопущення інтерцесії внутрішніх справ;

2. Сталий економічний розвиток держави для забезпечення якості життя населення та нарощування його рівня;

3. Євроінтеграційний вектор розвитку України у політичному, правовому економічному та безпековому просторі та розвиток паритетних взаємовигідних відносин з іншими країнами із перспективою набуття

повноправного членства в ЄС та в Організації Північноатлантичного договору [62]. Отже, аналіз формотворчих постулатів зазначеного Закону дає підстави стверджувати, що національна безпеку інспірує еклектичність трьох складників: національних життєво важливих інтересів, стратегічних загроз і національної системи захисту. Серед «актуальних загроз національній безпеці» «загрози критичній інфраструктурі» вперше було виділено у Стратегії національної безпеки України у 2015 р., який захист критичної інфраструктури відніс до державної політики національної безпеки [240].

Прислухаємось до позиції М. Б. Домарецького [40, с. 83], який пропонує життєво важливі інтереси держави варіантивувати на наступні напрями:

– гарантування ефективного захисту критично важливих об'єктів та населення в умовах надзвичайних ситуацій чи терористичних актів;

– підтримка безпеки та виживання населення у період війни;

– підтримка функціональності об'єктів, конче необхідних для виживання населення та стабільності функціонування економіки.

Отже, в авангарді національної безпеки України встановлено саме захист об'єктів критичної інфраструктури, що також підтверджує новий Закон «Про критичну інфраструктуру» від 16.11.2021 р.. Цілком погоджуємось із даним положенням, мотивуючись також і закордонним аргументом, закріпленим Стратегією внутрішньої безпеки США [300], який ідентифікує шість основних векторів забезпечення національної безпеки (рис.1.1.).

Рис.1.1. Структура системи забезпечення національної безпеки США

Джерело: сформовано авторами за даними [33],[300]

Перелік загроз національній безпеці, які варто враховувати при формуванні державної політики захисту критичної інфраструктури, також визначає Стратегія національної безпеки України [240]:

– ризики надзвичайних ситуацій техногенного і природного характеру, процеси змін клімату та виникнення і поширення інфекційних хвороб;

– світова гонка на основі нових типів озброєнь;

– прогресування міжнародної злочинності у кіберпросторі, тероризму, наркоторгівлі, сепаратизму, торгівлі людьми, розповсюдження зброї та ін.

– пандемія COVID-19, що детермінує каскад деструктивних проявів, зокрема: зростання безробіття, криза соціального захисту та охорони здоров'я, обмеження руху товарів та зниження продовольчої безпеки, міграція робочої сили, розвиток світової фінансово-економічної кризи;

– зростання проявів демонстрації «національної сили» у міжнародній конкурентній боротьбі, у тому числі збройна експансія рф проти України;

– рудиментарність систем озброєння радянського виробництва внаслідок дефіциту фінансування на модернізацію;

– низька результативність державних інститутів влади внаслідок прогресування корупційної складової;

– низький рівень добробуту населення;

– низький рівень правової захищеності у ключових сферах та значна доля державної власності в економіці та мінімальна конкуренція (зокрема секторах критичної інфраструктури), що стримує інвестиційну діяльність;

– регрес середовища життя громадян (нераціональне використання природних ресурсів, деградація якості води, повітря, продуктів харчування).

– посилення демографічної кризи та прогресування еміграції.

Варто також відзначити зростання загроз та ризиків для критичної інфраструктури у вигляді несанкціонованих фізичних- або кібер- втручань, погіршення її технічного стану, відсутністю інвестиційних вкладень у модернізаці, тривалі бойові дії на Сході країни, а також тимчасову окупацію

частини території. Вивчаючи окремі приклади нормативних актів іноземних держав [292], [300], відзначимо, що спільним знаменником можна вважати розподіл загроз критичній інфраструктурі на три основні категорії: зловмисні дії, надзвичайні ситуації техногенного характеру та надзвичайні ситуації природного характеру. Прислухаємось до думки Д. Г. Бобро [11, с. 86], який пропонує додати до цього списку ще сукупні ризики. Підтримуємо думку вченого, що дану категорію варто вважати особливо небезпечною, оскільки такі загрози можуть сприяти виникненню «ефекту доміно» у вигляді варіативних каскадних ефектів внаслідок синергії об'єктів критичної інфраструктури між собою. Вважаємо, що семантичний опис даного явища краще розкриє предикат «каскадний ефект дестабілізації критичної інфраструктури», як причинно-наслідкове явище, що виникає у результаті дестабілізації функціонування одного, або декількох інфраструктурних об'єктів, що інспірує масштабний збій у інших взаємопов'язаних системах. Наприклад, водопостачання корелює з енергозабезпеченням насосних станцій від яких залежать пожежні служби і т.п.

Влада розвинутих країн, при розбудові власної нормативно-правової бази, розглядають критичну інфраструктуру, як один із базових детермінант національної безпеки. Уряд України з недавнього часу теж звернув увагу на стратегічність даного сектору та ідентифікував спектр ключових тригерів забезпечення ефективної системи його захисту у Стратегії національної безпеки. Проте, сектор національної безпеки України все ж потребує пристальної уваги до радикальної модифікації, особливо у напрямку державного регулювання захисту критичної інфраструктури. Особливо актуалізувалось дане питання у світлі проголошеної євроінтеграції та з урахуванням світової практики формування й реалізації державної політики національної безпеки. Зазначені мотиватори особливо загострюють для наукових досліджень проблему вивчення, розробки та запровадження в Україні концепції державної політики у сфері захисту критичної інфраструктури. Запуск даного напрямку наукового пошуку варто розпочати

із обґрунтування дефініції «критична інфраструктура». Це дозволить зафіксувати наукове підґрунтя для подальшої розробки дієвих рішень посилення ефективності державного управління безпекою комплексу життєво-важливих для держави галузей.

Аналіз вітчизняної та закордонної нормативно-правової бази із регулювання суспільних відносини у сфері національної безпеки підтверджує, що термін «критично-важливі об'єкти» введений в нормативно-законодавчих актах більшості світових країн, однак його семантика дещо відрізняється. Як демонструють результати досліджень нормативно-правової бази та досвіду міжнародної семантики, перші згадки дефініції «критична інфраструктура» почали з'являтись у середині 90-х років минулого століття. В Україні предикат «критична інфраструктура» офіційно з'явився у вжитку із 2006 р.. Однак категоризація критичності об'єктів критичної інфраструктури була здійснена лише через 15 років Законом України «Про критичну інфраструктуру» як «ступінь (відносний рівень) важливості об'єкта критичної інфраструктури, класифікована (категоризована) залежно від його впливу на виконання життєво важливих функцій та/або надання життєво важливих послуг» [60], що стало важливим кроком у розбудові державної політики у сфері захисту критичної інфраструктури.

До сьогодні у наукових, ділових та урядових колах дефініція «критична інфраструктура» постійно коригується та удосконалюється, однак інтерсуб'єктивним індикатором у багатогранності трактувань можна вважати зв'язок державних та приватних об'єктів, які прямо чи опосередковано впливають на рівень національної безпеки та обороноздатності держави й підтримують життєво важливі функції у суспільстві. Зважаючи на це, можемо погодитись із переконанням учених [47, с.112], [251, с. 69], які до критичної інфраструктури відносять транспортні та енергетичні мережі, газо та нафтопроводи, системи життєзабезпечення, інфраструктуру річкового й морського транспорту, канали зв'язку, вивезення й нейтралізацію небезпечних відходів, оборонний комплекс, служби екстреного реагування

на надзвичайні ситуації і органи влади. У США до критичної інфраструктури нещодавно також віднесли національні символи та пам'ятки, а також комерційні об'єкти (музеї, виставки та інші місця, що становлять національну цінність) [13]. Під критично важливою інфраструктурою колектив авторів на чолі із С. П. Азаровим та В. Л. Сидоренко розуміють «набір взаємодіючих сегментів і складових їх (що входять до їх складу) об'єктів національного господарського комплексу, що підтримують сфери життєдіяльності, часткова деградація і повна втрата функціональності яких здатна прямо і протягом відносно короткого інтервалу часу впливати на стан тих чи інших складових національної безпеки, приводити до надзвичайних ситуацій певного рівня і масштабу» [1, с. 45].

Уряди більшості розвинених країн напрацювали власні автентичні підходи до трактування поняття критичної інфраструктури у законодавстві. Флагманом інтеграції у державну політику стратегії захисту критичної інфраструктури слід вважати США, де законотворці вперше офіційно зафіксували інтенцію «критична інфраструктура» і остаточно його утвердили 23 жовтня 2001 р., нормативним актом «USA Patriot Act» [353]. Даною інституцією поняття «критична інфраструктура» трактується як «система життєво важливих для країни фізичних чи віртуальних активів і засобів, повне знищення або навіть часткова недієздатність яких можуть призвести до негативного впливу на національну безпеку, економіку, здоров'я та безпеку населення, або будь-яку комбінацію з переліченого» [353]. Представлене формулювання вчергове закріпило політику безпеки критичної інфраструктури у ролі детермінанти національної безпеки.

Релевантним у процесі розширеного вивчення предмету дослідження, є аналіз підходів до інтерпретації інтенції критичної інфраструктури як складової державної політики європейських країн. Так, у 2002 р. у процесі роботи Євроатлантичної ради НАТО зазначалося, що «критична інфраструктура включає в себе кібернетичні та фізичні системи забезпечення важливих і необхідних видів діяльності економіки та державного

управління». У Директиві Європейської Комісії 2008/114 [295] сутність критичної інфраструктури трактували як «об'єкти, системи чи їх частини, розташовані в країнах-членах ЄС, які є суттєвими для підтримки життєво важливих функцій суспільства, здоров'я, безпеки, захищеності, економічного та соціального благополуччя людей, порушення функціонування або знищення яких матимуть значний вплив у країні-члені ЄС та призведуть до нездатності забезпечувати вказані функції» [295, с 168].

У нормативній базі Німеччини визначення «критична інфраструктура» міститься у Національній стратегії захисту критичної інфраструктури. Там вона тлумачиться як «фізичні та організаційні структури та засоби, які мають життєво важливе значення для суспільства та економіки країни, збій або дисфункція у роботі яких призведе до хронічного дефіциту поставок, суттєвого порушення громадської безпеки та інших драматичних наслідків» [331, с. 8]. Наведене формулювання за своєю суттю збігається із визначенням презентованим Європейською Комісією, за єдиним винятком, – у німецькому варіанті акцент зроблено на пріоритеті забезпечення стабільності поставок. Це можна розтлумачити як стабільність надання послуг життєвої необхідності та постачання відповідних товарів.

У Польщі даний предикат зафіксовано нормативним актом Ustawa o zarządzaniu kryzysowym (Закон «Про антикризове управління»), у якому під критичною інфраструктурою польські законотворці розуміють «системи та їх функціонально пов'язані об'єкти, включаючи будівельні об'єкти, пристрої, установи, ключові служби для безпеки держави та її громадян і забезпечення ефективного функціонування органів державного управління, а також приватних підприємств» [354, с.1]. Аналізуючи дане трактування відзначимо акцент на пріоритетності стабільної роботи органів державної влади та визначенні окремої категорії спеціалістів із забезпечення роботи критичних секторів країни. Важливо також зауважити, що закордонний досвід визначення критичної інфраструктури зміщує акцент із фізичного виміру об'єктів до значимості їх функцій та послуг у забезпеченні потреб

суспільства, держави та економіки.

Власну специфіку трактування критичної інфраструктури мають і інші країни. Наприклад, у Хорватії до даної сфери відносять діяльність, мережі, послуги, матеріальні блага та інформаційні технології, вихід з ладу або знищення яких значно вплинуло би на здоров'я та безпеку громадян, або на діяльність державної влади. У Австралії це фізичні об'єкти, інформаційні технології, комунікаційні мережі, ланцюжки постачань, які в разі знищення, модифікації або недоступності протягом тривалого часу матимуть істотний вплив на соціальне чи економічне благополуччя нації або негативно позначаться на здатності забезпечувати національну оборону Австралії та гарантувати її національну безпеку. У державному управлінні Ізраїлю критична інфраструктура ідентифікується об'єктами, порушення функціонування яких може призвести до значних соціально-економічних потрясінь, здатних підірвати стабільність у суспільстві і тим самим призвести до реалізації загроз національній безпеці країни. У Японії формування критичної інфраструктури покладається на суб'єктів господарювання і які надають настільки незамінні послуги, що зниження їхньої ефективності або недоступність може мати важливе значення для соціального життя та економічної діяльності людей [47, с.112].

Важливо зауважити, що за кордоном у ідентифікації критичної інфраструктури із фізичного виміру об'єктів акцент зміщено ближче до важливості їх послуг та функцій щодо забезпечення потреб держави, суспільства та економіки. Це надає ефективні методологічні можливості для визначення критеріїв відбору елементів критичної інфраструктури та першочерговості їх захисту.

Аналіз представленої різноманітності дефініцій дає підстави зробити узагальнення, що більшість з них сфокусовані на ключовому значенні даного сектору для безпеки держави, її громадян та суспільства вцілому. Погодимось із думкою вчених С. Гнатюка, В. Сидоренка, Н. Сєйлової [28, с.85], які уніфікують критичну інфраструктуру як глобальну систему

стратегічно-важливого значення, що об'єднує масив елементів різного типу, об'єднаних зв'язками, що демонструє синхронність критичних об'єктів різного профілю. З наведених визначень видно, терміну «критична інфраструктура» в різних країнах світу притаманні не суттєві відмінності, що очевидно відображають національну або організаційну специфіку сфери та особливості нормативно-правових систем застосування терміну.

Сфокусуємо увагу ще на одному важливому питанні – розпізнати об'єкти національної інфраструктури та виокремити серед них критично важливі відповідно до значимості виконуваних функцій та надаваних послуг. Аналіз вітчизняної нормативно-правової бази дає підстави узагальнити усі потенційно важливі об'єкти критичної інфраструктури у квадро-комплекс:

1. Об'єкти загальнонаціонального значення.
2. Життєво-необхідні об'єкти.
3. Стратегічно-важливі об'єкти.
4. Суспільно-необхідні об'єкти.

Окремі учені проблемою у реалізації державної політики у сфері захисту критичної інфраструктури вбачають складність ідентифікації її об'єктів у якості критичних на національному, регіональному та локальному рівнях. Ключ до відповіді на дане питання вітчизняні законотворці надали у Законі України «Про критичну інфраструктуру» [60] де зазначили перелік критично важливих послуг та виконуваних функцій, надавачі яких потребують пріоритетного захисту. До таких послуг включено: водопостачання та водовідведення, фармацевтична промисловість енергозабезпечення, стале функціонування біолабораторій, продовольче забезпечення, охорону здоров'я, виготовлення вакцин, інформаційні послуги, фінансові послуги, електронні комунікації, оборону та державну безпеку, транспортне забезпечення, цивільний захист населення та територій, правопорядок, здійснення правосуддя, тримання під вартою, служби порятунку, космічну діяльність, дослідницьку діяльність, космічні технології та послуги, хімічну промисловість. Вважаємо, що даний перелік є не є достатньо деталізованим

та вичерпним, він здатний варіювати залежно від розміру країни та може досягати декількох тисяч пунктів, як наприклад, у США, де список критичних об'єктів налічує близько 1,7 тис об'єктів на національному рівні та більше 33 тис на регіональному і місцевому рівнях [300]. Дане припущення підтверджує В. О. Євсєєв [45, с.170], який наголошує, що згідно із світовою практикою, до об'єктів критичної інфраструктури необхідно також включити об'єкти можливих терористичних посягань, об'єкти, які підлягають охороні і обороні в особливий період та під час надзвичайних ситуацій і, підприємства стратегічного значення для економіки та безпеки, важливі державні об'єкти, установи державної влади та місцевого самоврядування, об'єкти, що знаходяться під обов'язковою охороною за договорами із підрозділами Державної служби охорони, радіаційно небезпечні об'єкти, чергово-диспетчерська система екстреної допомоги, об'єкти підвищеної небезпеки, об'єкти, включені до Державного реєстру потенційно небезпечних об'єктів, аварійно-рятувальні служби, платіжні системи, Національну систему конфіденційного зв'язку, нерухомі об'єкти культурної спадщини. Відповідно, відзначимо суттєві перспективи до удосконалення спектру юрисдикції державної політики у сфері захисту критичної інфраструктури.

Критичність об'єктів інфраструктури визначається впливом загроз втрати або приведення в непридатний стан об'єкта на життєзабезпечення населення та нації в цілому. Наслідки категоризуються за різними напрямками і сегментами, зокрема: довкілля,економіка, здоров'я і безпека, фінанси, тривалість впливу, технологічне середовище та ін. Під час оцінки критичності інфраструктурних об'єктів береться до уваги не тільки масштаб ефекту його дизфункції, але і такі чинники, як час на його регенерацію.

Відповідно до визначають об'єкти критичної інфраструктури як «об'єкти, вплив на які, зокрема через об'єкти критичної інформаційної інфраструктури, може мати наслідки, що безпосередньо зачіпають національну безпеку, включаючи безпеку людини і громадянина, суспільства

та держави, до яких належать такі компоненти» [9] (рис. 1.2.).

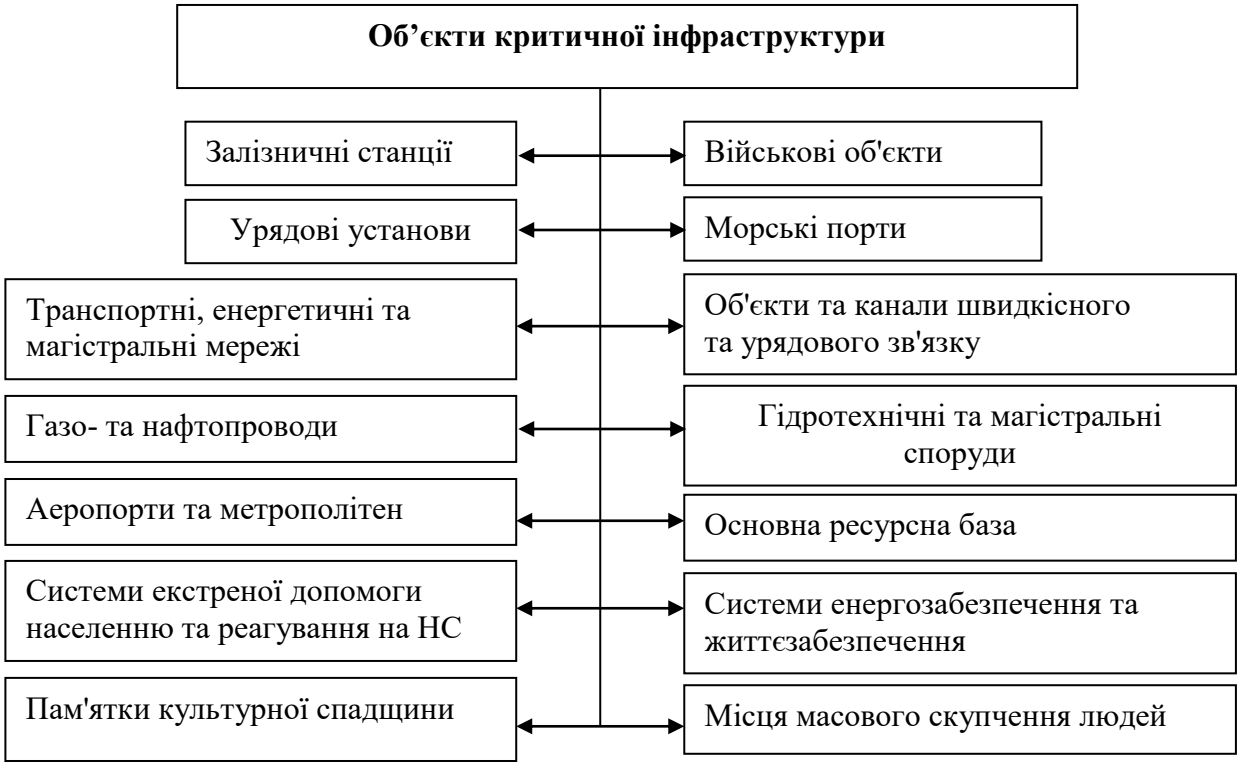


Рис. 1.2. Об’єкти критичної інфраструктури

Джерело:сформовано на основі [1]

Учені Бірюков Д.С., Кондратов С.І. за рівнем значущості об’єкти критичної інфраструктури поділяють на місцеві, регіональні та загальнодержавні, а ієрархію розглядають у основних групах [9, с.110]: здоров’я населення та безпека життєдіяльності, економічна безпека, державна оборона й безпека, національний імідж та самоповага держави.

Внаслідок проведеного аналізу нормативних актів іноземних держав можемо резюмувати, що у більшості країн виокремлюють 12 секторів критичної інфраструктури, із яких до основних відносять: фінансовий сектор (24 країни з 29), енергетику (29 країн з 29), транспорт (29 країн з 29), системи водопостачання (24 країни з 29), інформаційні, телекомунікаційні технології (27 країн з 29). В Україні на сьогодні чинна нормативно-правова база ідентифікує ряд категорій об’єктів, що підлягають особливим умовам безпеки:

– підприємства стратегічного економічного і безпекового

значення [205];

– об’єкти підвищеної небезпеки [64];

– важливі державні об’єкти [203];

– об’єкти, що підпадають під юрисдикцію підрозділів державної служби охорони за договорами [213];

– об’єкти, що підлягають обороні та охороні в умовах надзвичайного стану та в особливий період [64];

– особливо важливі об’єкти електроенергетики [229];

– особливо важливі об’єкти нафтогазової галузі [204];

– національна система конфіденційного зв’язку [63];

– платіжні системи [70];

– система екстреної допомоги населенню за єдиним номером 112 [71];

– аварійно-рятувальні служби [90];

– нерухомі об’єкти культурної спадщини [69].

Отже, проведений аналіз міжнародних нормативних актів та наукових доробків учених у напрямку регламентування захисту життєво-важливих об’єктів інфраструктури, дає підстави до більш диверсифікованої класифікації таких об’єктів що підпадатимуть під державну політику захисту. Визначення характеристик критичності об’єктів інфраструктури на базі нормативно-правових документів різних держав дає Україні перспективи переглянути вимоги до забезпечення їх безпеки з урахуванням можливих наслідків для населення та ступеня потенційної небезпеки.

Наступним важливим критерієм є взаємний вплив одного об’єкта на інший у вигляді згадуваного вище «каскадного ефекту дестабілізації критичної інфраструктури», коли припинення роботи одного із критичних об’єктів детермінує каскад масштабних наслідків. Зокрема, виведення з ладу енергооб’єктів призводить до припинення водопостачання або роботи телекомунікаційних мереж. Втрата зв’язку до порушення роботи, управління і контролю інших об’єктів, наприклад, автоматичних апаратів в банках і т. п. Як правило, ступінь критичності об’єктів учені поділяють на три категорії:

високий, середній і низький. Допускаються і деякі варіації цих категорій за різними методологічними підходам, так критичність діяльності різних об'єктів може по різному оцінюватись.

Лише надзвичайно важливі для забезпечення державної безпеки об'єкти національної інфраструктури можуть визначатися як критична інфраструктура. Загалом, проаналізувавши світовий досвід, відзначимо, що захист критичної інфраструктури поєднує три основні напрями:

1) захист від загроз у сфері державної безпеки; вони можуть включати внутрішні загрози та фізичне знищення критичної інфраструктури;

2) захист від кіберзагроз;

3) захист від надзвичайних ситуацій.

Загалом, аналізуючи поняття «критична інфраструктура», зрозуміло, що воно повинно включати ті найважливіші об'єкти, без яких чи з порушенням діяльності яких у державі можуть настати навіть невідворотні негативні процеси, можуть бути завдані великі збитки громадянам, їх здоров'ю та життю, соціально-економічній ситуації. Саме від стабільної діяльності критичної інфраструктури залежить функціонування національної інфраструктури та економіки в цілому.

Зазначимо, що тривала відсутність у вітчизняному законодавстві офіційного визначення даної категорії та чіткого переліку об'єктів приналежних до критичної інфраструктури детермінувало пролонгований у часі інституційний бар'єр, щодо розвитку ефективної державної політики безпеки у цій сфері та сприйняття критичної інфраструктури у якості складової національної безпеки. Перша офіційна згадка про критичну інфраструктуру зафіксована у тексті «Рекомендацій парламентських слухань з питання розвитку інформаційного суспільства» [240] у 2006 році. Наступною інституцією стала Стратегія національної безпеки 2012 р. «Україна у світі, що змінюється» [240] (втратила чинність), де термін «критична інфраструктура» використовувася у контексті захисту лише енергетичної та інформаційної безпеки. Більш комплексно критичну

інфраструктуру закріплено у тексті рішення Ради національної безпеки і оборони України від 01.03.2014 р. «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» [226], де Міністерству внутрішніх справ України наказувалося «забезпечити посилену охорону об'єктів енергетики та критичної інфраструктури» [226]. Однак у даному випадку, вважаємо, що законотворці допустились грубої помилки сепарувавши об'єкти енергетики окремо від критичної інфраструктури. При цьому чіткого формулювання поняття «критичної інфраструктури» та її складових не зафіксовано. Про поняття «критична інфраструктура» також йшлося в Указі Президента «Про рішення Ради національної безпеки та оборони України від 06.05.2015 р. «Про Стратегію національної безпеки України» від 26.05.2015 р. № 287/2015 [266], у якому, серед загроз національній безпеці України, визначено «загрози безпеці критичної інфраструктури» [266]. Також, відповідно до нової Стратегії національної безпеки України «Безпека людини – безпека країни» [265], серед поточних та прогнозованих загроз національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов визначено «посилення загроз для критичної інфраструктури, пов'язаних із погіршенням її технічного стану, відсутністю інвестицій в її оновлення та розвиток, несанкціонованим втручанням у її функціонування, зокрема фізичного і кіберхарактеру, триваючими бойовими діями, а також тимчасовою окупацією частини території України» [265]. Наступним кроком стало проведення низки експертних засідань при Національному інституті стратегічних досліджень у складі вітчизняних та зарубіжних експертів із країн-членів НАТО. У результаті цього було підготовлено проєкт «Зеленої книги з питань захисту критичної інфраструктури в України» [169], остаточний текст якої було оприлюднено на сайті Інституту на початку жовтня 2015 р.. В документі зазначається, що «критична інфраструктура України – це системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до

найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки» [79, с 15].

Інституційно в Україні дефініцію «критичної інфраструктури» вперше було визначено текстом Постанови КМУ №563 від 23.08.2016р. «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» [210]. Згідно даної інституції, критична інфраструктура визначалась як «сукупність об'єктів інфраструктури, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних фінансових збитків та людських жертв» [210]. Далі розпорядженням КМУ № 1009-р від 06.12.2017 р. «Про схвалення Концепції створення державної системи захисту критичної інфраструктури» [230] зміст даного поняття було звужено та викладено як «сукупність об'єктів, які є стратегічно важливими для економіки й безпеки держави, суспільства, населення та порушення функціонування яких може завдати шкоди життєво важливим національним інтересам України» [230].

Аналізуючи наукові погляди на визначення сутності та значення критичної інфраструктури, варто актуалізувати також думку О. П. Єрменчука, який тлумачить даний предикат як «систему надзвичайно важливих матеріальних та нематеріальних об'єктів національної інфраструктури, а також систему і активи, будь то фізичні або віртуальні, що забезпечують її стале функціонування, настільки життєво важливі для країни, що недієздатність, руйнація або пошкодження яких (наявними загрозами) може призвести до людських жертв і значних матеріальних збитків з найсерйознішими негативними наслідками для життєдіяльності суспільства, соціально-економічного розвитку країни та національної безпеки» [46, с. 138]. Аналізуючи дане судження, солідарні із думко Д. С. Бірюкова, який

вважає що таке визначення «є актуальним виходячи з пріоритету надання функцій та послуг життєво необхідних для суспільства, людини та держави» [8, с.160]. Однак, зауважимо, що наведене теоретизування не враховує та взаємовплив між окремими елементами критичної інфраструктури, на якому наголошувалось раніше. Саме ця особливість, на наш погляд, обумовлює масштабність та системність наслідків у формі «каскадного ефекту» функціонування системи критичної інфраструктури. Нашу позицію підтримує С. М.Чумаченко, наголошуючи, що «множинність елементів критичної інфраструктури об'єднана зв'язками різної природи і володіє загальною властивістю, відмінною від властивостей окремих елементів цієї сукупності» [279, с.43].

Аналізуючи приведені судження учених та положення нормативних актів, можна узагальнити ще одну ключову особливість об'єктів критичної інфраструктури – їх приналежність до національної інфраструктури, що є взаємопов'язаною системою державного управління та об'єктів інфраструктури, які гарантують безперебійне функціонування різних сфер держави її економіки та суспільства. Цю думку також підтримує О. П. Єрменчук, наголошуючи, що «критична інфраструктура формується на базі існуючих інфраструктур держави шляхом виділення в них життєво важливих для держави систем і активів» [46, с. 139]. Такі системи визначені у ст. 1 Закону України «Про основи національної безпеки України» [67]. Тому, можна стверджувати, що при формуванні державної політики у сфері захисту критичної інфраструктури її положення слід обґрунтовувати на основі положень національного законодавства у сфері захисту критичної інфраструктури а також національної безпеки й оборони.

Підсумок інституційної полеміки щодо нормативного врегулювання поняття «критична інфраструктура» підвів Президент, підписанням Закону України «Про критичну інфраструктуру» [60], який прийняла Верховна Рада 16.02.2021р. Формулювання у новому нормативно-правовому акті є максимально простим: «критична інфраструктура це – сукупність об'єктів

критичної інфраструктури», а під об'єктами критичної інфраструктури законотворці розуміють «системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам» [60]. Проте, варто відзначити, що український варіант Закону подає зміст даного предикату крізь призму технократичного підходу, що ставить в авангарді економіку. Це, на наш погляд, суперечить ст. 3 Конституції, де найвищою соціальною цінністю проголошується «життя, здоров'я, честь і гідність, а також недоторканність і безпека людини» [99]. Проаналізовані вище теоретизування такої важливої категорії, як критична інфраструктура охарактеризуємо фрагментарністю їх змістовно-сутнісного наповнення та не комплексним відображенням його характерних ознак. Відповідно семантичне структурування термінології яка стосується національної безпеки варто формулювати відповідно до антропоцентричного та гуманітарного підходів. Отже, варто акцентувати увагу на інтегруванні до неї об'єктів, без яких або з порушенням їх діяльності у державі можуть виникнути невідворотні негативні процеси у результаті яких буде завдано збитків громадянам, їх життю, здоров'ю та соціально-економічній ситуації [244].

Аналіз наукових доробків учених а також врахування закордонного досвіду теоретизування предикату «критична інфраструктура», дає підстави ініціювати авторське бачення змістовного наповнення даного терміну що буде відповідати принципам системності, множинності галузей, пріоритетної тріади людина-суспільство-держава, цілеспрямованості, відповідності антропоцентричного аспекту.

Так критичну інфраструктуру пропонуємо розуміти як «множинність розташованих в межах території країни функціонально пов'язаних елементів національної інфраструктури чи їх частини у вигляді фізичних, організаційних інформаційно-комунікаційних структур (незалежно від форми власності), технологій, активів, засобів, систем, мереж, поставок, процесів та

фахівців які ними управляють, які є вирішальними для забезпечення державою життєво важливих для суспільства функцій (здоров'я, захищеності, соціально-економічного благополуччя громадян, забезпечення суверенітету та сталого розвитку країни) порушення функціонування, знищення, збій або дисфункція у роботі яких матиме критичний вплив на здатність влади забезпечувати вказані функції та може спричинити виникнення людських жертв, значних матеріальних та екологічних збитків, інших драматичних наслідків та призведе до суттєвого порушення національної безпеки й оборони» [284]. Отже, авторське бачення у приведеному формулюванні дозволяє акцентувати приналежність критичних об'єктів до національної інфраструктури, а надання її складовим життєво важливих характеристик, свідчить про існування загроз до виникнення кризових ситуацій у національній безпеці.

Віднесення об'єктів до категорії критичної інфраструктури проводиться за сукупністю критеріїв, що імлікують їх важливість для надання критично-важливих послуг та виконання життєво важливих функцій, а також визначають тривалість робіт для ліквідації таких наслідків до відновлення штатного режиму роботи. До таких критеріїв належать:

– виконання функцій по забезпеченню національних життєво-важливих інтересів;

– наявність специфічних загроз, щодо об'єктів критичної інфраструктури;

– ризики руйнування нормальних умов життєдіяльності населення;

– ступінь вразливості об'єктів критичної інфраструктури та складність потенційних наслідків для здоров'я населення, соціальної сфери, економіки, природного середовища, обороноздатності та іміджу держави;

– масштабність негативних наслідків для держави, які вплинуть на діяльність життєзабезпечувальних об'єктів стратегічних секторів або призведуть до втрати національно значущих унікальних систем, активів чи ресурсів, що носитимуть пролонгований вплив на діяльність інших секторів

держави;

– терміни ліквідації деструктивних наслідків та період пролонгованої дії негативного впливу на функціонування інших секторів держави;

– каскадний вплив на суміжні сектори критичної інфраструктури [60].

Враховуючи результати проведених досліджень, зазначимо, що державна політика у сфері захисту критичної інфраструктури ґрунтується на наступних постулатах:

1) атрибуція потреби гарантування стійкості та безпеки об’єктів критичної інфраструктури;

2) встановлення законодавчих принципів та вимог до стратегічних пріоритетів захисту критичної інфраструктури;

3) ідентифікація суб’єктів національної системи захисту критичної інфраструктури, їх засад відповідальності повноважень та порядку взаємодії;

4) формування умов та здійснення заходів зі зниження ризиків, контролю загроз та ліквідацію наслідків кризових ситуацій на об’єктах;

5) створення системи раннього розпізнавання загроз критичній інфраструктурі;

6) розвиток державно-приватного партнерства, у напрямку інтеракції приватних суб’єктів господарювання та населення у питаннях захисту критичної інфраструктури;

7) підтримка міжнародного співробітництва напрямку стійкості об’єктів критичної інфраструктури;

8) створення кон’юнктури для оперативної регенерації можливостей надання життєво-важливих послуг функцій та у разі реалізації загрозу разі дизфункції об’єктів критичної інфраструктури.

Отже, державна політика у сфері захисту критичної інфраструктури орієнтована на формування комплексу інституційно-правових організаційних, ресурсних, інженерно-технічних, інформаційно-аналітичних та методологічних заходів, націлених на забезпечення безпеки об’єктів критичної інфраструктури.

Серед найбільш істотних в Україні проблемних питань державного регулювання сегменту захисту критичної інфраструктури варто зазначити тривалу інституційну невизначеність на загальнодержавному рівні у змістовному розумінні та узгодженості системи захисту та реагування на надзвичайні ситуації у критичній інфраструктурі. Також пролонгована розбалансованість нормативно-правової бази, яка б регламентувала повноваження відповідних органів державної влади у цій сфері. Додамо, що система нормативно-правових актів паралельно оперує термінами «критична інфраструктура», «національна інфраструктура», «критично важливі об'єкти інфраструктури» та «життєво важлива інфраструктура», а це за певних обставин може спровокувати протиріччя, або інституційну невизначеність.

Слід відзначити атрибутивність об'єктів критичної інфраструктури до структури національної інфраструктури. Дане припущення робить критичну інфраструктуру визначальним у функціонуванні економіки та суспільства у векторі сталого розвитку держави в цілому. Аналіз законодавчих ініціатив різних країн світу у ідентифікації термінології «критична інфраструктура» дає підстави наголосити про наявність у структурі змістовного наповнення даної дефініції пріоритетної тріади «людина-суспільство-держава». Дане твердження ілюструє особливо важливі для забезпечення національної суспільної безпеки об'єкти національної інфраструктури. Таким чином варто резюмувати, що інфраструктура в міру своєї культурної значимості та ролі у створенні відчуття національної ідентичності може нести символічну критичність, втрата якої може емоційно дестабілізувати суспільство нації та психологічно мати на нього тривалий деструктивний вплив.

1.2. Теоретико-методичні засади забезпечення захисту критичної інфраструктури.

У процесі гарантування державою сталого життєзабезпечення та безпеки суспільства, особливу увагу привертає процес мінімізації вразливості критично важливих систем, що детермінує актуальність квестії наукового обґрунтування векторів державної політики у сфері захисту об'єктів критичної інфраструктури. У продовженні даної наукової думки, звернемо увагу на запропоноване ученими С. В. Бєлай, І. В. Євтушенко, В. В. Мацюк припущення, що «державна політика у сфері захисту критичної інфраструктури повинна бути спрямована на формування комплексу організаційних, нормативно-правових, інженерно-технічних, експлуатаційних, наукових та інших заходів, що сприяють забезпеченню безпеки та стійкості критичної інфраструктури» [5, с.344]. Отже, дослідження проблематики державної політики у сфері захисту критичної інфраструктури держави, вимагає окреслення спектру небезпек, наявність яких обумовлює таку потребу. Звернемо увагу на Європейську програму захисту критичної інфраструктури [292], у якій члени Комісії європейських спільнот акцентують увагу на ключових загрозах, як можуть пошкодити, знищити або порушити функціональність об'єктів критичної інфраструктури. Серед таких небезпек відзначаються «терористичні акти, стихійні лиха, недбалість, професійна нещасні випадки, хакерські атаки, злочинна діяльність та зловмисна поведінка» [292]. Отже, можна стверджувати, що вектор державної політики Уряду має бути сфокусовано на забезпеченні безперебійної роботи критичної інфраструктури з метою захисту життя, здоров'я та майна свого народу, від загроз порушення її функціонування. У даному контексті забезпечення безпеки об'єктів критичної інфраструктури за рахунок інфраструктурної адаптивності та керованості пропонуємо розглядати у якості невід'ємної складової парадигми державного управління. Вважаємо, що для цього потрібна політика «експлуатаційної ефективності» – прагматизації розподілу та застосування державних безпекових ресурсів з

метою локалізації та нейтралізації потенційних джерел небезпеки. Варто сфокусувати увагу не стільки на продуктивності окремих їх елементів, а більше на стратегії міжсистемної та міжсекторальної комунікації [293].

Акцентуємо увагу на обґрунтуванні комплексу загроз для критичної інфраструктури. Відзначимо, що з початку 90-х років XX ст. учені Європи та США у різних галузях науки, розпочали активне дослідження такого поняття як «захист критичної інфраструктури», що на сьогодні пролонгується у наукових дослідженнях та нормативних актах різних держав. Процес захисту, як відомо, полягає у протидії загрозам. Аналізуючи вітчизняне законодавство, дефініцію «загроза» можемо знайти у діючому Законі України «Про національну безпеки України» де трактується як «явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України» [62]. Під «загрозою» в контексті захисту критичної інфраструктури Д. Г. Бобро пропонує розуміти «наявні та потенційно можливі явища та чинники, що створюють небезпеку сталому функціонуванню об'єктів критичної інфраструктури та можуть призвести до негативних наслідків» [11, с.85]. Дане формулювання вважаємо цілком об'єктивним, оскільки акцент передбачено саме на стійкості об'єктів. Це підтверджують розробники Зеленої книги захисту критичної інфраструктури ЄС, подаючи майже ідентичне формулювання загроз критичній інфраструктурі як «будь-яких обставин або подій, що можуть порушити стале функціонування або знищити критичну інфраструктуру чи будь-який її елемент а також будь-які спроби та наміри завдання шкоди критичним активам» [292, с. 55]. Даного змістовного вектору притримується також О. П.Єременчук, пропонуючи під загрозами об'єктам критичної інфраструктури розглядати «наявні або потенційно можливі явища і чинники, що можуть нанести шкоду такому об'єкту (фізичному або у кіберпросторі), вивести його з ладу або порушити стійкість функціонування відповідно до призначення, чим створюють небезпеку життєво важливим

національним інтересам України» [48, с. 108]. Отже, підтримуючи позиції європейських експертів та вітчизняних учених у напрямку вивчення державної політики захисту критичної інфраструктури, пріоритетом у даній діяльності вважаємо забезпечення стійкості функціональної спроможності таких об'єктів.

На думку більшості науковців [1, с. 55], [2, с. 512], [5, с 343] першими у обґрунтуванні та впровадженні концепції критичної інфраструктури та її захисту є США. Ця країна продовжує зберігати свої лідерські позиції у цій сфері завдяки застосуванню ефективних державно управлінських підходів, удосконаленню інформаційно-аналітичної підтримки процесу прийняття рішень, використанню новітніх технологій та активному поширенню різноманітних форм і методів забезпечення захисту критичної інфраструктури. Отже, узагальнюючи проаналізовані визначення можна прослідкувати точку наукового фокусу на видах загроз і ризиків, які здатні дестабілізувати роботу критичної інфраструктури на різних ієрархічних рівнях. Нормативно-правова база США конкретизує спектр загроз критичній інфраструктурі у межах сфер їх походження як «природні або техногенні явища, фізичних осіб, суб'єктів чи дії, що містять або несуть потенційну шкоду для життя, інформації, операцій, навколишнього середовища та/або власності» [46, с.137]. З огляду на це, в умовах сучасного динамічного макросередовища, яке генерує комплекс загроз, небезпек і викликів для державної безпекової політики України, об'єктивно посилюється роль державних інститутів у напрямку їх виявлення, прогнозування й нейтралізації. Деталізований список таких загроз у вітчизняній нормативній базі можемо зустріти у тексті Стратегії національної безпеки України 2020 року [256]. Аналізуючи ст. 19 Закону України «Про національну безпеку» [62] та ст. 24 Закону України «Про критичну інфраструктуру» [180], можна узагальнити спектр основних загроз об'єктам критичної інфраструктури: воєнні загрози, розвідувально-підривна діяльність, тероризм, кіберзагрози, економічні загрози, викрадення державної таємниці, надзвичайні ситуації,

аварії та технічні збої, кризові ситуації. Д. М. Павлов пропонує доповнити цей перелік гібридними війнами, сепаратизмом, техногенним тероризмом та ворожою колаборцією [180, с.147].

Акцентуємо також увагу на необхідності урахування сучасних обставин військового стану в Україні при розробці державної стратегії захисту критичної інфраструктури. У даному випадку, аналіз випадків пошкодження функціонування об'єктів критичної інфраструктури під час ведення війни учені виділяють дві основні групи:

1) умисні дії суб'єкта, націлені на порушення спроможності об'єкта інфраструктури виконувати свої функції;

2) дії без чіткого наміру, де порушення функціонування об'єктів інфраструктури, що є своєрідним випадковим наслідком збройного конфлікту, наприклад, неточність військових ударів під час бойових дій.

За ступенем руйнівного впливу загрози військового часу для критичної інфраструктури П. П. Богуцький виділяє наступні:

– припинення функціональності об'єктів, зокрема внаслідок фізичного захоплення, для завдання збитків попередньому власнику чи обміну на «потенційні» переваги в інших сферах;

– фізична окупація об'єктів при збереженні їх функціональності;

– розукомплектування окремих частин інфраструктури з метою отримання вигоди від їх перепродажу;

– перешкоджання діяльності з відновлення критичної інфраструктури та регенерації функціональності об'єктів;

– фізичне руйнування об'єкта для нанесення непоправних збитків у вигляді збільшення витрат противника на переборення стану порушення функціонування інфраструктури, так і формування суспільно-політичного невдоволення населення країни [15, с. 280].

Уразливість критичної інфраструктури до гібридних загроз учені [1, с. 242] виокремлюють наступні:

– намагання показати слабкість влади, яка не в змозі забезпечити

належні умови життєдіяльності людей;

– спричинення психоемоційного тиску на населення та уряд;

– економічної шкоди від руйнування та окупації інфраструктури;

– пошкодження інфраструктури шляхом наступальних дій, артилерійських ударів, або ураження за рахунок атаки безпілотних літальних апаратів по критично-важливим об'єктам;

– кібератаки (держава-агресор виступає ініціатором зловмисних дій проти інфраструктури);

– конспірованих диверсій з використанням кримінальних дій та актів тероризму.

Отже, дестабілізація у роботі інфраструктури життєзабезпечення та умисний саботаж у виконанні нею свої функції стає інструментом сучасної гібридної війни, орієнтованим на психологічну дестабілізацію населення та здійснення політичного тиску на уряд країни. Фідбеком до визначених загроз критичним об'єктам має стати інституціалізація гарантій їх безпеки. Нам імпонує позиція вітчизняних учених [100, с.18], які, аналізуючи предикат «безпеки», звертають увагу на філософський спектр даної категорії. Дану наукову ініціативу можна пояснити тим, що поняттю безпеки підпорядковано всі належні аспекти життєдіяльності людини, соціуму та держави. Перші відомі трактування інтенції «безпека» почали вживати ще в XII столітті та зустрічалися у працях грецьких і римських науковців-філософів Платона, Епікура, Арістотеля, Ціцерона та Лукреція у проекції філософської, політичної та юридичної думки. Окрім цього наукові доробки Ціцерона та Лукреція, відіграли вагому роль у еволюції поняття безпеки на рівні індивіда, держави та народу. Безпека трактувалася мислителями як спокійний стан духу людини, котра вважала себе захищеною від будь-якої небезпеки [321, с.54]. В українському «Політологічному енциклопедичному словнику» безпеку розтлумачили як «діяльність людей, суспільства, держави, світового співтовариства народів щодо виявлення (вивчення), запобігання, послаблення, усунення (ліквідації) і відвернення загрози, здатної згубити їх,

позбавити матеріальних і духовних цінностей, завдати невідшкодованих збитків, заблокувати шляхи для прогресивного розвитку» [189, с.47]. У сучасній науці триває полеміка відносно визначення безпеки, яке б задовольнило як вітчизняних, так і зарубіжних науковців. Здебільшого, при вивченні контекстних факторів безпеки учені фокусують увагу на трьох аспектах:

– концептуальному – поєднання онтологічних і епістемологічних базисів безпеки;

– практичному – ендемічність безпеки у якості базової потреби індивіда;

– ціннісному – гносеологічний підхід та культура безпеки.

Зауважимо, що при визначенні поняття «безпека» більшість науковців аргументують поняття безпеки як еклектичного стану захищеності, ліквідації загроз та пролонгованого комплексу безпекових заходів [100]. Прислухаємось до переконання польського дослідника А. Д. Родфельда, який пояснює це тим, що воно є значно ширшим та окремі складові безпеки динамічно еволюціонують, набуваючи певного значення або втрачаючи його, залежно від внутрішньої ситуації в державі та міжнародної обстановки [345, с.15]. Це явище пояснює М. Гладиш, аналізуючи питання глобальної безпеки. Він зазначає, що її стан не обов'язково мусить збігатися з відчуттям безпеки конкретної держави, а концепція безпеки окремої держави часто суперечить іншим чи, навіть, може порушувати безпеку регіону чи світу [25, с.30]. Це підтверджує і Б. Посен, наголошуючи, що «…те, що здається доречним для оборони однієї держави, буде здаватися, і часто так є, агресивним по відношенню до її сусідів» [337, с. 18].

Вітчизняні науковці визначають захист критичної інфраструктури як «комплекс заходів, реалізований у нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури» [79, с.11]. Позицію пріоритетності стійкості у захисті критичної інфраструктури підтримує також у своїх

доробках С. С. Теленик [258, с. 183].

Аналізуючи зміст забезпечення безпеки критичної інфраструктури на основі закордонної практики, заслуговує на увагу текст Директиви Президента США з питань національної безпеки, у якому «захист критичної інфраструктури» визначено, як «зменшення ризику критичної інфраструктури від втручання, атак або ефектів, спричинених природними катастрофами або людською діяльністю, за рахунок реалізації заходів із фізичного захисту або кіберзахисту» [300]. Даним формулюванням актуалізовано необхідність протидії кіберзагрозам. Слушною вважаємо також думку О. П. Єременчука, який до захисту критичної інфраструктури додає «систему скоординованих організаційних, нормативно-правових, адміністративних, пошукових, охоронних, режимних інженерно-технічних, наукових та інших заходів, матеріальних та нематеріальних засобів, спрямованих на забезпечення стійкості та безпеки критичної інфраструктури» [46, с. 37].

Офіційне визначення захисту критичної інфраструктури презентує новий Закон «Про критичну інфраструктуру» [60], де законотворці його трактують як «усі види діяльності, що виконуються перед або під час створення, функціонування, відновлення і реорганізації об’єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об’єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації [62]. Дане трактування вважаємо обгрунтованим, однак не досить вичерпним. Помітно, що у всіх проаналізованих формулюваннях провідну роль у захисті критичних об’єктів надано державі в особі уповноважених нею органів. Однак, варто зауважити, що значна, а подекуди й основна частина об’єктів критичної інфраструктури знаходиться у приватній власності. Окрім цього, упущено необхідність забезпечення стійкості об’єктів у виконанні ними своїх функцій. У такому випадку, захист критичної інфраструктури варто пов’язати із забезпеченням міжвідомчої координації, що обумовлюватиме необхідність розширення

кола відповідальних за межі державних інститутів. Аргументуємо свою позицію текстом Національної стратегії безпеки критичної інфраструктури Канади у якій підкреслюється, що «головна відповідальність за підвищення стійкості та швидкості регенерації критичної інфраструктури залишається за її власниками та операторами» [313, с. 8]. Отже, на основі приведеної гіпотези, пропонуємо авторське формулювання дефініції «захист критичної інфраструктури» – «цілеспрямована синхронізована спільна діяльність державних інститутів, власників, операторів а також стейкхолдерів об'єктів критичної інфраструктури із застосування комплексу заходів, спрямованих на забезпечення стійкості, профілактику, запобігання, своєчасне виявлення потенційних і нейтралізацію реальних загроз, мінімізацію та ліквідацію наслідків і швидке відновлення функціональної спроможності критичної інфраструктури у разі її пошкодження, що реалізовуються з метою уникнення людських жертв, значних матеріальних та екологічних збитків, або інших деструктивних наслідків які можуть призвести до порушення національної безпеки» [283]. Фактично дане тлумачення змінює фокус уваги державної безпекової політики із процесу безпосереднього захисту на розробку комплексу превентивних заходів орієнтованих на попередження евентуальних деструктивних ситуацій на об'єктах критичної інфраструктури, а також збалансовує відповідальність між власниками та операторами критичних об'єктів і державою.

Варто звернути увагу, що в українському законодавстві в лиці держави, тривалий час був відсутній єдиний інститут, відповідальний за державну політику у сфері захисту критичної інфраструктури. Фрагментарно протекцією критичних об'єктів займаються складові сектору безпеки, зокрема, Міністерство оборони України, Державна служба надзвичайних ситуацій (ДСНС), Служба безпеки України (СБУ), Міністерство закордонних справ (МЗС), Міністерство охорони здоров'я (МОЗ), які нині мають певні структури реагування та моніторингу: Ситуаційний центр Головного командного пункту Збройних сил України, Ситуаційний центр

ДСНС, Антитерористичний центр СБУ (координація органів виконавчої влади з попередження та припинення терористичних актів) тощо, проте координація їх дій та ресурсів викликає багато запитань. Окремі повноваження також належать системам боротьби з тероризмом, правоохоронних органів цивільного захисту, регулювання енергетики та енергоринку, кібербезпеки та ін. Аналізуючи успішну іноземну практику, заслуговує досвід США, де захист відповідних критичних секторів лежить у площині відповідальності спеціальних галузевих інститутів, серед яких департаменти внутрішньої безпеки, енергетики, продовольства, сільського господарства, охорони здоров'я, а також берегова охорона, управління безпеки транспорту та ін. [256, с.362]. Отже, серед пріоритетних дилем забезпечення ефективної державної політики захисту критичної інфраструктури слід передбачити необхідність затвердження та удосконалення нормативно-правових актів з питань державної системи захисту таких об'єктів у напрямку посилення стійкості та превентивних дій. Варто зазначити, що кожен стратегічний інститут держави, в рамках своєї профільної діяльності фіксує певний спектр загроз для підпорядкованих йому об'єктів і володіє відповідним набором ресурсів та інструментів для забезпечення захисту цих об'єктів у мирний час та в умовах військового стану. Продовжуючи дану думку, прислухаємось до твердження вчених Д. С. Бірюкова та С. І. Кондратова [9, с. 110], що заявлений інститут захисту об'єктів критичної інфраструктури при виконанні своїх повноважень має опиратися на результати аналітичного процесу до якого науковці пропонують включити:

– ідентифікацію областей та секторів критичної інфраструктури на національному, регіональному та локальному рівнях;

– ідентифікацію релевантних ризиків для секторів критичної інфраструктури;

– аналізу уразливості окремих секторів критичної інфраструктури;

– оцінки ризиків порушення або знищення секторів критичної

інфраструктури;

– прийняття відповідних запобіжних заходів, тобто в створенні системи захисту критичної інфраструктури.

Узагальнимо, що значення державного стратегічного інституту захисту об'єктів критичної інфраструктури полягає у тому, що:

– об'єкти критичної інфраструктури становлять визначальну роль для життєдіяльності суспільства і держави в мирний час та особливо в умовах військового стану;

– критична інфраструктура є інструментом у геополітичній боротьбі;

– критичні об'єкти належать до об'єктів підвищеної небезпеки як загальнодержавного, так і світового масштабу.

Аналіз всебічних наукових поглядів, дозволив дійти висновку, щодо важливості визначення та попередження ризиків в управлінні безпекою критичної інфраструктури. Загалом цей підхід передбачає виконання на рівні держави відповідних завдань, найбільш важливим із яких є визначення відповідних заходів та їх включення у документи державного планування. Фінальною місією при цьому є унеможливлення виникнення нових і зниження існуючих ризиків шляхом реалізації комплексних заходів на загальнодержавному, регіональному та місцевому рівнях з урахуванням таких пріоритетів, як розуміння спектру ризиків, вдосконалення інституційно-правових рамок управління ризиками, інвестування в заходи з мінімізації ризиків, зміцнення потенціалу протидії ризикам.

Обґрунтуємо даний тезис дослідженнями колективу авторів на чолі із С. І. Азаровим, які розвиток будь якої надзвичайної ситуації на об'єктах критичної інфраструктури розподіляють на чотири стадії:

1) Накопичення факторів ризику – відбувається у самому джерелі ризику та може тривати кілька діб, місяці, роки, десятиліття та більш тривалі періоди;

2) Ініціація надзвичайної ситуації – представляє собою удар, спусковий механізм у результаті чого, фактори ризику досягають стану неповернення і

стає вже неможливо стримати їх емерджентні прояви;

3) Процес перебігу надзвичайної ситуації – відбувається звільнення факторів ризику (енергії чи речовини) і починається їх вплив на природу, суспільство та об’єкти;

4) Стадія затухання – хронологічно охоплює відрізок часу від стримування джерела небезпеки (локалізації деструктивних факторів), до повного усунення її прямих і непрямих наслідків [1, с. 276].

Розкриємо дефінітивну функцію у державній політиці захисту критичної інфраструктури терміну «ризик». Дане поняття можна охарактеризувати як атрибут наукового апарату багатьох технічних, економічних, суспільних і природних наук. Відповідно у визначенні міри ризику в безпеці критичної інфраструктури варто виділяти соціальні, професійні, екологічні, техногенні, військові та інші небезпеки. Таким чином, ризик «міра цілком певних небезпек» [104, с. 5].

Під ризиком варто розуміти спрогнозовану ймовірність або частоту виникнення небезпек певного класу, або ж обсяг потенційного збитку (втрат, шкоди) від одіозної події, або ж певну комбінацію цих величин. Звернемо увагу на думку вчених В. В. Вітлінського, та Г. І. Великоіваненко, які ризик трактують як «ситуацію, у якій домінує невизначеність, конфлікт, наявна багатоваріантність, і коли одночасно не всі альтернативні варіанти однаковою мірою сприятливі» [22, с. 68]. Дану позицію підтримує Л. І. Донець, пов’язуючи її з подоланням аморфності ситуації потреби вибору управлінського рішення, у процесі якого є можливість кількісно і якісно розрахувати ймовірність отримання очікуваного результату, невдачі, або відхилення від мети [42, с. 212]. І. М. Посохов визначає ризик як невід’ємну умову для здійснення дій з імовірнісними несприятливими наслідками, що виражається в можливості отримання негативного або небажаного результату [190, с. 105]. Отже проаналізувавши ряд трактувань поняття ризику в управлінні безпекою критичної інфраструктури можемо розкрити його як імовірність виникнення нещасного випадку, небезпеки, аварії або катастрофи

у роботі об’єктів критичної інфраструктури за певних обставин, управління якими відбувається в умовах невизначеності та прогнозування альтернативних варіантів.

У процесі аналізу ризиків і розробки протоколу технологічної безпеки пильну увагу приділяють системності обліку та вивчення диференційованих факторів, що впливають на показники ризику, іменованого аналізом ризику. Аналіз ризику або ризик-аналіз учені визначають як – процес ідентифікації небезпек і оцінки ризику для окремих осіб, груп населення, критичних об’єктів та інших об’єктів [237, с. 123]. Отже, проаналізувавши ряд трактувань поняття ризику в управлінні безпекою критичної інфраструктури, можемо розтлумачити його як імовірність виникнення небезпеки, аварії, надзвичайної ситуації або катастрофи під час виконання об’єктами критичної інфраструктури своїх функціональних обов’язків, управління якими здійснюється в умовах невизначеності та необхідності прогнозування множини альтернативних варіантів розвитку ситуації [285, с. 125].

Різноманіття специфіки діяльності критичної інфраструктури та приналежності її об’єктів до самих різних сфер ілюструє багатовекторність в управлінні безпекою проблеми аналізу ризиків. Особливість критичного ризик-аналізу визначимо у тому, що розглядаються потенційно негативні ефекти, що виникають внаслідок дампів або збоїв технічних систем, або дизфункції у роботі обслуговуючого персоналу. Результати аналізу ризиків чинять суттєвий вплив на раціональність та обґрунтованість управлінських рішень стосовно проєктування і локації критичних об’єктів. Таким чином це актуалізує питання управління ризиками або ризик-менеджменту. Вважаємо доцільним приділити окрему увагу питанню управлінню критичними ризиками, як головної складової у державній політиці забезпечення безпеки критичної інфраструктури. Розділяємо думку В. О. Мусієнко, який тлумачить ризик-менеджмент як «процес прийняття та виконання управлінських рішень, які спрямовані на зниження ступеня ймовірності виникнення результату несприятливого характеру та мінімізацію можливих втрат, які викликані його реалізацією» [118, с. 102]. Погодимось також із точкою зору

вчених Н. С. Скопенко, І. В. Євсєєва-Северина [237, с. 125], які переконують у необхідності інтеграції ризик-менеджменту у охорону критичної інфраструктури. У даному випадку вчені приділяють увагу не тільки пошуку можливих шляхів зменшення ризиків, а й їх профілактиці, тобто розробці запобіжних заходів щодо уникнення майбутніх ризиків, оперативного реагування на різні види загроз для забезпечення об'єктів критичної інфраструктури та стабільного функціонування у довгостроковій перспективі. Прислухаємось також до пропозиції учених С. П. Потеряйко, К. Г. Бєлікова, О. С. Твердохліба які пропонують долучити до системи управління ризиками такі механізми: правовий, організаційний, структурно-функціональний та механізм прогнозування [221, с. 44]. Особливої уваги на нашу думку вимагає саме механізм прогнозування, який учені трактують як «сукупність взаємопов'язаних норм, заходів, засобів, методів, важелів, способів, за допомогою яких органи управління здійснюють аналіз функціонування структур сфери безпеки загалом та єдиної державної системи цивільного захисту, зокрема, задля передбачення їхньої дієвості та прийняття обґрунтованих рішень, що забезпечують досягнення мети їх дій у коротко-, середньо- та довгостроковій перспективах [221, с. 45].

Отже, вважаємо доцільним розглядати критичний ризик-менеджмент у якості складової частини державної політики у сфері захисту критичної інфраструктури. Цей процес варто визначити як спектр заходів, націлених на мінімізацію рівня потенційних небезпек, загрожуючих стабільності роботи об'єктів критичної інфраструктури, зменшення потенційних критичних ризиків та інших негативних наслідків. По суті, мова йде про попередження виникнення надзвичайних ситуацій на об'єктах критично-важливої інфраструктури, а також планування заходів по їх локалізації та мінімізації деструктивних наслідків при їх настанні. Оскільки, як зазначалося вище, управління ризиками у захисті критичної інфраструктури реалізовується в умовах невизначеності, у основу варто покласти економічний і соціальний аналіз, законодавчу базу, та методи прогнозування під час оцінки ризику.

Поле державного управління ризиком для критичної інфраструктури має

справу з аналізом альтернатив на основі оцінки ризику, аналізу ризику та прогнозування наслідків для мінімізації ризику. Тобто, даний процес передбачає реалізацію багатокритеріальних задач передуючих прийняттю рішення в умовах невизначеності. Оцінка ризиків є магістральною віссю дослідження і розробки заходів управління ризиком відповідно до алгоритму дій. У свою чергу це потребує створення алгоритму, що дозволить змоделювати аварійний процес і в подальшому дозволить персоналу адаптуватись в реальному житті.

Для опису ризикової ситуації як просторово-часового процесу для критично важливого об'єкту, учені І. Г. Фадєєва О. І. Гринюк пропонують використовувати три критерії:

– чітку ідентифікацію події, яка детермінує формування критичної загрози;

– вірогідність настання даної події;

– ступінь мінімізації деструктивних наслідків від її настання [273, с. 215].

Методологічну складову даної ідеї, можемо описати наступним алгоритмом, на основі послідовності ряду завдань:

Перше завдання – опис поведінки систем.

Друге завдання – пояснення поведінки.

Третє завдання – передбачення поведінки.

Четверте завдання – управління поведінкою.

П'яте завдання – створення систем з певною «поведінкою» [1, с. 230].

Подібна схема, на нашу думку, оптимально підходить для забезпечення подальшого наукового обґрунтування заходів із забезпечення захисту критичної інфраструктури через механізми адміністративно-правового регулювання в умовах невизначеності. Дану позицію обґрунтуємо думкою ученого О.О. Терещенко, який наголошує, що проблеми у сфері захисту критичної інфраструктури створюють не ризики як такі, а їх неконтрольованість [260], яка виникає у зв'язку з дефіцитом інформації та з

часовим лагом в діях управлінців різних ланок. Вчений також стверджує, що контрольованість ризиків забезпечується в результаті запровадження внутрішнього аудиту та системи ризик-менеджменту [260]. Доречною у даному випадку вважаємо також пропозицію Гончара М. Ф., який зазначає, що в умовах нормальних неістотних відхилень в сфері державної політики захисту критичної інфраструктури доцільно розглядати ризик-менеджмент (практика в умовах позитивних і негативних відхилень, які потребують реагування) та стрес-менеджмент (реалізується в умовах екстремальних, критичних негативних відхилень від очікуваної траєкторії розвитку критичного об'єкту) [30].

Прислухаємось до теорії учених О. Є. Кузміна, О. Г. Мельника та М. Є. Адамів, які стверджують, що при критичному зростанні дефіциту часових та інформаційних ресурсів для формування обґрунтованих управлінських рішень, значно інтенсифікується загроза неадекватного реагування на зміни умов діяльності критичних об'єктів. Виходом із такої ситуації вчені вбачають інтеграцію антисипативного управління, орієнтованого на прогнозування імовірних ризиків мікро- та макросередовища [103, с. 73]. Антисипативне управління націлено на забезпечення підготовки об'єктів критичної інфраструктури до будь-яких потенційно-дистабілізуючих подій, які можуть призвести до аномальних та екстремальних відхилень в їх діяльності. Тому вважаємо, що в таких умовах надзвичайно актуальним є застосування проактивного підходу до управління ризиками діяльності підприємств з метою недопущення настання критичних станів складної відкритої системи, що можуть перерости в кризові явища.

Акцентуємо також увагу, що характерними рисами державного управління безпекою об'єктів критичної інфраструктури в сучасних умовах є значимість інформаційного забезпечення прогнозування ризикових подій у середньо- та довгостроковій перспективі, а також брак часу на роздуми у прийнятті поточних управлінських рішень. Серед найпоширеніших підходів, що використовуються для оцінювання та прогнозування ризиків та кризових ситуацій, учені виділяють такі :

– скринінговий підхід на базі лінійних дискримінантних функцій;

– підходи з використанням нечіткої логіки та нейронних мереж;

– імовірнісний підхід, що базується на моделях множинного вибору;

– моделі інтегральної оцінки, які будуються на основі факторного аналізу, метода таксономічного показника розвитку, адитивної чи мультиплікативної згортки [89, с. 90].

Неповнота або відсутність статистичної інформації про розвиток ризиків та загроз для об'єктів критичної інфраструктури обмежує використання формалізованих моделей, заснованих на певних обмеженнях чи припущеннях. Опираючись на дослідження учених можна стверджувати, що для подібних задач, які не піддаються строгій формалізації і мають логіко-аналітичний характер (у нашому випадку – управління безпекою критичної інфраструктури) доцільно використовувати нечітку логіку як засіб моделювання в умовах невизначеності та стратифікації управлінських моделей. Теорію нечіткої логіки в технічних системах досліджували С. В. Козловський [92], О. В. Кочетков, Т. О. Гаур, В. М. Машін [100], А. В. Матвійчук [115] та інші. Моделювання на базі теорії нечіткої логіки передбачає поетапне розв'язання таких задач: виокремлення основних факторів впливу, які характеризують стійкість критичної інфраструктури, і формалізація взаємозв'язків між ними в узагальненому вигляді; визначення і формалізація лінгвістичних оцінок факторів, оптимізація параметрів нечіткої моделі [115, с. 185].

На практиці в багатьох випадках прийняття рішень відбувається в таких умовах, коли цілі, обмеження та наслідки можливих дій точно невідомі. Для операцій з неточно відомими величинами застосовується апарат теорії ймовірності, а також методи теорії прийняття рішень, теорії управління та теорії інформації. Тобто оперативний працівник інтуїтивно приймає припущення, певну неточність, яка незалежно від її природи може бути ототожнена з випадковістю.

Доречною вважаємо інтерпретацію моделі нечіткої логіки вченим

С. І. Ніколаюком, згідно якої працівник здійснює нечіткий кластерний аналіз (де кластерізація – розбивка множини даних та знань на підмножини (кластери) на основі певного функціонала (умови розбивки). Багатофакторний склад надзвичайних ситуацій, значне число об'єктивних та суб'єктивних факторів, які впливають на зміст і характер цих факторів, у своїх сполученнях утворюють велику кількість варіантів, що відрізняються один від одного [136, с. 285]. Тобто, при створенні алгоритму працівник критичного об'єкту буде виконувати аналіз вихідної ситуації, порівнюючи її з переліком раніше розроблених критеріальних факторів, які за змістом є ознаками ситуації. Таким чином, алгоритмізація можлива у конкретних ситуаціях, відносно незмінних у невеликий проміжок часу і з невеликим об'ємом значимої вихідної інформації і, по можливості, виключення випадкових (непередбачуваних) факторів, а формалізовані висновки алгоритму відповідають всім варіантам можливих вихідних даних ситуації – тобто спостерігається випадковість певних дій.

Учені Л. В. Дранишников та Є. О. Сугаль досліджували концепцію прийнятного ризику, яка визначає, що досягнути забезпечення абсолютної безпеки об'єктів критичної інфраструктури неможливо, тому необхідно домогтися їх відносної безпеки за рахунок введення так званого аварійно допустимого ризику, та доведення його до прийнятно-допустимого рівня. Такий рівень ризику, учені пояснюють прийнятністю для тієї чи іншої діяльності, виходячи з економічних, технологічних чи соціальних наслідків, відповідно принципам ризик-менеджменту, які мають бути сформульовані відповідно до державної політики захисту критичної інфраструктури. Сучасні методики управління ризиками для аналізу кожного виду ризику використовують ймовірність реалізації загроз і збиток від негативних наслідків, але реально оцінити ймовірність реалізації загроз і ступінь шкоди, що завдається, важко [43, с. 64]. У контексті наведеного вище, актуалізуємо дослідження В. В. Гордіної, яка пропонує доповнити систему управління ризиками ризик-контролінгом, основною метою якого є інформаційно-аналітична підтримка ризик-менеджменту для комплексного управління

ризиками [31, с. 33] (рис. 1.3.).

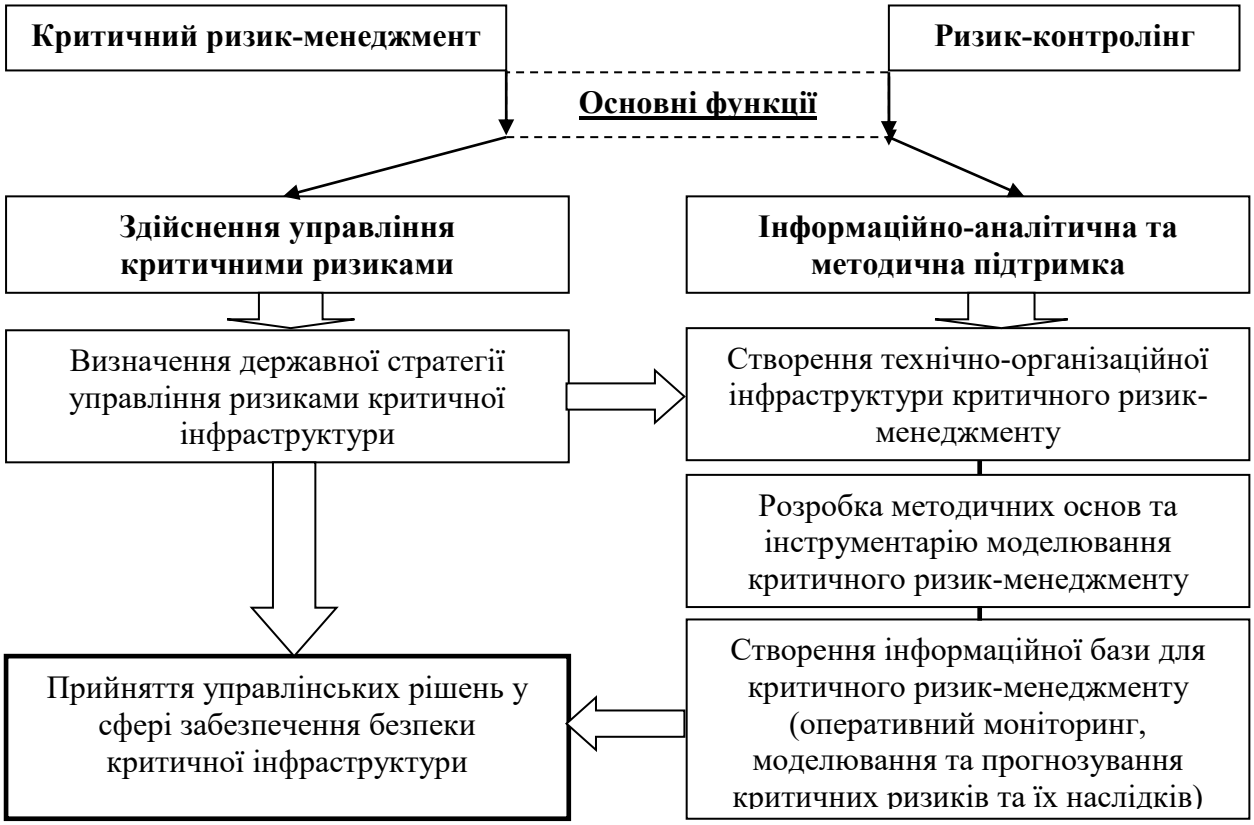


Рис. 1.3. Механізм прийняття управлінських рішень у сфері забезпечення безпеки критичної інфраструктури на основі критичного ризик-менеджменту

Джерело: сформовано автором з використанням [31],[273]

До головних завдань ризик-контролінгу вчена відносить:

– прогнозування ризиків, визначення цільових значень показників;

– контроль ризиків;

– підготовку звітності про стан ризиків об’єктів критичної інфраструктури та надання інформації в керівні підрозділи;

– формування системи ідентифікування, аналізування та оцінювання ризиків;

– координування різних фаз процесу управління ризиками всередині та між окремими елементами системи управління;

– консалтинг з питань, які стосуються управління ризиками [31, с. 33].

З метою забезпечення коректного проведення оцінювання та прогнозування ризиків, що є першочерговим завданням системи ризик-

контролінгу, І. Г. Фадєєва запропонувала каскадну нечітку модель Мамдані-типу оцінювання та прогнозування ймовірності настання ризиків у діяльності нафтогазовидобувних підприємств, яку описано у її публікації [305, с. 260]. Суттєвою перевагою даної моделі є встановлення зв'язків між вхідними та вихідними змінними, що є неявними та за своєю природою нелінійними**.**

Виникнення ризиків у роботі критичної інфраструктури можливе за наявності причин (процесів, явищ), які сприяють його виникненню. Такі явища І. Г. Фадєєва називає як ризикоутворюючі фактори.

Таблиця 1.1.

Характеристика ризиків для об'єктів критичної інфраструктури

Вид ризику	Опис ризику
Ризики зниження ефективності захисту	Потенційна можливість зниження ефективності захисту об'єктів критичної інфраструктури
Ризики виникнення потенційних загроз	Можливість виникнення потенційних загроз для об'єктів критичної інфраструктури
Ризики нанесення збитків	Можливість нанесення потенційних збитків для об'єктів критичної інфраструктури або порушення умов їх нормального функціонування

Джерело: сформовано на основі [98]

Для отримання висновків пропонується кілька алгоритмів в системах нечіткого умовиводу, опис яких заснований на структуруванні висхідного процесу на ряд послідовних етапів:

1. Створення бази даних регламентів нечіткого висновку.
2. Фазис вхідних змінних.
3. Синтез підумов нечітких умов та правил дії.
4. Композиція та активізація підвисновків.
5. Акумулювання висновків нечіткої умови.
6. Декомпозиція вихідних змінних.

Вчені О. В. Кочетков, Т. О. Гаур, В. М. Машін визначають оцінку ризиків як «процес, протягом якого виконується визначення збитків або збитку в кількісному або якісному вираженні» [98, с 99]. Всезростаючі складність та невизначеність зовнішнього середовища, його турбулентний, динамічний та важкопрогнозований характер зумовлюють необхідність

використання сучасних моделей менеджменту і, зокрема, моделей стратегічного планування, які мають забезпечувати на основі глибокого та всебічного аналізу зовнішнього оточення й внутрішнього середовища підприємства розроблення стратегії розвитку та її ефективну реалізацію. Визначальним етапом цього процесу є формування місії та стратегічних цілей об'єктів критичної інфраструктури. Ця процедура є досить складною, неструктурованою та трудомісткою й потребує ґрунтовних фахових знань, експертних міркувань та оцінок, які мають «розмитий», нечіткий характер. Забезпечення ефективності виконання цього етапу великою мірою визначає успішність подальшої роботи з розроблення державної політики захисту критичної інфраструктури та її реалізацію. Сьогодні гостро постала дилема отримання, концентрації та обробки актуальних даних, оскільки об'єкти критичної інфраструктури характеризуються просторовою розосередженістю. Тому, для оперативного управління має сенс застосовувати геоінформаційні системи і технології, що дозволить проаналізувати просторове розташування об'єктів з урахуванням впливу на стан об'єкту зовні та взаємодії процесів, які відбуваються у середині об'єкту. Ефективні методи та засоби для моделювання складних систем і процесів при недостатніх та невизначених знаннях про систему надає нечітке моделювання, орієнтоване на знання методи та моделі, як продукційні моделі, семантичні мережі, фрейми, формальні логічні моделі.

1.3. Сучасні наукові парадигми формування державної політики у сфері захисту критичної інфраструктури.

Сучасна ера розвитку суспільства характеризується безліччю масштабних катастроф у вигляді природних катаклізмів, цунамі, землетрусів, повеней, виверження вулканів, терористичних актів, техногенних аварій, військових конфліктів, кібератак та ін.. Такі умови підіймають на новий рівень потреби сучасного суспільства у захисті й готовності протидіяти таким негативним подіям, а також відновлюватися після них. З метою

гарантування зазначених напрямків державної політики, Уряду варто сфокусувати особливу увагу на розробці заходів зі зниження вразливості важливих систем економіки, екології та соціального життєзабезпечення суспільства. Іншими словами – захистити сферу критичної інфраструктури як складову національної безпеки. Погодимося із науковим переконанням П. П. Богуцького, що національна безпека знаходить відображення у свідомості як стан захищеності національних інтересів від потенційних і реальних загроз, серед яких воєнні загрози є найбільш небезпечними [16, с. 10]. Варто зазначити, що сучасні військові загрози в Україні породжують небезпеку для територіальної цілісності та суверенітету держави. Окрім цього, ескалація таких загроз становить небезпеку для життєдіяльності людини, що унеможливлює нейтральний дискурс, у якому інші наслідки воєнної діяльності могли б розглядатися в одному вимірі з небезпекою для життя людини, а в глобальному значенні – для людства. Відтак, аналіз сучасних наукових парадигм формування державної політики у сфері захисту критичної інфраструктури є вкрай важливим. Це дозволить забезпечити наукову складову обґрунтування концептуальних положень захисту критичної інфраструктури у складі державної політики національної безпеки. Відзначимо, що у даному напрямку наука із розгалуженістю її світоглядних моделей мають має передувати практичній частині реалізації державної політики захисту.

Для осмислення логіки та наукового обґрунтування стрижневих компонентів державної політики у сфері захисту критичної інфраструктури в Україні, інспірованих радикальними змінами безпекового середовища та породженням нових стратегічних загроз, ми обрали дефінітивну конструкцію «парадигма», запропоновану Томасом Куном. Дане теоретизування також актуалізовували у своїх наукових доробках Р. К. Мертон [324, с. 28] та Ф. М. Рудич [233, с. 68]. Обґрунтуємо релевантність наукової інтерпретації даного конструкту в площину дослідження державної політики у сфері захисту критичної інфраструктури, опираючись на судження М. Цюрупи,

який наголошує, що парадигма дає можливість мобілізувати у єдиний теоретичній конструкт конкретні гіпотези та відповідей на поставлені питання. Тобто, у нашому випадку це дасть можливість сформувати надійний інструмент наукового дослідження важливих векторів формування та удосконалення державної безпекової політики на принципах наукового скептицизму та організованого наукового колективізму висловлених положень [277, с. 124].

Особливу увагу варто приділити вкрай важливій сфері – аналізу сучасних наукових парадигм формування державної політики у сфері захисту критичної інфраструктури. Від ідентифікації успішної науково-обгрунтованої парадигми захисту критичної інфраструктури буде залежати ефективність формування та реалізації державної політики у цьому напрямку. За основу даного процесу встановимо завдання з узагальнення існуючих наукових поглядів на дослідження основ державної політики у сфері захисту критичної інфраструктури, що на основі наукового пізнання надасть фундамент для генерації власних пропозицій із удосконалення даної сфери.

Аналізуючи теорію формування наукових парадигм, відзначимо, що її засновником вважається Томас Кун, який довів, що рушійною силою розвитку науки є людина, яка утворює наукове співтовариство, а не щось, закладене в саму логіку розвитку науки. Розвиток знання вчений визначає зміною наявних парадигм, а не простим підсумовуванням знань, тобто відбуваються не тільки (і не стільки) кількісні, а й якісні зміни в структурі наукових знань. Розвиток науки, на думку Куна, відбувається за принципом чергування періодів «нормальної» і «революційної» науки, а не шляхом накопичення знань і приєднання їх до вже наявних [322, с. 188]. Отже, наукові парадигми змінюються залежно від їх зрілості, ступеня застосування математичного апарату, техніки експерименту та наукових традицій конкретної дисципліни.

У класичній філософії інтенцію «парадигма» тлумачиться як «вихідна

концептуальна схема, модель постановки проблем і їх вирішення, методів дослідження, що панують протягом певного історичного періоду» [238, с. 427]. Науковий термін «парадигма» у наш час найчастіше ототожнюється із означеннями «теорія», «концепція», «доктрина», «модель», «уявлення», «система поглядів». У більш загальному вигляді парадигма – це те, як ми «бачимо» інші події, ситуації, майбутнє, коли говоримо про управління в смислі розумового сприйняття, розуміння, тлумачення.

Посилаючись на наукові напрацювання Томаса Куна, вкажемо на дві характерні риси, які мають бути властиві парадигмі формування державної політики у сфері захисту критичної інфраструктури:

– по-перше, створення парадигми повинно бути безпрецедентним, щоб залучити на довгий час вчених із конкурентних напрямів наукових досліджень;

– по-друге, ця парадигма має бути достатньо відкритою, щоб нові покоління вчених могли знайти в їх змісті нерозв'язні проблеми [322, с. 145].

Узагальнення обох наведених підходів надає можливість до основних якостей парадигми формування державної політики у сфері захисту критичної інфраструктури віднести: багатоплановість, фундаментальність, конкретність, певний ступінь усталеності, здатність віддзеркалювати сутнісні характеристики відповідних об'єктів і процесів, відтворюваність, системність, суб'єктність, прийнятність для більшості вчених, дієвість, мультиплікативність із ступенем розвитку суспільства та об'єктивністю реальності, орієнтація на світоглядні принципи, спроможність еволюціонувати до нової парадигми, що з'являються у результаті суттєвих змін в науці. Тому все більшої актуальності набувають сучасні дослідження окремих аспектів захисту критичної інфраструктури, в рамках яких автори здебільшого зорієнтовані на бачення усіх складових критичної інфраструктури в контексті певної системи.

Для розуміння основних трендів у зміні безпекових пріоритетів, необхідно проаналізувати парадигму національного безпекознавства.

Аналізуючи історичні факти, варто згадати перший приклад обґрунтування безпекової парадигми – американську інтервенцію в зону Панамського каналу у 1904 році. Для обґрунтування важливості даного процесу для національних інтересів США, президент Т. Рузвельт оперував терміном «національна безпека». У даному сенсі сутність парадигми національної безпеки науковці визначають станом, при якому надійно захищено життєво важливі політичні, економічні, соціальні, екологічні, духовні, військові та інші інтереси країни (нації) [250, с. 288]. Науковці звертають увагу, що парадигма безпеки у повоєнні роки (1945-1954 рр.) обмежувалась лише безпекою військовою, в епоху біполярного світу (1954-1991 рр.) носила оборонний характер, в епоху пост біполярного світу (1991-11 вересня 2001 року) характеризується розширенням розуміння феномена безпеки, куди окрім військової, включено інформаційну, екологічну, економічну, соціальну та ін. [111, с. 180]. Парадигма формування державної політики у сфері захисту критичної інфраструктури сьогодні набуває системного характеру, що обумовлює сучасний етап розвитку поліполярного світу в умовах експресивного розвитку інформаційних технологій і комунікаційних засобів. У таких умовах безпека стає основоположною не лише потребою, а й цінністю людини та навколишнього середовища, або іншими словами – умовою подальшого існування антропо-соціо-культурного середовища. Як справедливо зазначає А. Д. Пілько, сучасна безпекознавча парадигма, з одного боку – «це стиль наукового мислення та підходу до безпеки з позиції державницьких реалій, концепцій, стратегій, доктрин, програм і технологій» [188, с. 334]. З іншого – це підхід до безпекотворення з позиції реалізації у них ідеї безпеки, починаючи від конкретного громадянина і закінчуючи глобальними корпораціями. Отже, аналізуючи зазначені вище позиції вчених, можна аргументувати необхідність обґрунтування нової парадигми державної політики у сфері захисту критичної інфраструктури як складової безпеки. Зауважимо, на неоднозначність у розумінні сутності безпеки критичної інфраструктури, яка породжує певну змістовну дуальність у

розумінні даного явища. Можемо виділити два основні підходи: так, якщо під безпекою розуміти «стан захищеності» об'єктів критичної інфраструктури, то забезпечення безпеки будується навколо критичних загроз, від яких необхідно захищатися. Якщо ж сфера безпеки критичної інфраструктури ототожнюється з відсутністю загроз або небезпек, то забезпечення безпеки набуває характер нейтралізації (усунення) джерел (носіїв) небезпек, тобто ризиків [111, с. 185]. Відповідно до цього, показниками безпеки будуть показники, які характеризують рівень захищеності в широкому розумінні слова інтересів територіальних громад регіону, або ж обсяги ресурсів, необхідних для ефективної нейтралізації або усунення впливу джерел (носіїв) небезпек для об'єктів критичної інфраструктури. В. А. Ліпкан виділяє чотири підходи до трактування поняття «безпека»: статистичного (безпека як стан захищеності від ризиків), апофатичного (безпека як відсутність загроз і небезпек), діяльнісного (система заходів, спрямованих на створення певних безпечних умов), пасивного (дотримання певних параметрів та норм, від забезпечення яких безпосередньо залежить безпека) [110, с.345]. В. М. Пасічник при забезпечені безпеки основну увагу приділяє проблемі захисту життя та умов, від яких це життя залежить, беручи до уваги теорію потреб А. Маслоу. Безпеку, згідно з ієрархією людських потреб, можна розглядати як потребу людини у впевненості, стабільності життя, захисту від того, що може йому зашкодити [182]. Учений також акцентує увагу на необхідності зміни традиційної парадигми безпеки за якої державна політика передбачає забезпечення безпеки у час коли вже реально виникла загроза чи небезпека. Образно – це політика «звернення до лікаря під час загострення хвороби». Натомість новітня парадигма державної політики безпеки критичної інфраструктури вимагає проведення «профілактичних обстежень» та виявлення потенційної «хвороби» на ранніх стадіях та проведення заходів профілактики загострення. Тобто, вчений робить наголос на необхідності боротьби не з наслідками, а з причинами виникнення загроз безпеки

критичної інфраструктури. Можна також погодитися з думкою В. Ліпкана, який вважає, що нова парадигма безпеки повинна включати в себе: «символічні узагальнення (аксіоми, теореми, закони, визначення ядра концептів націобезпекознавства); метафізичні елементи, які задають спосіб бачення системи національної безпеки та її антропологію, онтологію, гносеологію й аксіологію; консенсуальні патерни - алгоритми вирішення конкретних завдань, що забезпечують існування націобезпекознавства» [110, с. 234]. Сердцевиною нової парадигми має бути розуміння безпеки як категорії, пов'язаної з філософською категорією буття, усвідомлення її ключового значення для трактування функції держави, формування й реалізації державної політики та здійснення державного управління. Р. Валіхновський [17, с. 245] також актуальним завданням вважає необхідність розробки теоретико-методологічних засад державної політики безпеки Україні, які б ґрунтувалися на принципово новій моделі гуманітарної парадигми цивілізаційного розвитку. Мова йде про модель, яка має бути побудована у світлі сучасного соціального знання щодо причин, наслідків, взаємозв'язку та взаємообумовленості світоглядно-ціннісних, політичних, економічних, соціальних, техногенних, екологічних та інших криз і кризових явищ різного рівня, які, на думку переважної частини фахівців, експертів та аналітиків, мають тенденцію щодо загострення в сучасних умовах глобалізації.

В контексті безпекознавства, під парадигмою будемо розуміти сукупність теоретичних і методологічних передумов, які визначають конкретний напрям наукового дослідження, який втілюється на визначеному етапі історичного розвитку. Парадигма є підставою вибору наукових задач, а також моделлю і зразком для вирішення дослідницьких завдань Певна модель соціальної системи породжує відповідні уявлення про безпеку, які у міру досягнення суспільного визнання отримують парадигмальну форму існування. Враховуючи, що будь-яка діяльність, у тому числі й у сфері безпеки, здійснюється людьми та ґрунтується на певних уявленнях, то зміст

тієї або іншої системи забезпечення безпеки слід розуміти в контексті пануючої моделі стереотипної поведінки або парадигми безпеки, тобто сталого зразка розуміння і вирішення теоретичних і практичних питань забезпечення безпеки. Професор Г.Ситник [236, с. 27] звертає увагу на необхідності формування єдиної загальнонаукової парадигми, орієнтованої на дослідження квестій державно-управлінських аспектів забезпечення національної безпеки, яку він називає «класичною». В її основу вчений вкладає твердження, яке набуло обрисів канонічної дослідницької моделі: національна безпека є інтегральною характеристикою безпеки людини, безпеки суспільства та державної безпеки, а її оптимальний рівень залежить від дотримання в процесі державного управління певної прийнятної тріади складових: «можливостей держави до управління», «національних інтересів» та «небезпеки щодо виникнення загроз». Тому політика національної безпеки формується з використанням результатів, отриманих за допомогою вказаної моделі, а її пріоритетом, як правило, є побудова системи національної безпеки, яка б гарантувала створення належних умов для підтримки бажаного рівня захищеності національних інтересів, забезпечення цілісності об’єктивно диференційованого суспільства, нейтралізацію небезпеки здатності держави відстоювати вказані інтереси.

Парадигми управління безпекою С. А. Мушникова розглядає як фундаментальні закони і поняття; «метафізичні компоненти», критерії, відповідність яким необхідна для сприйняття пояснень фактів як «наукових» [119, с. 132]. Тобто, парадигмальний зміст управління безпекою полягає у мультивимірності цього процесу. Дане явище учена пояснює обґрунтуванням трансдисциплінарної безпекової парадигми, яка за своєю суттю передбачає науково-філософську платформу для підтвердження гіпотез дослідження, створення підстав для формування комунікативних управлінських практик взаємодії залучених до досліджень соціальних агентів. Проєктуючи тези запропонованої парадигми у площину наукового дослідження алгоритму формування державної політики у сфері захисту

критичної інфраструктури, узагальнимо базові постулати безпекової трансдисциплінарної парадигми:

– ліквідація потенційних протиріч у будь-яких наукових тлумаченнях предикату захисту критичної інфраструктури;

– міждисциплінарний фідбек між системами знань у процесі наукової транспозиції у формі колективних робіт учених різних галузей у дослідженнях перспектив удосконалення державної політики у сфері захисту критичної інфраструктури;

– розгляд варіантів процесу формування державної політики захисту критичної інфраструктури поза формалізованими рамками (наприклад у інноваційних формах міжсекторальної взаємодії);

– інтеграція принципу наукового пізнання, що передбачає інтеракцію у науковому плюралізмі при комплексному вирішенні проблем забезпечення безпеки критичної інфраструктури.

Автори багатьох досліджень зазначають, що трансдисциплінарна парадигма є всеохоплюючою, оскільки поєднує різні фрагменти реальності в єдину картину. Трансдисциплінарна парадигма не протиставляє, а об'єднує за принципом додатковості те, що розглядалося як протилежне. Трансдисциплінарна парадигма намагається зрозуміти реальність в її складності, а це саме та установка, яка властива синергетиці [134, с. 144]. Отже, трансдисциплінарну парадигму управління безпекою критичної інфраструктури, як інтеграцію та диференціацію наук різних областей знання для дослідження одного й того ж об'єкта, С. А. Мушникова [120, с. 448] пропонує розглядати у вигляді трикутника, вершинами якого є: філософія – для пізнання трансформацій законів світу; інтеграційний комплекс соціально-гуманітарних наук (соціологія, політологія, психологія та ін.) – для пізнання трансформаційних законів суспільства, які дають уявлення про розвиток соціальних комунікаційних відносин у суспільстві під впливом трансформаційних змін буття; управління (менеджмент) – для наукового обґрунтування прийняття управлінських рішень. Таким чином,

спостерігається всеохоплення принципів, методів, підходів різних «вершин» трикутника трансдисциплінарної парадигми та формування нового міждисциплінарного інструментарію управління безпекою критичної інфраструктури. Проілюструємо зміст даної парадигми на рис. 1.4.

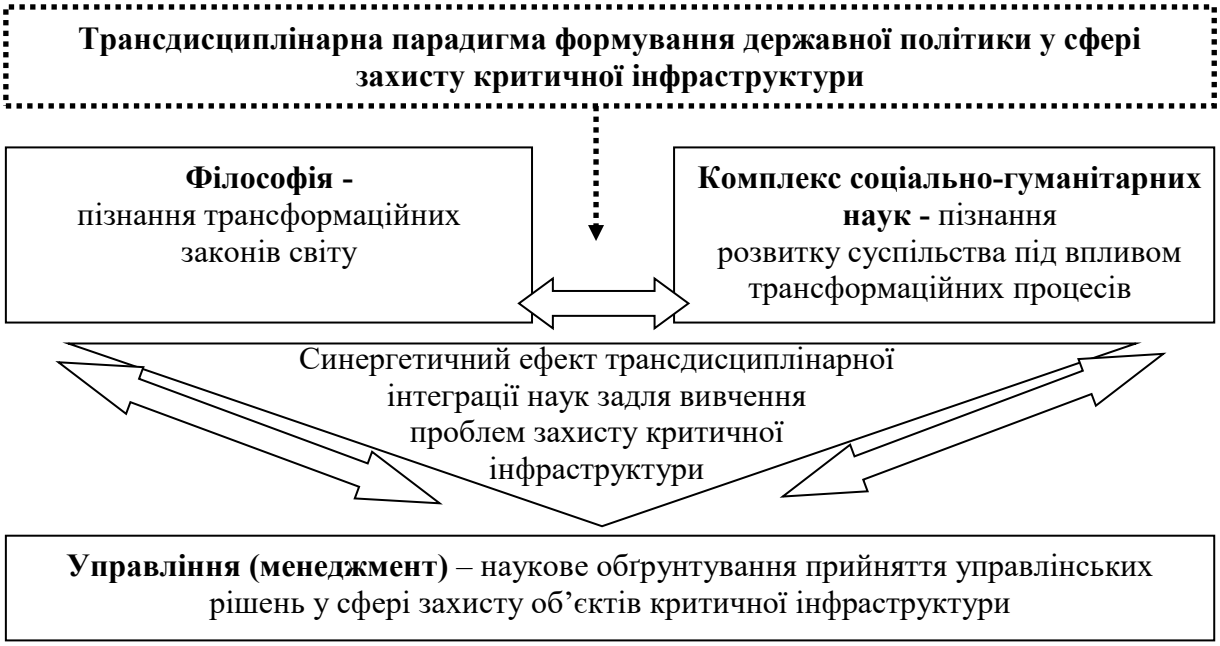


Рис 1.4. Трансдисциплінарна парадигма управління у сфері захисту критичної інфраструктури

Джерело: узагальнено автором з використанням [119], [120]

Трансдисциплінарна безпекова парадигма може стати комунікативним каналом, який забезпечує оптимальну конфігурацію соціо-гуманітарних, філософських та управлінських інструментів для пенетрації їх інноваційних продуктів та технологій у систему державного управління у сфері захисту критичної інфраструктури. В подальшому це передбачає еволюцію нового типу керівника, котрий володітиме трансдисциплінарною ідеологією у поєднанні з якостями ученого щодо здатності розрізняти і вирішувати багатоаспектні квестії у процесі функціонування критичної інфраструктури, володіти знаннями своєї профільної дисципліни, працювати в спільних проєктах, що є ознакою трансдисциплінарних досліджень [120, с. 449].

Перехресною інтерпретацією трансдисциплінарної безпекової парадигми С. А. Мушникова пропонує розглядати поліпарадигмальну

модель управління безпекою, яка доповнює попередню джерелами (дослідницькими парадигмами) (рис. 1.5.).

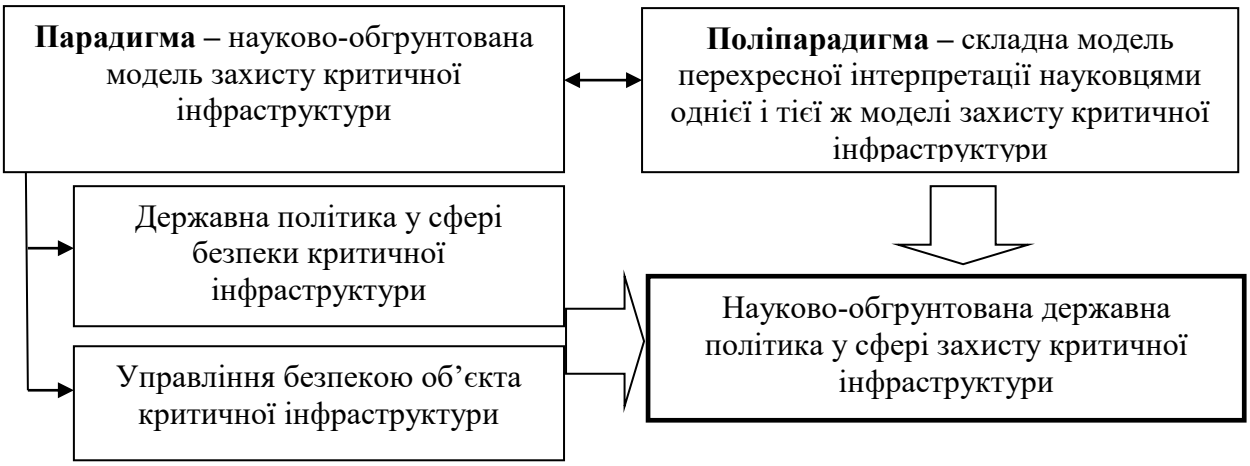


Рис. 1.5. Формування поліпарадигмальної моделі формування державна політики у сфері захисту критичної інфраструктури

Джерело: узагальнено автором з використанням [119], [120]

Вважаємо доречним розглянути можливість інтеграції зазначених наукових парадигм у сферу політики державного управління у сфері безпеки критичної інфраструктури, що дозволить, по-перше – врахувати диференційованість наукових поглядів на дане питання, а по-друге – сприятиме більш повному та різнобічному відпрацюванню безпекових заходів. При цьому, С. А. Мушникова підкреслює, що поліпарадигмальна модель не є новою парадигмою, чи інноваційною системністю, а забезпечує комплексний підхід до наукового обґрунтування управлінських рішень [120, с. 450].

Дане судження вважаємо прецедентом для більш детального вивчення та відпрацювання ідеї відносно інтеграції трансдисциплінарної парадигми та поліпарадигмальної моделі ієрархії стратегій управління у процес формування та реалізації державної політики забезпечення захисту критичної інфраструктури.

Звернемо увагу на вагомий внесок у вивчення проблематики захисту критичної інфраструктури фахівцями Національного інституту стратегічних досліджень, зокрема у аналітичній доповіді «Організаційні та правові

аспекти забезпечення безпеки і стійкості критичної інфраструктури в Україні» [13]. Зазначимо, що у даному документі значна увага приділяється системам взаємодії та обміну інформацією, підготовки кадрів та наголошується на необхідності переформатування архітектури загальнодержавної мережі інформаційно-аналітичних та ситуаційно-кризових центрів. Також прослідковується пропозиція сформувати аналітичні спільноти як системні та концептуальні центри аналітичних досліджень питань безпеки критичної інфраструктури. Даний тезис актуалізує проаналізовану вище трансдисциплінарну парадигму управління у сфері захисту критичної інфраструктури, що дозволить систематизувати інструментарій моделювання нелінійних системних взаємозв'язків однорідних елементів у межах проаналізованого у попередніх пунктах критичного ризик-менеджменту на основі моделювання нечіткої логіки. Цей комплекс забезпечить фундамент для генерації подальших наукових пропозиції, виходячи із заявленого у роботі об'єкту дослідження, а саме – процесу формування та реалізації державної політики у сфері захисту критичної інфраструктури.

Дану теорію також підтверджує і С. С. Теленик, який пропонуючи інноваційний підхід до вивчення державної системи захисту критичної інфраструктури у якості макросистеми, звертається до застосування принципу міждисциплінарності, опираючись на теорію Урі Бронфенбреннера [352], стосовно розподілу процесів суспільного життєзабезпечення на системи мезо-, екзо- та макро- рівнів [257, с. 223]. Сутність теорії, яка береться за основу, полягає в тому, що макросистема підпорядковує не тільки мікросистему, а й мезо-, ендо- й екзосистеми. Тобто вчений демонструє структурно-організаційну можливість здійснення прямих і зворотних зв'язків, взаємного впливу на результативність складових державної політики безпеки в цілому та безпосередньо – критичної інфраструктури. Врахуємо також переконання професора Г.Ситника [236, с. 28], який наголошує на необхідності здійснити перехід до нової

загальнонаукової парадигми застосування принципів і підходів системно-синергетичного аналізу, які знайшли відображення в так званій цивілізаційній парадигмі дослідження суспільних процесів й передбачають комплексне застосування сучасних принципів та підходів до наукового аналізу. Свою позицію стосовно задоволення потреб у безпеці на усіх рівнях учений аргументує необхідністю врахування низки факторів, які справляють вплив на безпечний розвиток, серед яких:

– стійка тенденція сталого розвитку за якого досягається гармонія екологічних, соціальних, економічних, політичних взаємовідносин;

– необхідність одночасного врахування культурно-історичних особливостей національного розвитку та складових і характеристик міжнародної безпеки;

– суперечливість змін загальнолюдських, національних, групових, особистісних інтересів та ціннісних орієнтацій, а отже, непрогнозованість і невизначеність суспільно-політичних трансформацій, оскільки зміна будь якої підсистеми соціального організму часто викликає спонтанну зміну багатьох його підсистем;

– глобалізація та розвиток інформаційних технологій, які призводять до поширення віртуальних груп за інтересами й знижують здатність держав до ефективного управління.

Отже, можна стверджувати, що зміст поліпарадигмальної моделі формування державної політики у сфері захисту критичної інфраструктури полягає у доповненні ієрархії врахуванням чинників впливу, дії загроз і ризиків. За своєю сутністю у статичному аспекті останні являють собою комбінацію кількох мікросистем. С. С. Теленик у динамічному аспекті протидії пропонує формування інститутів, що створюються з метою виконання спільних проміжних завдань чи функцій. Наприклад, за певних умов, не зважаючи на чітко визначений розподіл функцій, активізується взаємодія Служби безпеки України з МВС України. Внаслідок цього виникає мезосистема окремих правоохоронних органів. З іншого боку, в якості

мезосистеми можна розглядати й окремі сектори критичної інфраструктури, наприклад, сектор водопостачання, залізниці чи енергопостачання, які в свою чергу складаються з ряду мікросистем, що функціонують у відповідній галузі [257, с. 115].

З позицій інституціоналізму державна політика безпеки критичної інфраструктури є досить складною політико-правовою і організаційно-технічною системою, до якої Г. Ситник [236, с. 28] пропонує віднести сукупність суб'єктів забезпечення національної безпеки (органи державної влади та місцевого самоврядування, інститути громадянського суспільства, окремі громадяни, ЗМІ); сукупність інструментів влади (політичних, економічних, воєнних), які можуть бути використані для підтримки належного рівня захищеності (збройні сили, спецслужби, підприємства оборонно-промислового комплексу, дипломатичні засоби, державні та мобілізаційні резерви, інші ресурси, які цілеспрямовано скеровуються на захист); масив чинного національного законодавства, який визначає пріоритети державної політики безпеки; суб'єкти (фізичні та юридичні особи), які породжують загрози та ризики; множина факторів національної безпеки (до вказаних факторів виходячи із загальносистемних принципів дослідження складних систем можна віднести не тільки змінні, зокрема ті, які характеризують тенденції, показники, цілі, а й інші системи, наприклад міжнародні структури безпеки, цілі та наслідки їх діяльності) та відповідно сукупність самих об'єктів критичної інфраструктури.

Зазначимо, що прогресивна парадигма державної політики у сфері захисту об'єктів критичної інфраструктури має бути націлена на забезпечення дієздатності інституційної складової захисту критичної інфраструктури. Цей процес за словами О. П. Єрменчука «потребує відпрацьованого алгоритму необхідних заходів, обов'язкових для кожного об'єкта критичної інфраструктури» [48, с. 87], який за пропозицією вченого має мати наступний склад:

– ідентифікація виду потенційних загроз та їх інтенсивності (природні

явища, технічні збої, недбалість персоналу, злочинні чи терористичні дії);

– оцінка уразливих місць критичного об’єкта;

– аналіз стійкості об’єкта критичної інфраструктури;

– визначення пріоритетних ризиків;

– визначення категорії об’єкта, його рівня захисту (від наявних та потенційних загроз);

– відпрацювання можливих сценаріїв розвитку ситуації залежно від наслідків та загроз;

– формування мети захисту та визначення заходів, необхідних для її досягнення;

– реалізація спільних заходів держави і приватних партнерів;

– на основі аналізу та з урахуванням розвитку ситуації постійне внесення коректив у спільні дії та регулятивні нормативно-правові акти.

Актуальними вважаємо дослідження вчених О. П. Постельжука, Л. І. Валюха, Г. Я. Невинної та Р. Ю. Михальчука, які наголошують, що формування новітньої парадигми захисту критичної інфраструктури, потребує врахування військово економічного та інформаційно-комунікаційного потенціалу російської федерації, у якості стратегічного ворога [220, с. 110]. Думку вченого можемо обґрунтувати тим, що продумана та далекоглядно-прогнозована політика дозволить мінімізувати можливості росії із задіяння таких структур, які проникають у різні управлінські сфери держави, тим самим, системно послаблюючи її. Дані слабкі місця проявились у 2014 році та на початку 2022 року, коли Україні не вдалося захистити свої кордони від проникнення диверсантів та окупаційного вторгнення. Використовуючи різний транснаціональний злочинний елемент, рф направила та скеровувала його на розпалювання національної ворожнечі та руйнацію територіальної цілісності України [220, с. 109]. При цьому окупаційні війська, з метою дестабілізації соціально-економічної та логістичної стабільності, систематично завдавали ударів по об’єктам критичної інфраструктури. Новітню безпекову парадигму вважаємо

доцільним формувати на основі ретельного, лінгвістичного та ідейно-політичного аналізу воєнно-політичних фундаментальних ідей та принципів оборони у доктринах воєнної безпеки України.

Аналізом даних відповідних документів займався у своїх працях М. Цюрупи. Аналізуючи оборонні доктрини незалежної України у період 1993-2021 рф вчений відзначив «стійку миролюбну, оборонну спрямованість, та відсутність тез щодо превентивних дій по відношенню до сусідів, захисту громадян поза межами території». Тобто вчений характеризує Україну як «не агресивну державу» цитуючи американського воєнного соціолога Чарльза Москоса [277, с. 123]. Отже, можемо з упевненістю стверджувати що умови сучасних військових реалій в Україні детермінують критичну необхідність реформування системи захисту критичної інфраструктури у контексті змін парадигми національної безпеки. У даному випадку, актуальною вважаємо пропозицію Д. М. Павлова стосовно максимального залучення до цього процесу не лише органів публічної адміністрації, а й представників громади, що висвітлює перспективи розширення вектору державно-приватного партнерства. Про його ефективність, як одного із головних елементів забезпечення належного рівня безпеки та стійкості критичної інфраструктури свідчить багатий закордонний досвід. Розділяємо також позицію ученого щодо налагодження даного процесу у сфері захисту критичної інфраструктури в Україні, який має стати невід'ємним напрямом забезпечення національної безпеки, оскільки «значна частина об'єктів критичної інфраструктури сьогодні перебуває у приватній власності» [179, с. 72] і «потребує відповідного правового регулювання» [180, с. 146]. Даний тезис також закріплено у Стратегії національної безпеки України «Безпека людини – безпека країни» [265] у переліку основних напрямів зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки, де зазначається, що «держава створить ефективну систему безпеки та стійкості критичної інфраструктури, засновану на чіткому розподілі відповідальності її суб'єктів

та державно-приватному партнерстві».

Слушними у даному випадку вважаємо також теоретичні напрацювання П. П. Богуцького, який для оптимізації державної політики захисту пропонує модель військово-правової парадигми взаємодії громадянського суспільства та сектору безпеки і оборони. Її суть полягає у формуванні на основі конституційних положень певної системи правового забезпечення участі інститутів громадянського суспільства та окремих громадян у діяльності сил оборони, здійсненні контролю за реалізацією силами оборони, оборонно-промисловим комплексом держави повноважень щодо захисту суверенітету, територіальної цілісності України та критичної інфраструктури. Режим відносин взаємодії громадянського суспільства та сектору безпеки і оборони є вкрай складним завданням, проте виключно необхідним для забезпечення національної безпеки та захисту критичної інфраструктури, що стосується, насамперед, діяльності сил оборони у взаємодії з громадянським суспільством, його інститутами та окремими громадянами. Тут важливо виявляти не лише спільне розуміння існуючих проблем, потенційних і реальних критичних загроз та ризиків, але й постійно демонструвати злагодженість у їх подоланні [15, с. 115].

Актуальними у досліджуваному напрямку вважаємо наукові доробки О. М. Суходолі, який стверджує, що основними положеннями парадигми захисту критичної інфраструктури мають стати визначення, аналіз та оцінка ефективності застосування методів та інструментів впливу однієї системи на іншу, а також розробка методів та інструментів запобігання, стримування, нейтралізації або пом’якшення наслідків такого впливу та сприяння посиленню готовності, своєчасного реагування та швидкого відновлення штатного режиму функціонування системи. Серед результатів наукових досліджень ученого прослідковується ідея парадигми «національної стійкості». Визначаючи процеси, що впливають на «національну стійкість», учений формалізує їх через системи критичної інфраструктури, як детермінанти забезпечення національної безпеки і, зокрема, сектору безпеки.

Зокрема визначено сім основоположних тригерів забезпечення національної стійкості: безперервність урядування та надання найважливіших державних послуг; здатність ефективно справлятись з неконтрольованим переміщенням людей; здатність одночасно надавати допомогу значній чисельності людей, що отримали пошкодження; стійкість енергозабезпечення; стійкість водопостачання та продовольчої безпеки; стійкість систем комунікацій; стійкість транспортної системи [251, с. 67].

Учений Г. Ю. Зубко звертає увагу, що сучасні умови динамічних трансформацій і перерозподіл світового ринку супроводжуються прагненнями окремих держав встановити контроль над інфраструктурними системами інших країн [83, с. 38]. Що можна спостерігати у сучасних діях росії. У цьому випадку пролонгуючи парадигму «національної стійкості» у формуванні безпекової політики, погоджуємось із думкою вченого, що, відповідно до такого роду загроз, інфраструктурна політика має розглядатися крізь призму реалізації нової соціально-економічної парадигми сталого розвитку. Дану позицію пропагує також професор Г.Ситник [236, с. 29], який стійку тенденцію сталого розвитку при гармонізації екологічних, соціальних, економічних та політичних взаємовідносин відносить до спектру потреб у безпеці на усіх напрямках національної безпеки.

Термін сталий розвиток, як добре відомо, введений у широкий вжиток Міжнародною комісією по навколишньому середовищу і розвитку (Комісія Брунтланд) у 1987 р. Під сталим розуміють такий розвиток, який «задовольняє потреби нинішнього часу, але не ставить під загрозу здатність майбутніх поколінь задовольняти свої власні потреби» [131, с. 75].

Нам імпонує дослідження учених В. Є. Хаустова та Ш. А. Омарова, котрі дотримуються думки про необхідність вирішення проблеми розвитку з урахуванням потреб і безпеки майбутніх поколінь шляхом зниження виробництва та нульове, або навіть негативне економічне зростання, на відміну від ідеї, що людина повинна відмовитися від комфорту промислової революції, запропонував загальний план дій, який містить основні ідеї

досягнення цього: припинення воєн, що дозволить звільнити величезні продуктивні сили для допомоги бідним країнам; використання з великою відповідальністю не відновлюваних ресурсів та уникнення непотрібних втрат енергії, доки використання сонячної енергії або будь-яких інших альтернативних джерел енергії стане загальноприйнятим процесом; поступове зменшення населення планети до того моменту, коли воно буде годуватися тільки через органічне сільське господарство; економне використання речей, техніки та транспортних засобів у побуті [274, с.269].

Серед офіційно узгоджених ООН Цілей сталого розвитку, які можуть бути дотичними до парадигми розробки державної політики у сфері захисту критичної інфраструктури слід виокремити наступні:

1) створення стійкої інфраструктури, сприяння забезпеченню всеохоплюючої та стійкої індустріалізації і впровадженню інновацій;

2) зниження рівня нерівного доступу до інфраструктурних об’єктів та використання інфраструктурного потенціалу всередині країни;

3) забезпечення раціонального використання об’єктів інфраструктури з метою підтримання органічного балансу між потребами і виробництвом;

4) сприяння неухильному, всеохоплюючому та стійкому зростанню, повної залученості об’єктів інфраструктури для реалізації національних інтересів [172].

Приймаючи до уваги складові парадигми сталого розвитку – економічної, соціальної, екологічної безпеки, концепції сталого розвитку, зміст безпеки критичної інфраструктури вчені А. Д. Пілько, Т. П. Гарда пропонують розглядати:

1) як поняття дещо іншого змісту, ніж поняття сталого розвитку, а саме, як таке, що вказує на межі, в рамках яких можуть варіювати значення як окремих інтегральних показників розвитку модельованих систем, так і параметри взаємокомпенсації впливу чинників безпеки, задля отримання динаміки збалансованого досягнення цілей розвитку територіальної системи;

2) як поняття, яке акцентує увагу на пріоритетності цілей соціального

розвитку в широкому розумінні даного слова перед іншими локальними цілями розвитку суспільства – економічними, військовими, екологічними, цілями науково-технічного прогресу [187, с. 114].

Справедливим можна вважати позицію вчених про те, що відповідні пропозиції щодо урахування парадигми сталого розвитку при формуванні державної політики у сфері захисту критичної інфраструктури, стосовно реалізації механізмів забезпечення економічної, соціальної, екологічної безпеки, повинні ґрунтуватися на відповідному інституційному забезпеченні. Іншими словами, для успішної практичної реалізації ідеальних з точки зору науки рекомендацій, необхідним є існування формальних і неформальних інститутів, котрі є визнаними суспільством. Тобто суспільство та його еліти повинні розділяти і поширювати відповідні цінності розвитку і його безпеки, а не обмежуватися виключно декларуванням відповідних пріоритетів.

За результатами проведених досліджень, погодимось із пропозиціями вітчизняних учених [114, с. 434] щодо векторів модернізації державної політики у сфері захисту критичної інфраструктури за наступними напрямами:

– комплексний підхід до формування нормативно-правової бази із питань забезпечення захисту об’єктів критичної інфраструктури;

– спрямувати зусилля на досягнення узгодженості національного законодавства з нормативними актами ЄС та впровадження чинних в ЄС стандартів захисту критичної інфраструктури, включаючи державно-приватне партнерство;

– створення інституту-координатора державного управління безпекою критичної інфраструктури, на базі якого слід розробити механізм моніторингу інформації щодо стану об’єктів критичної інфраструктури;

– запровадити систему профілактичних заходів, посилення охорони, запровадження заходів самозахисту критичних об’єктів;

– налагодження державно-приватного партнерства та міжнародного співробітництва у сфері захисту критичної інфраструктури.

Варто відзначити, що проведене наукове дослідження дозволило виявити сучасні проблеми державної політики України у сфері захисту критичної інфраструктури, серед яких домінує:

– нормативно-правова неузгодженість суб'єктної конкретизації державного інституту координації захисної політики;

– інституційне забезпечення укріплення стійкості об'єктів критичної інфраструктури до впливу дестабілізаційних факторів мікро- та макросередовища;

– не має єдності політичних та наукових поглядів на створення регіональної моделі захисту населення та територій під час надзвичайних станів різного характеру на об'єктах критичної інфраструктури.

– певні пробіли у механізмах ефективної протидії загрозам стабільності роботи критичних об'єктів, подолання яких потребує узгодженого комплексного підходу.

Реалізація в межах новітньої парадигми формування державної політики у сфері захисту критичної інфраструктури заходів активізації інформаційного моніторингу, паспортизації інфраструктурних об'єктів, міжвідомчої координації охоронної діяльності, налагодження державно-приватного партнерства та міжнародної співпраці дозволить уникнути виникнення надзвичайних ситуацій на об'єктах критичної інфраструктури та забезпечити мінімізацію їх наслідків. Зазначені заходи мають бути чітко визначені й прогнозовані як обов'язковий алгоритм дій для власників та операторів об'єктів критичної інфраструктури та інших учасників. Вважаємо раціональним запропонувати до розгляду можливість закріплення такого алгоритму на загальнодержавному рівні в Україні.

Висновки до розділу 1

1. Розкрито теоретичні підходи до сутності критичної інфраструктури як об'єкту державного управління, у результаті чого визначено, що захист критичної інфраструктури позиціонується складовою частиною забезпечення національної безпеки України, та обґрунтовано приналежність об'єктів критичної інфраструктури до національної інфраструктури. Запропоновано

авторське формулювання дефініції «захист критичної інфраструктури» як цілеспрямованої синхронізованої спільної діяльності державних інститутів, власників, операторів а також стейкхолдерів об’єктів критичної інфраструктури із апропріацією комплексу заходів, націлених на превенцію, своєчасне виявлення потенційних і нейтралізацію реальних загроз, мінімізацію та ліквідацію наслідків і швидке відновлення функціональної спроможності критичної інфраструктури у разі її дизфункції, що реалізовуються з метою уникнення тотальних матеріальних та екологічних збитків, людських жертв, або інших деструктивних наслідків які можуть призвести до порушення національної безпеки. Даним тлумаченням змінено кут уваги від процесу захисту критичної інфраструктури до процесів попередження кризових ситуацій, а також диференційовано відповідальність між державою, власниками, безпосередніми працівниками критичних об’єктів, а також їх стейкхолдерів.

2. Узагальнено розподіл загроз критичній інфраструктурі на основні категорій: надзвичайних ситуацій природного характеру, техногенного характеру, зловмисних дій та комбінованих загроз. Значимість об’єкта критичної інфраструктури категоризовано на основі його ролі у забезпеченні життєво важливих функцій та послуг від яких залежить рівень національної безпеки. Визначено взаємний вплив одного об'єкта на інший у вигляді «каскадного ефекту дестабілізації критичної інфраструктури», коли припинення роботи одного із критичних об’єктів детермінує каскад масштабних наслідків.

3. Проаналізовано світовий досвід, наукові підходи вітчизняних учених, а також іноземні наукові теоретизування дефініції «критична інфраструктура» як множинність функціонально пов’язаних елементів національної інфраструктури розташованих в межах території країни чи їх частини у вигляді фізичних, організаційних, інформаційно-комунікаційних структур (незалежно від форми власності), технологій, активів, засобів, систем, поставок, процесів, мереж та фахівців які ними управляють, що є

вирішальними для забезпечення державою життєво важливих для суспільства функцій (захищеності, здоров'я, соціально-економічного благополуччя громадян, забезпечення суверенітету країни та її сталого розвитку) пошкодження, знищення, або дисфункція у роботі яких матиме критичний вплив на здатність влади забезпечувати вказані функції та може спричинити виникнення людських жертв, значних матеріальних та екологічних збитків, інших драматичних наслідків, що інспірує суттєві ризики порушення національної безпеки й оборони. Даним формулюванням підкреслено приналежність критичної інфраструктури до національної інфраструктури, вплив її на національну безпеку, а також наголошено на ролі фахівців, як детермінанти стабільності надання її елементам життєво важливих послуг, що відповідає принципам системності, цілеспрямованості, множинності галузей та пріоритетної тріади людина-суспільство-держава у відповідності до антропоцентричного аспекту й концепції сталого розвитку.

4. Визначено ключові особливості формування сучасної державної політики у сфері захисту критичної інфраструктури та певні проблемні питання, серед яких стратегічна необхідність орієнтації державної політики на створення комплексу нормативно-правових, інженерно-технічних організаційних, наукових, експлуатаційних та державно-партнерських заходів; урахування при розробці державної стратегії захисту критичної інфраструктури сучасних обставин військового стану в Україні; значний відсоток приватної власності, що обмежує можливості адміністрування державними інститутами сфери захисту критичної інфраструктури; тривала відсутність централізованої інформаційної платформи для накопичення інформації про об'єкти критичної інфраструктури; масштабність суб'єктного складу та наявність дезорганізованих режимів функціонування, процедур і планів реагування на різний комплекс загроз і ризиків у сфері захисту критичної інфраструктури; тривала відсутність на національному рівні затвердженого визначення її змісту, відповідної законодавчої бази та тектологічної системи захисту, що б передбачала урівноваженість у одній

системі активностей, спротивів і реагування на випадок виникнення надзвичайних ситуацій на об’єктах критичної інфраструктури; слабко відпрацьована практика інтерпретації механізму державно-приватного партнерства у сферу захисту критичної інфраструктури.

5. Розкрито змістовне наповнення поняття «ризик» у державній політиці захисту критичної інфраструктури як очікувану частоту або імовірність виникнення певного класу небезпек, або ж розмір можливого збитку (шкоди, втрат) від небажаної події, або будь яку комбінацію цих явищ. У визначенні міри ризику в безпеці критичної інфраструктури виділено соціальні, професійні, екологічні, техногенні, військові та інші небезпеки. Обгрунтовно перспективи інтегрування у сферу державного управління складової ризик-менеджменту, який базується на відпрацюванні альтернатив з використанням результатів оцінки ризиків, аналізу ризиків та прогнозування наслідків для їх мінімізації. Прогнозується, що результати даної діяльності матимуть істотне значення для прийняття обґрунтованих і раціональних рішень під час генерування управлінських рішень у сфері захисту критичної інфраструктури. Критичний ризик-менеджмент розглянуто як спектр заходів, націлених на мінімізацію рівня потенційних небезпек, загрожуючих стабільності роботи об’єктів критичної інфраструктури, зменшення потенційних критичних ризиків та інших негативних наслідків, що фіксує вектор превентивності державної політики щодо виникнення надзвичайних ситуацій на об’єктах критичної інфраструктури та реалізацію запланованих заходів із ліквідації та мінімізації деструктивних наслідків за умов їх виникнення.

6. Промоніторено сучасні наукові парадигми формування державної політики у сфері захисту критичної інфраструктури. Застосування дефінітивної конструкції парадигми дає можливість мобілізувати у монолітний теоретичний конструкт конкретні гіпотези до вирішення поставлених завдань. До основних якостей парадигми віднесено фундаментальність, багатоплановість, конкретність, здатність

віддзеркалювати сутнісні характеристики відповідних об’єктів і процесів, системність, певний ступінь усталеності, суб’єктність, прийнятність для переважної більшості дослідників, взаємозалежність із сучасним рівнем розвитку суспільства та об’єктивною реальністю, відтворюваність, дієвість, орієнтація на світоглядні підходи, здатність трансформуватись в результаті нових наукових результатів. У даному сенсі сутність парадигми контексті безпекознавства розтлумачено як сукупність теоретичних і методологічних передумов, які визначають конкретний напрям наукового дослідження, який втілюється на визначеному етапі історичного розвитку.

7. Проаналізовано класичну модель забезпечення національної безпеки, гуманітарну парадигму цивілізаційного розвитку, в результаті чого встановлено необхідність розвитку державної політики у сфері захисту критичної інфраструктури на основі сучасного соціального знання щодо причин, наслідків, взаємозв'язку та взаємообумовленості світоглядно-ціннісних, політичних, економічних, соціальних, техногенних, екологічних та інших криз і кризових явищ різного рівня, які мають тенденцію до загострення в сучасних умовах глобалізації. Досліджено фундаментальні аспекти парадигми національного безпекознавства та традиційної парадигми безпеки, що лало підстави дійти висновку, що в основу наукового обґрунтування магістральної основи державної політики у сфері захисту критичної інфраструктури варто закласти вектор безпекової трансдисциплінарної парадигми.

8. Аналіз сучасних парадигм державної політики у сфері захисту критичної інфраструктури дало підстави дійти висновку, що від стабільності критичної інфраструктури залежить рівень національної безпеки, тому провадження ефективної державної політики у сфері захисту критичної інфраструктури є одним із її фундаментів. Проведені наукові розвідки мультипліканд зазначеного процесу дає підстави окреслити базові постулати у напрямку гарантування захисту об’єктів критичної інфраструктури, серед яких комплексна модернізація інституційно-правового поля у напрямку

ліквідації рудиментарних елементів та інспірації інноваційного забезпечення захисту критичної інфраструктури, актуалізація трансдисциплінарної та поліпарадигмальної моделі державного управління у даному секторі, іррадація суб'єктного складу захисту критичної інфраструктури та забезпечення їх дієздатності та інституційної спроможності на основі розвитку державно-приватного партнерств шляхом максимального залучення до цього процесу усіх зацікавлених сторін, моніторинг оперативної інформації стосовно загроз критичній інфраструктурі, розвиток прогресивних форм міжсекторальної взаємодії, досягнення узгодженості національного законодавства з нормативними актами ЄС та впровадження чинних в ЄС стандартів захисту критичної інфраструктури.

РОЗДІЛ 2.
АНАЛІЗ СУЧАСНОЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

2.1. Інституційно-правові аспекти реалізації державної політики у сфері захисту критичної інфраструктури.

Процес формування сучасної державної політики у сфері захисту критичної інфраструктури України передбачає еклектичність у напрямку інституціалізації, легітимації та валідності такої політики. Латентність інституційно-правових аспектів адаптації державної політики у сфері захисту критичної інфраструктури до умов воєнного стану потребує методологічного осмислення цього політико-правового феномена у максимально можливих інваріантах. Від цього залежатиме не тільки розуміння сутності інституційно-правових особливостей державної політики у сфері захисту критичної інфраструктури, а й розроблення та удосконалення механізмів її адміністративно-правового регулювання.

Як відомо, усе, що пов’язано з державною політикою виходить від уповноважених державою суб’єктів, насамперед її органів влади. Таким чином, обов’язковою ознакою державної політики варто розглядати владний характер її інститутів, що інспірується правоздатністю та загальнообов’язковістю генерованих ними нормативно-правових актів [235, с. 120].

Логіко-семантичний аналіз стрижневих компонентів атрибутиву інституційно-правових аспектів державної політики дозволяє зафіксувати синергетичну дуальність її ключових тригерів – механізму державного управління та механізми правового регулювання [261, с. 345]. Звернемось до Великого тлумачного словника сучасної української мови, який визначає «механізм» як внутрішню будову, систему, сукупність станів і процесів, з яких складається певне явище [20, с. 665]. Опираючись на вихідні постулати та принципи державного управління, С. І. Крук ,

пролонгуючи змістовне наповнення попередньої дефініції, пропонує суб'єктно-об'єктні відносини, що виникають під час реалізації державної політики у сфері захисту об'єктів критичної інфраструктури, трактувати у формі правовідносин через необхідність їх державного врегулювання та легітимації [101, с. 77]. Цей процес передбачає імплементацію ряду заходів, зокрема:

1) ідентифікації базових векторів державної політики, стратегічного планування та прогнозування у сфері захисту критичної інфраструктури;

2) пошук, виявлення, профілактика та ліквідація загроз та ризиків безпеки об'єктів критичної інфраструктури;

3) суб'єктна корекція та координування діяльності органів державної влади у сфері забезпечення захисту критичної інфраструктури;

4) визначення обсягу та рівня необхідної ресурсної бази у сфері забезпечення захисту критичної інфраструктури та її забезпечення [102, с. 72].

Усі зазначені заходи та відносин, що виникають у напрямку реалізації державної політики у сфері захисту критичної інфраструктури, реалізуються з метою протидії органами державної влади різним ризикам, загрозам і небезпекам, зокрема щодо застосування безпеко-орієнтованого державно-управлінського інструментарію, який передбачають дотримання принципів публічності, легітимності, результативності, що детерміновано ефективністю механізму правового регулювання. Прислухаємось також до думки С. І. Бевза, який обґрунтував поняття механізму правового регулювання як «сукупності засобів, за допомогою яких забезпечується вплив права на суспільні відносини» [4, с. 44]. Дане судження доповнимо контекстним викладенням, що пропонує Великий енциклопедичний юридичний словник, у якому атрибутив «правового регулювання» тлумачиться як «один із основних засобів державного впливу на суспільні відносини з метою їх упорядкування в інтересах людини, суспільства і держави» [19, с. 335]. Цю позицію підтримують і вчені

Ю. С. Шемшученко та С. В. Бобровник, зазначаючи, що «...правове регулювання є одним із основних засобів державного впливу на суспільні відносини з метою їх упорядкування в інтересах людини, суспільства і держави» [281, с. 40]. Тобто акцент у провадженні державної політики захисту критичної інфраструктури варто робити саме на тріаді людина-суспільство-держава. Можемо аргументувати інституційне значення даної позиції крізь призму положень Конституції України, а саме у ст.3 проголошено «людина, її життя і здоров'я, честь і гідність, недоторканість і безпека визнається в Україні найвищою соціальною цінністю» [99], а також ст. 43, яка додає, що «кожен має право на належні, безпечні і здорові умови праці» [99].

Державний механізм інституційно-правового регулювання не може працювати без застосування особливого «інструментарію» державної влади, що передбачає генерацію або санкціонування відповідних юридичних норм в межах певних типів юридичного впливу. Учені В. Колпаков та О. Кузьменко, аналізуючи механізм інституційно-правового регулювання, диференціюють комплекс державно-правових механізмів, а саме: механізм правового регулювання, механізм дії права, механізм правотворчості, механізм соціального управління, механізм правового впливу, механізм державного управління, механізм забезпечення правових режимів [93, с. 156].

Отже, узагальнюючи отримані результати аналізу, варто зазначити, що інституційно праве регулювання – це один із проявів правового впливу органів державної влади за допомогою інституційних засобів правової дійсності, які реалізують регуляторну силу права, а механізм інституційно-правового регулювання варто розглядати як комплекс цих засобів, які пов'язані між собою та сприяють досягненню визначеної мети правовим регулюванням. Проведений аналіз наукових доробків учених, дозволяє екстраполювати власне розуміння інституційно-правового регулювання здійснення державної політики у сфері захисту об'єктів

критичної інфраструктури. Отже, механізм інституційно-правового регулювання у сфері формування та реалізації державної політики у сфері захисту об'єктів критичної інфраструктури вважаємо за можливе визначити як систему організаційно-управлінських і правових заходів, що реалізовують інститути державної влади, за допомогою яких реалізується цілеспрямований (з метою максимізації безпеки об'єктів критичної інфраструктури) адміністративний вплив на суспільні відносини орієнтовані на запобігання диференційованим ризикам, загрозам і небезпекам об'єктам критичної інфраструктури основані на тріаді людина-суспільство-держава [244. с. 215]. Як основу механізму слід розглядати сукупність об'єктивних залежностей і зв'язків між явищами і процесами саморозвитку і саморуху інституційних засобів правової дійсності. Тому механізм забезпечення безпеки критичної інфраструктури здатний динамічно змінюватися, носити адаптивний характер відповідно до безпекової реальності мікро- та макросередовища, а також глобальної геополітичної ситуації [40, с. 83].

Проведений скринінг нормативно-правової бази, що формує магістральну основу інституційно-правового механізму державної політики у сфері захисту критичної інфраструктури дозволив узагальнити спектр основоположних інституцій, які структурують архітектуру безпекової парадигми об'єктів критичної інфраструктури.

Імплементація інституційних підходів до забезпечення захисту критичної інфраструктури у безпекову парадигму держави зафіксована Законом України «Про національну безпеку України» № 2469-VIII від 31.03.2023 р. [62], відповідно до якого (ст. 4) пріоритетні вектори державної політики у сферах національної безпеки і оборони сфокусовані на «..забезпеченні воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інших її напрямах» [62]. Також, ст. 34 Кодексу цивільного захисту передбачає реалізацію низки заходів інженерного

захисту територій у тому числі на об’єктах критичної інфраструктури [90].

У Стратегії забезпечення державної безпеки, затвердженої Указом Президента України від 16 лютого 2022 року № 56/2022 [267] об’єкти критичної інфраструктури згадуються у числі атрибутів забезпечення національної безпеки, державного суверенітету, конституційного ладу і територіальної цілісності країни. Документом також констатовано, що має місце високий рівень загроз об’єктам критичної інфраструктури (п.19) пов’язаним із тимчасовою окупацією частини території України, триваючими гібридними впливами з боку суб’єктів розвідувально-підривної діяльності, націлених на дисфункцію такої інфраструктури [267]. До основних завдань державної політики (п.24) включено розвиток спроможностей суб’єктів забезпечення державної безпеки щодо превентивного комплексу заходів на об’єктах критичної інфраструктури, контррозвідувального режиму, інтенсифікація боротьби з тероризмом та організованою злочинністю спрямованої на дестабілізацію чи захоплення важливих об’єктів критичної інфраструктури, нарощування технологічних можливостей державної безпеки, прийняття на озброєння новітніх систем апаратних комплексів та спеціальних засобів, підвищення професійного рівня фахівців із забезпечення безпеки, удосконалення нормативно-правового забезпечення, організаційних засад, упровадження дієвих механізмів взаємодії суб’єктів забезпечення державної безпеки із громадянським суспільством, подальший розвиток міжнародного співробітництва в безпековій сфері з питань захисту об’єктів критичної інфраструктури та запровадження національної системи стійкості [267].

Досліджуючи роль органів державної влади у механізмі інституційно-правового регулювання реалізації державної політики, О. Л. Хитра [275, с. 78] констатує, що функціонуюча архітектура інституційного забезпечення національної безпеки України, згідно з розділами IV–VI Конституції України, включає Верховну Раду,

Президента та Кабінет Міністрів України. Розширений суб'єктний склад уповноважених до формування та реалізації державної політики у сфері захисту критичної інфраструктури, ідентифікує також Закон України «Про критичну інфраструктуру» №1882-IX. Проаналізуємо спектр ключових інститутів у досліджуваній сфері.

1. Президент України. Правовий статус Президента у сфері захисту критичної інфраструктури регламентований у розділі V Конституції України, зокрема ст. 102 визначає його гарантом державного суверенітету, територіальної цілісності України, додержання Конституції України, прав і свобод людини і громадянина [96]. Президент України забезпечує національну безпеку України (п.1 ст.106), очолює Раду національної безпеки і оборони України (РНБО) (п.18 ст.106) та особисто формуючи її склад [72], є гарантом адміністрування процесу реагування на кризові ситуації, що загрожують національній безпеці [96]. Отже, повноваження Президента України в сфері захисту критичної інфраструктури можна розмежувати на повноваження: орієнтовані на профільний суб'єктний сегмент; диференційовані за сферами впливу; повноваження із досягнення загальнодержавної мети.

2. Рада національної безпеки та оборони (РНБО). Цей безпековий інститут є координаційним органом з питань національної безпеки і оборони при Президентові України [72]. РНБО України координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони (ч1 ст.107 Конституції України) [96], може подавати Президенту свої пропозиції, що стосуються важливих стратегічних питань із захисту критичної інфраструктури та приймає відповідні рішення [72].

3. Кабінет Міністрів України (КМУ). Даний інститут є найвищим органом в ієрархії органів виконавчої влади. Згідно ст.2 Закону України №794-VII від 27.02.2014 р. «Про Кабінет Міністрів України» [59] до його основних завдань у сфері захисту критичної інфраструктури належать:

– забезпечення державного суверенітету та економічної

самостійності України;

– розроблення і виконання загальнодержавних програм у сфері захисту критичної інфраструктури;

– здійснення заходів щодо забезпечення національної безпеки та обороноздатності України [59].

Отже, Кабінет Міністрів України слід вважати ключовим інститутом, відповідальним за формування та реалізацію в країні державної політики у сфері захисту критичної інфраструктури, організацію та забезпечує національну систему захисту критичної інфраструктури потрібними ресурсами, силами та засобами для її функціонування [231].

4. Верховна Рада України (ВРУ). До її повноважень у сфері захисту критичної інфраструктури входить прийняття законів, визначення засад внутрішньої і зовнішньої політики, затвердження Державного бюджету України, затвердження загальнодержавних програм захисту, заслуховування щорічних та позачергових послань Президента України про внутрішнє і зовнішнє становище України, контроль за діяльністю Кабінету Міністрів України, затвердження рішень про одержання Україною від іноземних держав, банків і міжнародних фінансових організацій макрофінансової допомоги, затвердження указів Президента України про введення надзвичайного чи воєнного стану в окремих місцевостях, про оголошення окремих місцевостей зонами надзвичайної ситуації, надання згоди на обов'язковість міжнародних договорів України та їх денонсація, затвердження переліку об'єктів права державної власності, що не підлягають приватизації, визначення правових засад вилучення об'єктів права приватної власності [96].

5. Функціональні органи у сфері захисту критичної інфраструктури. Відповідають за забезпечення роботи окремих державних систем захисту та реагування, долучаються до реагування на кризові ситуації з метою гарантування безпеки та стійкості критичної інфраструктури, формують

перелік об’єктів критичної інфраструктури, готують пропозиції щодо включення інфраструктурних об’єктів до Реєстру, здійснюють оцінку загроз і ризиків критичній інфраструктурі у відповідних сферах та надають операторам і власникам об’єктів консультації щодо наявності таких загроз і ризиків, а також протоколи дій щодо їх нейтралізації, приймають участь у оцінюванні загроз та ризиків критичній інфраструктурі на національному рівні, генерують пропозиції щодо загальнодержавних та секторальних проєктних загроз і ризиків, здійснюють організацію комунікації та інформаційного реверсу між суб’єктами національної системи захисту критичної інфраструктури, проводять моніторинг рівня безпеки об’єктів критичної інфраструктури за сферами їх діяльності [60].

6. Секторальні органи у сфері захисту критичної інфраструктури. Відповідальні за формування та реалізацію державної політики у довірених їм сегментах критичної інфраструктури. Створюють у своєму складі структурних підрозділів відповідальних за безпеку критичної інфраструктури, акумулюють, систематизують та аналізують дані щодо об’єктів критичної інфраструктури та особливостей їх функціонування, здійснюють разом із їх операторами категоризацію таких об’єктів за ввіреними їм секторами, створюють секторальні каталоги об’єктів та відправляють інформацію до Реєстру. Окрім цього, розробляють та затверджують на секторальному рівні: проєктні загрози критичній інфраструктурі, вимоги до захисту критичних об’єктів за категоріями, плани коінтеграції функціональних органів, регламенти і норми захисту критичної інфраструктури у відповідних секторах, проектні загрози критичній інфраструктурі на об’єктовому рівні, погоджують паспорти безпеки об’єктів критичної інфраструктури за профільними секторами, здійснюють інспекцію стану захищеності критичних об’єктів, займаються розробкою рекомендацій до врахування проєктних ризиків та загроз критичній інфраструктурі національного рівня та щорічної їх оцінки на

загальнодержавному рівні, координують процес підготовки, навчання та тренування персоналу, щодо забезпечення захисту та стійкості секторів критичної інфраструктури, формують щорічний звіт по стану забезпечення безпеки критичної інфраструктури у відповідному секторі, долучаються до реагування на кризові ситуації, що загрожують безпеці та стійкості об'єктів критичної інфраструктури, а також до створення належних умов виконання розвідувальними, правоохоронними та контррозвідувальними органами своїх функцій щодо захисту критичної інфраструктури [60].

7. Уповноважений орган у сфері захисту критичної інфраструктури України. Відповідає за «формування та реалізацію державної політики у сфері захисту критичної інфраструктури, координацію діяльності суб'єктів національної системи захисту критичної інфраструктури…» [60]. Також, відповідно до його повноважень, систематизує пропозиції інститутів національної системи захисту критичної інфраструктури, створює та веде Реєстр об'єктів, організовує здійснення оцінки захищеності об'єктів критичної інфраструктури та оцінює загальний стан їх захищеності, здійснює моніторинг загроз критичній інфраструктурі на загальнодержавному рівні та оцінює загрози національній безпеці із залученням функціональних та секторальних органів. Окрім цього Уповноважений орган проводить щорічну оцінку національного рівня загроз і ризиків критичній інфраструктурі, візує проєктні загрози й ризики на секторальному рівні, узагальнює пропозиції щодо регламентування вимог до забезпечення стійкості та захисту секторів критичної інфраструктури. В межах реалізації інституційних повноважень розробляє та затверджує Проєктні загрози критичній інфраструктурі національного рівня, що містять дані з обмеженим доступом, надсилає пропозиції Кабінету Міністрів України щодо формування Національного плану захисту та забезпечення стійкості критичної інфраструктури, форми, змісту та порядку розробки, паспорта безпеки та планів заходів щодо

захисту критичної інфраструктури загальнодержавного рівня, готує пропозиції до проєктів стратегічних документів щодо забезпечення стійкості та безпеки, здійснення захисту критичної інфраструктури, приймає участь у розробці нових галузей знань, програм підвищення кваліфікації та навчання, навчальних програм з питань забезпечення захисту та стійкості критичної інфраструктури. Також Уповноважений орган узагальнює висновки та рекомендації для власників (операторів) об'єктів щодо зміни їх цільового призначення, права власності чи режиму роботи, формує бази даних щодо загроз і вразливостей критичної інфраструктури, підтримує функціональність системи інформаційного обміну між суб'єктами національної системи захисту критичної інфраструктури, координує роботу секторальних органів, налагоджує співпрацю із іноземними державами та міжнародними організаціями, гарантує виконання і дотримання зобов'язань по захисту критичної інфраструктури згідно підписаним міжнародним договорам [60].

8. Державна служба захисту критичної інфраструктури та забезпечення національної системи стійкості України (ДЗКІ). Ідентифікується як центральний орган виконавчої влади із спеціальним статусом, діяльність якого спрямовується і координується Кабінетом Міністрів України і який опікується забезпеченням національної системи стійкості та формуванням та реалізацією державної політики у сфері захисту критичної інфраструктури. Положення «Про Державну службу захисту критичної інфраструктури та забезпечення національної системи стійкості України» [217] ДЗКІ визначено як «уповноважений орган у сфері захисту критичної інфраструктури України» [217]. Отже, констатуємо факт, що ці дві організації усособлюють один інститут. Законом України № 2684-IX від 18.10.2022 р. «Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України» [51] установлено, що «…під час дії воєнного стану, а також протягом 12 місяців після його припинення чи скасування

повноваження уповноваженого органу у сфері захисту критичної інфраструктури України, передбачені цим Законом, здійснюються Державною службою спеціального зв'язку та захисту інформації України» [51]. Зауважимо, що фактично дана установа (Держспецзвязку) перейняла зазначені повноваження лише через 4 місяці, відповідно до Постанови КМУ № 167 від 24.02.2023 р. «Про внесення змін до Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України» [199], яка внесла відповідні зміни до Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України. Однак зміни було внесено лише через 3 місяці Наказом Адміністрації державної служби спеціального зв'язку та захисту інформації України № 467 від 31.05.2023 р. «Про затвердження Змін до Положення про територіальний орган Адміністрації Державної служби спеціального зв'язку та захисту інформації України» [123]. Зміни стосувалися основних завдань територіального органу, які було розширено діяльністю із реалізації державної політики у сфері захисту критичної інфраструктури, які безпосередньо здійснюють боротьбу з тероризмом, забезпечення здійснення Адміністрацією Держспецзв'язку функціонального управління національною системою захисту критичної інфраструктури, участь Держспецзв'язку у координуванні роботи міністерств та операторів критичних об'єктів з питань забезпечення захисту критичної інфраструктури [159]. Серед напрямків роботи було додано участь у межах регіону у координації діяльності місцевих органів виконавчої влади у сфері захисту критичної інфраструктури, взаємодію в регіоні операторів критичної інфраструктури та функціональних органів з питань забезпечення захисту об'єктів, участь у регіональній організації здійснення оцінки захищеності об'єктів критичної інфраструктури, участь у проведенні в межах регіону оцінки загроз критичній інфраструктурі на загальнодержавному рівні та моніторингу загроз національній безпеці в результаті дій загроз критичній інфраструктурі, участь у підготовці

щорічного моніторингу загроз і ризиків критичній інфраструктурі національного рівня та ін. [123].

Організація налагоджує співробітництво із міжнародними установами та контролює виконання зобов'язань, взятих відповідно до міжнародних договорів, проводить із залученням секторальних і функціональних органів моніторинг загроз критичній інфраструктурі та національній безпеці на загальнодержавному рівні внаслідок впливу загроз критичній інфраструктурі, розробляє та затверджує Проєктні загрози критичній інфраструктурі, направляє Кабінету Міністрів України пропозиції стосовно удосконалення:

– форми, порядку розробки та змістовного наповнення паспорта безпеки об'єктів критичної інфраструктури;

– Національного плану захисту та забезпечення стійкості критичної інфраструктури;

– форми, порядку розроблення та змістовного наповнення національних планів заходів щодо захисту об'єктів критичної інфраструктури.

У 2020 році Держспецзв'язку перейняла функцію зі створення каталогу та Реєстру об'єктів критичної інформаційної інфраструктури [217].

9. Оператор критичної інфраструктури. Законом України «Про критичну інфраструктуру» [60] даний інститут ідентифіковано як «юридична особа будь-якої форми власності та/або фізична особа-підприємець, що на правах власності, оренди або на інших законних підставах здійснює управління об'єктом критичної інфраструктури та відповідає за його поточне функціонування» [60]. Їх також Законом включено до складу національної системи захисту критичної інфраструктури на яку покладено обов'язки розробки та провадження державної політики у сфері захисту критичної інфраструктури.

Разом із Секторальними органами оператори також проводять

категоризацію об’єктів інфраструктури у своїх секторах, формують секторальні переліки об’єктів критичної інфраструктури, подають інформацію до Реєстру, забезпечують захист об’єктів критичної інфраструктури, розробляють і подають на затвердження до відповідних секторальних та функціональних органів паспорт безпеки, розробляють, оновлюють та гарантують виконання об’єктових планів щодо забезпечення стійкості й безпеки критичної інфраструктури, здійснюють моніторинг ризиків на об’єктах, організовують заходи оперативного реагування на фізичні атаки чи протиправні дії що націлені на дестабілізацію, пошкодження або знищення об’єктів критичної інфраструктури, проводять навчання, тренінги, підготовку та тестування працівників, відповідальних за безпеку, охорону та захист об’єктів критичної інфраструктури [60].

Окрім зазначених вище інститутів суб’єктний склад національної системи захисту критичної інфраструктури налічує й інші органи, як: Центральна виборча комісія, Апарат Ради національної безпеки і оборони України, Національний банк України, Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг, Національна комісія, що здійснює державне регулювання у сфері інформатизації та зв’язку, Національна комісія з цінних паперів та фондового ринку, Фонд державного майна України, Державна служба спеціального зв’язку та захисту інформації України, Служба безпеки України, Збройні Сили України й інші військові формування, а також інші органи влади із спеціальним статусом та які залучаються до формування та реалізації державної політики у сфері цивільного захисту, місцеві органи виконавчої влади, органи місцевого самоврядування, функціональні та секторальні органи, інші міністерства, правоохоронні та розвідувальні органи, суб’єкти контррозвідувальної й оперативно-розшукової діяльності, установи, підприємства та організації незалежно від форми власності, що провадять діяльність із забезпечення стійкості та

безпеки критичної інфраструктури [60].

Зазначимо також, що спектр суб'єктів реалізації державної політики у сфері безпеки критичної інфраструктури не обмежується виключно державними інститутами, а акумулює в собі ще й приватних суб'єктів господарювання, а також окремих осіб – надавачів послуг, пов'язаних із національними інформаційними ресурсами. Слушною тут вважаємо пропозицію Г. Ю. Зубка що стосується удосконалення нормативно-правової бази досліджуваної сфери. Пропозиції стосуються регламентування та чіткої фіксації у нормативних документах спектру завдань і відповідних повноважень зазначених суб'єктів на основі затвердження відповідних положень [80, с. 170]. Доречною також буде розробка концепції міжсекторальної взаємодії та синергії сил зацікавлених сторін на основі механізму державно-приватного партнерства.

Загальну архітектуру суб'єктного складу державної політики у сфері безпеки критичної інфраструктури структуровано Законом України «Про критичну інфраструктуру» [60] на рівні управління, серед яких встановлено:

І. Загальнодержавний рівень – реалізується Кабінетом Міністрів України, Національним банком України, уповноваженим органом у сфері захисту критичної інфраструктури України, інститутами державної влади відповідно до транспарентності повноважень, іншими центральними органами виконавчої влади та державними органами.

ІІ. Регіональний та галузевий рівні – здійснюється центральними та місцевими органами виконавчої влади, відповідальними за функціонування окремих державних систем захисту та реагування, відповідальними за формування, забезпечення та реалізацію державної політики у захисту об'єктів критичної інфраструктури по секторах.

ІІІ. Місцевий рівень – реалізується органами місцевого самоврядування (в межах повноважень), а також місцевими органами

виконавчої влади, а в умовах воєнного стану – військово-цивільними адміністраціями.

IV. Об'єктовий рівень – здійснюється безпосередньо операторами критичної інфраструктури.

Відповідно до Закону «Про критичну інфраструктуру» [60], державна політика у сфері захисту критичної інфраструктури передбачає мобілізацію безпекових заходів нормативно-правового, організаційного, інженерно-технічного, інформаційно-аналітичного, ресурсного та методологічного характеру у єдиний комплекс.

Зазначимо, що у системі складових гарантування національної безпеки Г. Ю. Зубко пропонує ідентифікувати інфраструктурну значущість автономних державних систем захисту критичної інфраструктури, серед яких:

1. Єдина державна система цивільного захисту (ЄДСЦЗ) – захисна інфраструктурна значущість;

2. Єдина система реагування, запобігання, й припинення терористичних актів та мінімізації їх наслідків (ЄСЗРПТА) – антитерористична інфраструктурна значущість;

3. Державна система фізичного захисту (ДСФЗ) – фізична інфраструктурна значущість;

4. Національна система кібербезпеки (НСК) – кібербезпекова інфраструктурна значущість;

5. Державна служба забезпечення національної системи стійкості та захисту критичної інфраструктури України (ДСЗКІ) – стійкісна інфраструктурна значущість [217];

6. Система національної безпеки (СНБ) – безпекова інфраструктурна значущість;

7. Система територіальної оборони (СТРО) – оборонна інфраструктурна значущість;

8. Система правоохоронних органів (СПО) – правоохоронна

інфраструктурна значущість [82, с. 40].

Особливої уваги вимагає вивчення інституційно-правових засад функціонування Національної системи кібербезпеки (НСК), що обумовлено пріоритетністю підвищення кібербезпеки та безпеки даних відповідно до найкращих практик. Даний напрям захисту критичної інфраструктури регулюють наступні нормативно-правові акти:

1. Закон України № 2163-VIII. від 05.10.2017 р. «Про основні засади забезпечення кібербезпеки України» [68], ст. 8 якого визначає предикат Національної системи кібербезпеки як «…сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури» [68].

2. Указ Президента України від № 447/2021 26.08.2021 р. «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 р. «Про Стратегію кібербезпеки України» [268], що увів в дію рішення РНБО України від 14 травня 2021 р. та затвердив «Стратегію кібербезпеки України», яка визначає завдання, серед яких забезпечення захисту критичної інформаційної інфраструктури від кібератак та серед проблем визнає недостатню убезпеченість від кіберзагроз об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів.

3. Закон України № 3475-IV від 23.02.2006 р. «Про Державну службу спеціального зв'язку та захисту інформації України» [56], що визначає статус, основні завдання, принципи та особливості функціонування Державної служби спеціального зв'язку та захисту інформації України.

4. Наказ Адміністрації Держспецзв'язку від 10.06.2008 № 94, яким

утверджено «Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [125].

5. Постанова КМУ № 1772 від 16.11.2002 р. «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах», якою затверджено «Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах», що прийнята з метою підвищення рівня захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах [208].

6. Постанова КМУ № 373 від 29.03.2006 р. «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» [212], якою затверджено «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» Правила визначають загальні вимоги та організаційні засади забезпечення захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах [212].

7. Наказ Адміністрації Держспецзв'язку № 660 від 02.12.2014 р. «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» [126], яким затверджено «Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [126], що регламентував правові та організаційні засади

проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах державних органів, органів місцевого самоврядування, військових формувань та підприємств, установ і організацій критичної інфраструктури.

8. Наказ Адміністрації Держспецзв'язку № 20 від 15.01.2016 р. «Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті» [127], яким затверджено «Порядок сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті», що визначає організаційні засади даного процесу.

9. Постанова КМУ № 563 від 23.08.2016 р. «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» [210], якою затверджено «Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» [210], яким регламентовано механізм створення переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави.

10. Постанова КМУ № 518 від 19.06.2019 р. «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» прийнята відповідно до ч.2 ст.6 Закону України «Про основні засади забезпечення кібербезпеки України» та регламентує організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури [201].

11. Постанова КМУ № 1295 від 23.12.2020 р. «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» «Деякі питання забезпечення

функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» [191], що затвердила Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки та визначила відповідальним за функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації.

12. Наказ Міністерства енергетики України № 417 від 15.12.2022 р. «Про Вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури» [128] виданий відповідно до п.14 Загальних вимог до кіберзахисту об'єктів критичної інфраструктури з метою реалізації державної політики захисту об'єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури. Затверджені вимоги визначають заходи кіберзахисту об'єктів критичної інформаційної інфраструктури, що експлуатуються на об'єктах критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури для досягнення конкретного цільового стану кібербезпеки.

13. Постанова КМУ № 257 від 24.03.2023 р. «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури», що прийнята у відповідності до ч.3 ст. 6 Закону України «Про основні засади забезпечення кібербезпеки України» та ввела в дію Порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, що визначає механізм організації та проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та вимоги до його проведення [197].

14. Постанова КМУ № 1175 від 14.10.2022 р. «Деякі питання подання інформації у сфері захисту критичної інфраструктури» [196], що прийнята відповідно до ч.2 ст.19 та п.4 ч.4 ст.21 Закону України «Про критичну інфраструктуру» та затвердила форму річного звіту про виконання секторальним органом повноважень та форму річного звіту про

виконання оператором критичної інфраструктури повноважень.

15. Постанова КМУ № 1174 від 14.10.2022 р. «Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури» [215], що прийнята відповідно до ч.4 ст.13 Закону України «Про критичну інфраструктуру» та затвердила Регламент інформаційного обміну між суб'єктним складом національної системи захисту критичної інфраструктури, яким визначено механізм інформаційного реверсу між суб'єктами, залученими до захисту критичної інфраструктури з метою забезпечення її захисту та стійкості.

16. Указ Президента України № 56/2022 від 16.02.2022 р. «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки»» [267], яким утверджено Стратегію забезпечення державної безпеки, яка зафіксувала перелік загроз об'єктам критичної інфраструктури у сфері інформаційної та кібербезпеки (п.19) та основних завдань державної політики (п.24), серед яких у пріоритеті подальший розвиток і посилення спроможності національної системи кібербезпеки, оптимізація координації її суб'єктів з метою ефективної протидії кіберзагрозам у сучасному безпековому середовищі, створення ефективної системи обміну інформацією між суб'єктами забезпечення державної безпеки та запровадження дієвих механізмів доступу суб'єктів забезпечення державної безпеки до державних електронних інформаційних ресурсів та автоматизованих інформаційних і довідкових систем, реєстрів, банків (баз) даних [267].

Реалізація державної політики у інших сферах захисту критичної інфраструктури інспірує необхідність інституційно-правових заходів реалізовуваних органами державної влади в межах яких розроблено та введено у дію низку законодавчих, нормативних документів та методичних регламентів, що закладають основу для безперебійності функціонування об'єктів критичної інфраструктури. Відзначимо основоположні інституційно-правові зміни, серед яких:

1. Постанова КМУ «Про внесення змін до переліку секторів критичної інфраструктури» № 455 від 09.06.2023 р. [198] доповнила позицію «Харчова промисловість та агропромисловий комплекс» у графі «Тип основної послуги» пунктом «виробництвом ветеринарних препаратів та експлуатацією елеваторів»;

2. Постанова КМУ № 1109 від 09.10.2020 р. «Деякі питання об'єктів критичної інфраструктури» [78] є однією із найважливіших нормативних актів, прийнята відповідно до ч.1 ст.8, ч.3 ст. 9 та ч.4 ст.10 Закону України «Про критичну інфраструктуру» та розроблена з урахуванням вимог законодавства ЄС – Директиви Європейського Парламенту та Ради (ЄС) 2016/1148 від 06.07.2019 р. «Про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» [35], Директиви Ради 2008/114/ЄС від 08.12.2008 р. «Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту» [36]. Постанова одночасно урегулювала цілий ряд інституційно-правових аспектів у напрямку реалізації державної політики у сфері захисту критичної інфраструктури, а саме ввела в дію Порядок віднесення об'єктів до критичної інфраструктури, Методику категоризації об'єктів критичної інфраструктури та Перелік секторів критичної інфраструктури, який гармонізовано з відповідним переліком, наведеним у Директиві ЄС 2016/1148 [36].

3. Постанова КМУ «Деякі питання об'єктів критичної інформаційної інфраструктури» № 943 від 09.10.2020 р. прийнята відповідно до абзацу 1 ч.3 ст.4 Закону України «Про основні засади забезпечення кібербезпеки України» та вводить в дію Порядок формування переліку об'єктів критичної інформаційної інфраструктури та Порядок внесення об'єктів критичної інформаційної інфраструктури до державного Реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування [192].

4. Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України № 23 від 15.01.2021 р. «Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури» [124]. Даний нормативний акт став логічним доповненням Методики категоризації об'єктів критичної інфраструктури (п.5), затвердженої постановою КМУ № 1109 від 09.10.2020 р. [193] та розроблена на виконання вимог ст.6 Закону України «Про основні засади забезпечення кібербезпеки України» [68]. Присвоєння об'єктам інфраструктури статусу критичного проводиться за сукупністю відповідних критеріїв, що ідентифікують їх соціальну, економічну, політичну та екологічну значимість для забезпечення безпеки громадян, оборони країни, суспільства, правопорядку, надання життєво-важливих послуг, свідчать про існування для них ризиків та загроз, перспективи виникнення деструктивних ситуацій, людський фактор чи природні лиха, припинення функціонування, тривалість робіт для ліквідації негативних наслідків та повної регенерації потужностей штатного режиму. Визначено предикат рівня критичності як «відносної міри важливості об'єктів критичної інфраструктури, якою враховується вплив раптового припинення функціонування або функціонального збою на безпеку постачання, забезпечення суспільства важливими товарами і послугами» [124] Для визначення категорії об'єкта критичної інфраструктури уповноважені органи у своїх секторах разом з операторами критичної інфраструктури проводять бальну оцінку критичності кожного об'єкта критичної інфраструктури за допомогою форм із секторальними та міжсекторальними критеріями визначення рівня негативного впливу. Зазначені критерії враховують важливість об'єкта критичної інфраструктури на основі аналізу потенційної шкоди, яку суспільство, навколишнє середовище, економіка та національна безпека держави можуть зазнати внаслідок порушення або припинення функціонування об'єкта інфраструктури. Важливість об'єктів інфраструктури оцінюється

за допомогою низки секторальних та міжсекторальних критеріїв [193].

5. Постанова КМУ № 818 від 04.08.2023 р. «Деякі питання паспортизації об'єктів критичної інфраструктури» [195] затвердила «Порядок розроблення та погодження паспорта безпеки на об'єкт критичної інфраструктури» [195], що передбачає ч.4 ст.12 Закону України «Про критичну інфраструктуру» [60].

6. Постанова КМУ № 821 від 22.07.2022 р. «Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури» [209] затвердила форму Акту оцінки стану захищеності об'єкта критичної інфраструктури, що складається у результаті проведення моніторингу рівня безпеки даних об'єктів, відповідно вимог ч.4 ст. 23 Закону України «Про критичну інфраструктуру» [60].

7. Постанова Правління НБУ № 151 від 30.11.2020 р. «Про затвердження Положення про визначення об'єктів критичної інфраструктури в банківській системі України» [219] що встановила критерії та порядок віднесення банків України до об'єктів критичної інфраструктури, а також порядок ведення переліку таких об'єктів в банківській системі України та переліків об'єктів критичної інформаційної інфраструктури в банках, обсяги та порядок подання банками інформації, необхідної для ведення реєстру об'єктів критичної інформаційної інфраструктури.

8. Постанова КМУ № 415 від 28.04.2023 р. «Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього» [207] Положеннями переважної більшості зазначених інституцій передбачено формування та ведення Реєстру об'єктів критичної інфраструктури, однак Уряд ухвалив відповідну Постанову лише 8 квітня 2023 року, чим виконав вимоги ст.11 Закону України «Про критичну інфраструктуру», прийнятого у 2021 році [60]. Цей документ регламентував процедуру включення об'єктів та формування і ведення Реєстру, а також внесення до нього

інформації про ці об’єкти. Постанова регламентує умови доступу до даних Реєстру, що має на меті «..узгодження дій суб’єктів національної системи захисту критичної інфраструктури» [207]. Аналіз нормативного акту дозволив відзначити наступні ключові положення:

І. Визначено поняття «власник об’єкта критичної інфраструктури» як «юридична особа будь-якої форми власності або фізична особа-підприємець, якій на праві власності належить об’єкт критичної інфраструктури». Варто акцентувати увагу, що у даному формулюванні регламентовано лише приватну форму власності, однак у «Порядку розроблення та погодження паспорта безпеки на об’єкт критичної інфраструктури» [195] дана умова розширена і включає також інші речові права – господарське відання та оперативне управління.

ІІ. Адміністратором, власником та держателем Реєстру визначено державу в особі Уповноваженого органу у сфері захисту критичної інфраструктури України (Держспецзв’язку), який проводить облік, узагальнення, систематизацію, аналіз та надання інформації, а інформацію ідентифіковано у якості державного ресурсу.

ІІІ. Користувачами Реєстру є суб’єкти національної системи захисту критичної інфраструктури.

IV. До Реєстру вносяться відомості про секторальний орган, який подає інформацію, оператора критичної інфраструктури, документ, на підставі якого ідентифіковано та категоризовано об’єкт критичної інфраструктури, об’єкт критичної інфраструктури, погодження (перегляд) паспорта безпеки на об’єкт критичної інфраструктури.

V. Дані про об’єкти критичної інфраструктури, що внесені до Реєстру, є публічними та безкоштовними, окрім інформації з обмеженим доступом. Зауважимо, що війна в Україні внесла певні корективи до даного регламенту і частину даних про критичну інфраструктуру було закрито в інтересах національної безпеки. Так, НКРЕКП внесла зміни до своєї Постанови № 349 від 26.03.2022 р. «Щодо захисту інформації, яка в

умовах воєнного стану може бути віднесена до інформації з обмеженим доступом, у тому числі щодо об'єктів критичної інфраструктури» [218]. У документі визначено, що «під час дії воєнного стану в Україні та до останнього дня місяця, наступного за місяцем припинення або скасування воєнного стану, на веб-сайтах ліцензіатів повинен бути закритий доступ» [218]. Частково була прихована також інформація з приводу інших секторів – освітніх і медичних закладів, кадастру, системи життєзабезпечення та захисту населення. Такі обмеження є цілком виправдані й повністю відповідають національним інтересам та особливостям регулювання відносин у воєнний час.

VI. Інформація у Реєстрі розподілена на дві категорії доступу: відкриту (інформація про: секторальний орган, який подав інформацію, найменування, місцезнаходження, код ЄДРПОУ, форму власності, країну реєстрації, КВЕД основної діяльності оператора критичної інфраструктури, кінцевого бенефіціара, реєстровий номер об'єкта критичної інфраструктури, дату внесення інформації) та з обмеженим доступом (назва об'єкта критичної інфраструктури, категорія критичності, дата останнього оновлення інформації про об'єкт, дата затвердження паспорта безпеки, адреса місцезнаходження, кадастровий номер, найменування, місцезнаходження власника (суб'єкта управління) об'єкта, форма власності, країна реєстрації власника, сектор, підсектор, тип основної послуги, життєво важлива функція та послуга, яку надає об'єкт, назва секторального органу, який погодив паспорт безпеки, дата його погодження, дата погодження функціональними органами планів захисту від загроз, відомості про особу, відповідальну за організацію та забезпечення захисту об'єкта, додаткові відомості щодо об'єкта критичної інфраструктури.

VII. Секторальні органи подають окремо про кожен об'єкт критичної інфраструктури інформацію до Реєстру за формою. До повідомлення про внесення до Реєстру відомостей про об'єкт критичної інфраструктури

додаються документи, що обґрунтовують розрахунок віднесення об’єкта критичної інфраструктури до однієї з категорій критичності, здійснений відповідно до Методики категоризації об’єктів критичної інфраструктури [207]. Інформація про об’єкт критичної інфраструктури подається у місячний строк з моменту внесення об’єкта критичної інфраструктури до секторального переліку об’єктів критичної інфраструктури.

VIII. Об’єкт критичної інфраструктури виключається з Реєстру у зв’язку з невідповідністю такого об’єкта критеріям віднесення його до критичної інфраструктури [207].

Постановою КМУ № 415 визначено, що «оператори критичної інфраструктури протягом трьох місяців з дня внесення відомостей про об’єкт критичної інфраструктури до Реєстру об’єктів критичної інфраструктури забезпечують подання на погодження паспорта безпеки на об’єкт до відповідного державного органу, визначеного законодавством відповідальним за забезпечення формування та реалізацію державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури» [207].

Вкрай важливою процедурою у напрямку упорядкування інституційно-правових аспектів провадження державної політики у сфері захисту критичної інфраструктури стала розробка й погодження паспорта безпеки об’єкту критичної інфраструктури. Порядок паспортизації було затверджено Постановою КМУ «Деякі питання паспортизації об’єктів критичної інфраструктури» № 818 від 04.08.2023 р., що вимагає ч.4 ст.12 Закону України «Про критичну інфраструктуру». Цей Порядок визначає вимоги до його розробки оператором критичної інфраструктури та його складових, а також механізм погодження секторальними і функціональними органами у сфері захисту критичної інфраструктури [195]. Даний документ містить загальну характеристику об’єкта критичної інфраструктури, плани захисту та акти оцінки стану

захищеності об’єкта критичної інфраструктури.

Акт оцінки стану захищеності об’єкта критичної інфраструктури складається за формою, визначеною в Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури, затвердженому Постановою КМУ № 821від 22.07.2022 р. [209], яка відповідає вимогам ч.4 ст. 23 Закону України «Про критичну інфраструктуру» [60]. Документ відображає результати моніторингу безпеки об’єктів критичної інфраструктури, що проводиться один раз на три роки функціональними й секторальними органами у сфері захисту критичної інфраструктури.

План захисту (як складову паспорта безпеки) розробляє оператор за кожною із проектних загроз національного, секторального та об’єктового (у разі наявності) рівня відповідно до форм планів захисту та рекомендацій з розроблення планів захисту, що затверджуються відповідними функціональними органами у сфері захисту критичної інфраструктури щодо кожної проектної загрози. Відповідно до зазначених проектних загроз визначаються функціональні органи.

Варто відзначити привенційну значимість зазначених інституційних новелизацій, оскільки Реєстр дає уявлення про спектр критично важливих інфраструктурних об’єктів та їх характеристики, а Паспорт безпеки містить такі важливі атрибути, як плани захисту та акти оцінки стану захищеності таких об’єктів. Акт оцінки стану захищеності, включає критерії оцінки стану захищеності, їх показники та методику оцінки стану захищеності визначає уповноважений орган у сфері захисту критичної інфраструктури [195]. Вони підлягають обов’язковому погодженню відповідними функціональними органами, до яких, зокрема, належать МОЗ, Міноборони, Держспецзв’язку, ДСНС, Національна поліція. А у разі загроз диверсій, терористичних актів, актів кібертероризму підлягають обов’язковому погодженню СБУ, Національною гвардією, іншими державними органами [195].

Важливим кроком також є ідентифікація проєктних загроз та ризиків

об’єкта критичної інфраструктури, що представляє собою оформлений за встановленим зразком протокол, який регламентує характеристики і властивості потенційних та реальних загроз об’єкту критичної інфраструктури, на зниження ризиків настання яких має бути орієнтоване функціонування системи захисту критичної інфраструктури, візує Уповноважений орган у сфері захисту критичної інфраструктури України. Органи державної влади, призначені відповідальними за роботу окремих державних сил реагування «формують пропозиції щодо національних та секторальних проектних ризиків і загроз» [60]. Проектні загрози критичній інфраструктурі секторального та об’єктового рівня розробляють та затверджують Секторальні органи.

Задля забезпечення функціонування зазначеної системи важливим є регламентація інформаційного забезпечення. Відповідно до ч.4 ст.13 Закону України «Про критичну інфраструктуру» [60] Кабінет Міністрів України Постановою № 1174 від 14.10.2022 р. затвердив «Регламент обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури» [215]. Даний нормативний акт регламентує інформаційну взаємодію, що забезпечується шляхом послідовного інформаційного реверсу між суб’єктами національної системи захисту критичної інфраструктури, що здійснюється відповідальними особами, визначеними такими суб’єктами, з використанням засобів електронних комунікацій, національної системи конфіденційного зв’язку, спеціального зв’язку, шифрувального зв’язку та інформаційно-комунікаційних систем [215]. Обмін інформацією здійснюється послідовно між операторами критичної інфраструктури та секторальними органами, між секторальними органами та уповноваженим органом а також між секторальними органами та КМУ. Регламентує також порядок передачі інформації в умовах кризової ситуації та об’єктах критичної інфраструктури та інформування про хід ліквідації кризової ситуації на об’єктах критичної інфраструктури. Однак, не достатньо врегульованим

залишається інформаційний реверс між службами реагування на надзвичайні ситуації та об'єктами критичної інфраструктури стратегічного значення інформація про які належать до категорії державної таємниці. Отже, описана інституційно-інформаційна система ведення Реєстру, паспортизації та фіксації проєктних загроз об'єктів критичної інфраструктури та обміну інформацією потрібна для виявлення джерел небезпеки та також оцінки здатності систем захисту критичної інфраструктури протистояти усім типам загроз, тим самим активізуючи дієвість національної системи захисту критичної інфраструктури.

2.2. Аналіз інституційної спроможності національної системи захисту критичної інфраструктури.

У сучасних умовах глобалізаційних процесів у світі, питання збереження власної суверенності виходить на авангард політики національної безпеки будь якої незалежної держави. У даному ракурсі наукових досліджень варто відзначити позицію Г. Ю. Зубка, який наголошує на необхідності забезпечення інфраструктурної ідентичності, інфраструктурної спроможності та інфраструктурної значущості з метою забезпечення втілення національних інтересів. Вчений стверджує, що у сфері функціонування об'єктів критичної інфраструктури Україна повинна володіти могутнім та системним інфраструктурним комплексом у тандемі із ефективною функціональною державною політикою [83, с. 215].

Сучасні безпекові виклики в умовах гібридних загроз безпековій парадигмі створюють небезпеку для суверенітету та територіальної цілісності України. У таких умовах ключового значення набуває процес захисту критичної інфраструктури у якості детермінанти національної безпеки, що вимагає якісно нового рівня державного управління безпекою критичної інфраструктури. Це у свою чергу інспірує забезпечення належного рівня інституційної спроможності публічних інституцій, що полягає в ефективному виконанні покладених на них функцій на усіх

державно-управлінських рівнях.

Проаналізуємо сутнісне наповнення інтенції національної системи захисту критичної інфраструктури, яка утверджена Законом України «Про критичну інфраструктуру» [60] як «сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади (військово-цивільних адміністрацій – у разі утворення), органів місцевого самоврядування, операторів критичної інфраструктури, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури» [60]. Дане формулювання вважаємо оптимальним, оскільки воно передбачає залучення до національної системи захисту критичної інфраструктури військово-цивільних адміністрацій та операторів критичної інфраструктури.

Аналіз інституційної спроможності національної системи захисту критичної інфраструктури варто розпочати із трактування інституційного розвитку на рівні реалізації державної політики, який О. Г. Рось ідентифікує як системний розвиток організаційних структур публічної влади, оновлення форм і методів діяльності, механізмів і засобів їх взаємодії [232, с. 98].

Європейська Комісія відзначає, що зміцнення інституційної спроможності національної системи захисту критичної інфраструктури орієнтовано передусім на інститути (системи і структури), однак зміцнення спроможності індивідів (тобто штату інституцій) може бути так само важливим для зміцнення здатності інститутів діяти більш ефективно і результативно [304, с. 5].

Організація економічного співробітництва та розвитку (OECD) визначає інституційну спроможність як суму організаційних, структурних та технічних систем, а також індивідуальні компетенції, які створюють та впроваджують політику, що відповідає потребам громадськості [339, с.77]. Згідно з позицією Світового банку, підвищення інституційної спроможності охоплює три основні види діяльності: підвищення

кваліфікації, удосконалення процедур та зміцнення організаційної функціональності [174]. Проаналізований спектр наукових розвідок у вивченні інституційної спроможності національної системи захисту критичної інфраструктури дає підстави даний процес визначати у фокусі на спроможності структурних, організаційних, технічних систем та окремих індивідів, що включає розвиток навичок і компетенцій на всіх рівнях здійснення державної політики захисту критичної інфраструктури крізь діоптрій процесних інституцій, що включає правила, процедури, засоби, інструменти, методи, організацію і ресурси.

Вважаємо раціональним акцент, стосовно впливу на інституційну спроможність індивідуальних компетенцій фахівців які ініціюють та провадять державну політику, що відповідає потребам громадськості. Дану позицію підтримує і О. А. Дмитренко [37, с.50], який, досліджуючи феномен інституційної спроможності, акцентує увагу на евентуальнісних детермінантах комплексного виконання інститутами захисту критичної інфраструктури своїх функцій. Окрім зазначеного вище рівня компетенції фахівців у цій галузі, учений вважає доцільним охопити також наявність ресурсів, характер та обсяги поставлених завдань, рівень оперативності прийняття рішень в умовах системних змін [38, с. 154]. Узагальнивши проаналізовані наукові доробки, інституційну спроможність національної системи захисту критичної інфраструктури можемо визначити як комплементарність внутрішньої системи профільних інститутів та відповідних інституцій, що детермінує їх здатність синхронно забезпечувати захист об’єктів критичної інфраструктури з метою безперебійності їх функціонування. Виходячи із вищезазначеного, а також, опираючись на дослідження учених [239, с. 65], [336, с. 10] варто виокремити тріаду базових індикаторів інституційної спроможності системи національного захисту критичної інфраструктури:

Внутрішня синхронізація – передбачає взаємну узгодженість інститутів усередині системи захисту критичної інфраструктури, тобто

вузькоспеціалізованих структур безпеки, операторів критичних об’єктів.

Зовнішня компліментарність – розглядається як взаємоузгодженість та відповідність інституційної системи захисту критичної інфраструктури із системою безпеки та оборони в цілому, а з одного боку, а з іншого боку, із національною інституційною системою публічного управління, а також узгодженість із розвитком світових тенденцій державної політики у сфері захисту критичної інфраструктури.

Конгруентність внутрішніх та зовнішніх складових інституційної системи – означає, що відносини всередині інститутів відповідають соціальним відносинам, які упорядковуються і підтримуються цими інститутами [336, с. 15].

Обґрунтування зазначених складових інституційної спроможності національної системи захисту критичної інфраструктури можна знайти у Концепції створення державної системи захисту критичної інфраструктури [230], пізніше його було доповнено Законом України «Про критичну інфраструктуру» [60]. Концепцією узагальнено поступальні кроки розвитку та удосконалення інституційної спроможності системи захисту критичної інфраструктури на національному, регіональному (галузевому), місцевому та об’єктовому рівнях, реалізація яких детермінує досягнення інституційної спроможності.

1.На національному рівні:

– визначення інституту, відповідального за формування та провадження державної політики у сфері захисту критичної інфраструктури;

– інтеграція засад державно-приватного партнерства у сферу захисту критичної інфраструктури, що посилить атавізм взаємодовіри, інформаційного обміну, інвестиційної мотивації у напрямку захисних заходів критичної інфраструктури;

– визначення повноважень, завдань та відповідальності державних органів у сфері захисту критичної інфраструктури, а також обов’язків,

прав та відповідальності власників об’єктів критичної інфраструктури;

– організація взаємодії суб’єктів державної системи захисту критичної інфраструктури, обміну інформацією між ними про загрози критичній інфраструктурі, створення мережі ситуаційних центрів;

– створення системи підготовки та перепідготовки кадрів у сфері захисту критичної інфраструктури;

– затвердження переліку секторів критичної інфраструктури та визначення державних органів, що відповідатимуть за їх захист;

– визначення режимів функціонування державної системи захисту критичної інфраструктури та порядку їх ротації відповідно до змін у безпековому середовищі;

– розробка і затвердження єдиної методології проведення оцінки загроз критичній інфраструктурі;

– розробка переліку об’єктів критичної інфраструктури;

– розробка методології та визначення критеріїв ідентифікації інфраструктурних об’єктів критичної інфраструктури, а також порядку їх паспортизації та категоризації;

– встановлення вимог до планування заходів щодо захисту критичної інфраструктури, включаючи аварійні плани, плани комунікації, плани регенерації об’єктів критичної інфраструктури, плани проведення здійснення навчань;

– здійснення категоризації та паспортизації об’єктів критичної інфраструктури;

– розробка та затвердження Національного плану стійкості та забезпечення захисту критичної інфраструктури.

2. На регіональному (галузевому) рівні:

– підготовка пропозицій щодо включення об’єктів інфраструктури до критичної інфраструктури;

– збір, аналіз та систематизація інформації про самі об’єкти

критичної інфраструктури та їх функціонування;

– організація постійного обміну інформацією та моніторинг стану захищеності об’єктів критичної інфраструктури;

– розробка, у відповідно до законодавства, порядку реагування на кризові ситуації й загрози критичній інфраструктурі, а також забезпечити захист і стійкість критичної інфраструктури;

– здійснення превентивного інформування власників об’єктів критичної інфраструктури про загрози та надання їм експертної, інформаційно-консультативної та технічної допомоги;

– розробка стандартів та інших інституцій з питань захисту критичної інфраструктури у відповідних секторах;

– здійснення систематичних заходів державного нагляду, контролю та визначення стану захищеності об’єктів критичної інфраструктури;

– розробка і затвердження галузевих програм з протидії загрозам критичній інфраструктурі;

– проведення інспекцій об’єктів критичної інфраструктури з метою визначення їх рівня інформаційної та кібербезпеки;

– погодження та ведення обліку паспортів безпеки об’єктів критичної інфраструктури, а також карт ризику адміністративно-територіальних одиниць.

3. На місцевому рівні:

– розробка, затвердження і виконання локальних програм стійкості та забезпечення захисту критичної інфраструктури;

– розробка та погодження місцевих планів взаємодії суб’єктів системи захисту об’єктів критичної інфраструктури та планів їх відновлення;

– розробка та виконання локальних програм із посилення стійкості громад до кризових ситуацій, пов’язаних із дизфункією об’єктів критичної інфраструктури;

– розробка та проєктування інженерно-технічних заходів захисту цивільного населення у містобудівній документації щодо безпечного розміщення та експлуатації об’єктів критичної інфраструктури.

4. На об’єктовому рівні:

– розробка та здійснення заходів із запобігання кризовим ситуаціям на об’єктах критичної інфраструктури;

– розробка та виконання об’єктових планів заходів щодо захисту і забезпечення стійкості об’єктів критичної інфраструктури;

– розробка, виконання та перегляд об’єктових програм протидії загрозам, а також програм забезпечення інформаційної безпеки та кібербезпеки;

– забезпечення виконання законних вимог конфіденційності інформації про об’єкти критичної інфраструктури;

– забезпечення відновлення функціональності об’єктів критичної інфраструктури в разі аварій та збоїв.

Передбачалося, що реалізація положень Концепції сприятиме досягненню інституційної спроможності національної системи захисту критичної інфраструктури, що визначатиметься:

– здатністю забезпечувати належний рівень захисту такої інфраструктури від усіх видів загроз;

– відпрацюванням ефективних механізмів реагування на кризові ситуації, та ліквідації їх наслідків, а також швидкому відновленню функціональності об’єктів критичної інфраструктури;

– налагодженням ефективної суб’єктної взаємодії інститутів, що входитимуть до складу національної системи захисту критичної інфраструктури та суспільства, місцевих громад, засобів масової інформації та профільних наукових установ;

– гармонізацією законодавства України та ЄС у сфері захисту критичної інфраструктури;

– розвитком міжнародного співробітництва України у сфері захисту критичної інфраструктури та світових систем безпеки.

Важливим кроком у досягненні інституційної спроможності національної системи захисту критичної інфраструктури є затвердження Розпорядженням КМУ № 825-р від 19.09.2023 р. «Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури» [228]. Він передбачає реалізацію стратегічного цільового пента-комплексу, а кожна із цілей передбачає відповідну еманацію архітектури її практичної реалізації у вигляді послідовних етапів. Проаналізуємо ключові положення зазначеної інституції:

Ціль 1 – передбачає правову регламентацію функціонування суб'єктів національної системи захисту критичної інфраструктури. Досягатиметься за рахунок уточнення завдань та повноважень інститутів національної системи захисту критичної інфраструктури шляхом модернізації нормативно-правової бази у сфері діяльності суб'єктів національної системи захисту критичної інфраструктури, фіксації вимог та забезпечення спостереження за рівнем захищеності об'єктів критичної інфраструктури за рахунок розроблення вимог щодо захисту об'єктів критичної інфраструктури та моніторингу і звітування щодо стану виконання вимог законодавства та з питань захисту критичної інфраструктури.

Ціль 2 – формування системи координування та інтеракції інститутів національної системи захисту критичної інфраструктури. Передбачає розробку порядку комунікації під час реагування на виникнення кризових ситуацій та їх загроз на критичній інфраструктурі за рахунок удосконалення протоколів взаємодії інфраструктури, та розробки планів співробітництва структурних підрозділів національної системи захисту критичної інфраструктури, забезпечення функціонування системи обміну інформацією за рахунок удосконалення регламенту інформаційного обміну між суб'єктами національної системи захисту критичної

інфраструктури в разі порушення функціоналу об’єктів.

Ціль 3 – запровадження управління ризиками критичної інфраструктури. Передбачає періодичне проведення оцінки ризиків і загроз шляхом оцінки ризиків і загроз критичній інфраструктурі, управління рівнем захисту та розвиток у суб’єктів національної системи захисту критичної інфраструктури спроможностей реагувати на загрози, що виникають через їх проєктування.

Ціль 4 – посилення стійкості національної системи захисту критичної інфраструктури. Досягатиметься шляхом розробки механізмів співробітництва у проблемних ситуаціях на регіональному та секторальному рівнях, систематичного підвищення кваліфікації операторів критичної інфраструктури, локалізації наслідків надзвичайних ситуацій, удосконалення переліку спеціальностей та галузей знань, за якими проводиться підготовка здобувачів вищої освіти, новими позиціями сфери забезпечення захисту та стійкості критичної інфраструктури, ампліфікація стійкості суспільства до умов відсутності стабільних життєво-важливих послуг шляхом набуття територіальними громадами спроможностей підтримувати мінімальний рівень життєзабезпечення власними силами, та інтеграції механізму державної підтримки заходів з посилення стійкості населення у критичних ситуаціях

Ціль 5 – налагодження міжнародної співпраці. Передбачає розширення міжнародного співробітництва з іноземними державами та міжнародними організаціями у сфері захисту критичної інфраструктури шляхом здійснення заходів колективної оборони [228].

Отже, зазначений документ дає підстави виокремити ряд ключових положень, що на наш погляд заслуговують особливої уваги щодо розвитку державної політики у сфері захисту критичної інфраструктури. Серед них:

– фіксація регламентів, норм та вимог до захищеності критичної інфраструктури;

– проєктування та дотримання планів заходів захисту і забезпечення

стійкості, а також локалізації та ліквідації наслідків аварій;

– розробка та удосконалення кожні три роки планів інтеракції суб'єктів національної системи захисту критичної інфраструктури, розробка і затвердження секторальних планів співробітництва, планів взаємодії, відновлення, проведення навчань та тренувань і програм з протидії загрозам критичній інфраструктурі;

– проведення колективних тактико-спеціальних, командно-штабних навчань, спільних занять та тренувань із оборони, захисту, охорони, кібератак та припинення злочинних дій;

– удосконалення переліку спеціальностей та галузей знань, за якими проводиться підготовка здобувачів вищої освіти компетентностями щодо забезпечення захисту та стійкості критичної інфраструктури;

– розробка, затвердження та погодження зі стейкхолдерами програм навчання населення, місцевих планів взаємодії у кризовій ситуації та планів відновлення функціонування критичної інфраструктури.

Законом України «Про критичну інфраструктуру» [60] (ст. 6) також регламентовано основні принципи функціонування національної системи захисту критичної інфраструктури, дотримання яких сприяє досягненню нею інституційної спроможності. Серед них відзначимо забезпечення єдності методологічних засад, координованість, розвиток державно-приватного партнерства, гарантування безпеки, захисту та охорони інформації з обмеженим доступом, розширення міжнародного співробітництва.

Як стверджує G. D. Bhatt, поштовхом для розвитку та практичного удосконалення інституційної спроможності національної системи захисту критичної інфраструктури варто розглядати перегляд та врахування нових суспільно-економічних, безпекових та геополітичних реалій; використання сучасних форм і методів об'єктово-суб'єктної взаємодії; удосконалення виявлених прогалин у нормативно-правій базі [287, с. 122]. Цього можна досягнути за рахунок залучення до даного напрямку

наукових установ та профільних закладів освіти.

Звернемо увагу на компетентності фахівців у галузі забезпечення впливу на інституційну спроможність індивідуальних компетенцій фахівців впливу на інституційну спроможність індивідуальних компетенцій фахівців. Результатами наукового пошуку M.Zollo та S.Winter визначають інституційну спроможність як результат організованого навчання, через яке організація посилює свою здатність систематично генерувати і модифікувати операційну діяльність у напрямі підвищення управлінської ефективності [357, с. 3].

Отже, констатуючи результати проведеної наукової розвідки, варто зазначити, що одну із фундаментальних детермінант інституційної спроможності національної системи захисту критичної інфраструктури складає спектр компетенцій, якими володіють фахівці та оператори у даній галузі, а також наукова складова. Головними суб'єктами провадження державної політики у сфері захисту критичної інфраструктури являються органи публічної влади [283], котрі, як відомо, не проводять власних наукових досліджень, а знання, необхідні їм для реалізації даної діяльності, отримують лише в закладах вищої освіти та спеціалізованих установах підвищення кваліфікації, на основі чого формується їх рівень компетентності. Відзначимо, що рівень компетентності публічних службовців з питань захисту критичної інфраструктури обумовлюється наявністю відповідних освітньо-професійних та освітньо-наукових програм у закладах вищої освіти держави. Тому, варто припустити, що, що рівень інституційної спроможності національної системи захисту критичної інфраструктури напряму залежить від якості освіти та наявності й ефективності профільних науково-аналітичних центрів, що провадять практичні дослідження у цій сфері.

Відповідно має бути забезпечено взаємодію та співпрацю з науковими та навчальними установами у напрямі підвищення

компетентності працівників органів публічного управління, тобто сформовано систему підготовки кадрів щодо захисту критичної інфраструктури. Нагадаємо, що Концепцією створення державної системи захисту критичної інфраструктури, схваленої Розпорядженням КМУ № 1009-р від 06.12.2017 р. [230], одним зі шляхів розв'язання зазначеної проблеми визначено «створення системи підготовки та перепідготовки кадрів у сфері захисту критичної інфраструктури» [230]. Окрім цього, Національний плану захисту та забезпечення безпеки та стійкості критичної інфраструктури [228] передбачає більш конкретизовані заходи, серед яких особливу увагу привертає посилення освітньої складової у забезпеченні спроможності системи забезпечення безпеки та стійкості критичної інфраструктури.

Прогалиною у компетентнісному векторі забезпечення інституційної спроможності національної системи захисту критичної інфраструктури вважаємо відсутність у Національному класифікаторі професій України [132] професії з питань державного управління у сфері захисту критичної інфраструктури та безпеки критичної інфраструктури вцілому. Аналізуючи зміст документу, констатуємо наявність професій із приналежністю до окремих секторів критичної інфраструктури: соціальний захист населення (шифр 2446); цивільний захист (1120.1); захист інформації (1210.1); фізичний захист (сфера використання ядерної енергії) (1222.2); енергетична сфера (2143.2); електрохімічний захист (2146.2); захист інформації з обмеженим доступом (2149.2); захист секретної інформації (3439); радіаційний та хімічний захист (3439); газовий захист (5169); захист підземних трубопроводів (7241). Розділ 4.1 Класифікатора «законодавці», «вищі державні службовці», «менеджери» взагалі не представлений відповідними професіями з питань безпеки стратегічної інфраструктури. Також розділ 4.2 «професіонали» містить професії, пов'язані тільки з соціальним та цивільним захистом населення та захистом інформації, при цьому інші сектори критичної інфраструктури

відсутні, що знижує інституційну спроможність національної системи захисту критичної інфраструктури.

Також варто звернути увагу на ст. 49 Закону України «Про Державну службу» [56], де передбачено наявність індивідуальних програм підвищення рівня професійної компетентності державного службовця, яка розробляється відомчою службою управління персоналом. Центральним органом виконавчої влади з провадження державної політики у сфері державної служби є Національне агентство України з питань державної служби, яке відповідно до покладених на нього завдань сприяє розвитку системи закладів освіти надає освітні послуги з підготовки, спеціалізації та підвищення кваліфікації державних службовців, а також організовує та координує підготовку здобувачів вищої освіти за освітнім ступенем магістра за спеціальністю 281 «Публічне управління та адміністрування».

Ґрунтуючись на положеннях загальної теорії державного управління [44, с. 15], державну політику безпеки варто трактувати крізь діоптрій формотворчого виміру соціально-економічної системи, схильному до еклектичності внутрішніх зв’язків населення, об’єктів території, економіки, інфраструктури та управлінських інститутів [87, с. 190]. З огляду на вищезазначене, можна виділити ще один (найважливіший) вид інституційної здатності – стратегічну (багатофункціональну) здатність.

Аналізуючи сучасну структурно-функціональну характеристику вітчизняної державної політики у сфері захисту критичної інфраструктури, розглянемо спроможність ключового інституту – уповноваженого органу з питань захисту критичної інфраструктури України (Держспецзв’язку) [159]. Зробити це можемо на основі аналізу Звіту про відстеження результативності постанови КМУ № 1109 від 09.10.2020 р. «Деякі питання об’єктів критичної інфраструктури» [78] за підсумками 2022 року.

Згідно із даними, на листопад 2023 року було ідентифіковано,

категоризовановано, утверджено та внесено до Реєстру:

– 159 об’єктів критичної інфраструктури паливно-енергетичного сектору, відповідальний секторальний орган – Міністерство енергетики України;

– 5 об’єктів критичної інфраструктури відповідальний секторальний орган – Міністерством з питань стратегічних галузей промисловості України;

– 3 об’єкта критичної інфраструктури відповідальний секторальний орган – Міністерство охорони здоров’я України та Міністерство розвитку громад та територій України.

За останнім пунктом варто відзначити, що перелік наразі створений, проте, дані до Держспецзв’язку ще не подано. Окрім цього іншими секторальними органами у сфері захисту критичної інфраструктури перелік таких об’єктів досі не сформовано по своїх секторах (підсекторах). Отже, за результатами аналізу зазначеного Звіту, резюмуємо, що відомості відносно секторальних переліків об’єктів критичної інфраструктури надали до Адміністрації Держспецзв’язку лише чотири міністерства: Міністерство енергетики, Міністерство з питань стратегічних галузей промисловості, Міністерством розвитку громад та територій, Міністерство охорони здоров’я. Відносно перспектив інформаційного наповнення Реєстру об’єктів критичної інфраструктури у звіті Держспецзвязку вказано, що «на даний час продовжується робота над формуванням секторальних та зведеного переліків об’єктів критичної інфраструктури на основі наданої інформації від міністерств, центральних органів виконавчої влади, державних органів, операторів критичної інфраструктури, фізичних та юридичних осіб які є потенційно визначеними об’єктами критичної інфраструктури. Надається консультативна та методична допомога щодо ідентифікації, категоризації та віднесення об’єктів до об’єктів критичної інфраструктури» [78].

На сайті Держспецзв’язку [159] наголошується, що Адміністрацією

перед Кабміном неодноразово ставилося питання щодо невиконання секторальними органами у сфері захисту критичної інфраструктури, завдань з ідентифікації та категоризації об'єктів визначеними Постановою по відповідним секторам (підсекторам). Даний факт можна вважати підтвердженням низької інституційної спроможності даних інститутів. Також уповноваженим органом з питань захисту критичної інфраструктури України встановлено, що оцінка результатів та ступеня досягнення визначених цілей із наповнення Реєстру об'єктів критичної інфраструктури проводитиметься з інтервалом у три роки після проведення повторного відстеження. Даний термін вважаємо за необхідне скоротити, з метою активізації даного процесу, оскільки наступні перевірки відбудуться не раніше 2026 року. Зауважимо, що відповідальність за безпеку об'єкта несе його оператор, а держава не має повноважень втручатися у безпеку приватних об'єктів критичної інфраструктури та може бути лише партнером у її забезпеченні [60]. У такому випадку вважаємо, що оперативність ідентифікації та категоризації об'єктів інфраструктури як критично важливих сприятиме посиленню дієвості державної політики у сфері захисту критичної інфраструктури.

Зазначимо, що експліцитність інституційної спроможності національної системи захисту критичної інфраструктури імплікує комплементарність ряду паралельно функціонуючих систем:

1. Єдиної державної системи цивільного захисту (ЄДСЦЗ). Представляє собою об'єднання сил і засобів центральних та місцевих органів виконавчої влади, органів управління, виконавчих органів рад, підприємств, інших установ та організацій, котрі забезпечують реалізацію державної політики у сфері цивільного захисту. В межах ЄДСЦЗ центральними органами виконавчої влади у відповідних сферах суспільного життя створюються функціональні та територіальні підсистеми [206].

2. Єдина державна система запобігання, реагування та припинення

терористичних актів і мінімізації їх наслідків (ЄСЗРПТА). Інституційну спроможність системи протидії тероризму в Україні регламентують Конституція та Закони «Про боротьбу з тероризмом» [52]. Силами протидії тероризму (СПТ) є, перш за все, спеціально уповноважені Урядом суб'єкти виконавчої влади у питаннях протидії тероризму і захисту населення, об'єктів критичної інфраструктури та територій від загроз терористичного характеру: СБУ, МВС, ДСНС. Одним із основоположних органів у цій системі є Служба безпеки України. Для цього у своїй структурі містить Антитерористичний центр (АТЦ), сформований у грудні 1998 року Указом Президента України № 1343/98 від 11.12.1998 р. «Про Антитерористичний центр» [272]. АТЦ регулює діяльність суб'єктів боротьби з тероризмом з метою протидії терактам та запобігання диверсіям на об'єктах критичної інфраструктури.

До компетенції названих сил входять завдання ліквідації та попередження наслідків, викликаних терористичними акціями на об'єктах критичної інфраструктури. запобігання терористичній діяльності на об'єктах критичної інфраструктури, у тому числі превенція терактів; сповіщення населення про загрози можливих терактів на об'єктах критичної інфраструктури; убезпечення об'єктів критичної інфраструктури від потенційних терористичних дій. Серед основних заходів варто зазначити:

– проведення комплексних перевірок антитерористичної захищеності (уразливості) об'єктів критичної інфраструктури та їх категорування за ступенем потенційної небезпеки;

– залучення до обов'язкової антитерористичної паспортизації об'єктів критичної інфраструктури в терористичному відношенні;

– підготовка списку об'єктів критичної інфраструктури особливо уразливих та небезпечних в терористичному плані;

– розробка та подання антитерористичної комісії на затвердження методичних рекомендацій щодо реагування на кризові ситуації, які

виникають внаслідок диверсійно-терористичних актів на об’єктах критичної інфраструктури;

– залучення до розробки державних стандартів, нормативів та інших обов’язкових вимог відносно антитерористичної захищеності об’єктів критичної інфраструктури;

– коригування організаційних, режимних та оперативних заходів по організації антитерористичної захищеності об’єктів критичної інфраструктури на підставі розробки моделі загроз;

– організація систематичного проведення з персоналом і співробітниками охорони об’єктів відпрацювань порядку дій при виникненні загроз терористичних актів і в умовах їх настання.

3. Державна система фізичного захисту (ДСФЗ). Відповідно до Закону України № 2064-III від 19.10.2000 р. «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» [75] фізичний захист визначено як «діяльність у сфері використання ядерної енергії, спрямована на забезпечення захищеності ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання та на зміцнення режиму нерозповсюдження ядерної зброї» [75]. До об’єктів ДСФЗ включено ядерні об’єкти та установки, призначені для поводження з радіоактивними відходами, радіоактивні відходи, ядерні матеріали, радіоактивні матеріали, виявлені в незаконному обігу, інші джерела іонізуючого випромінювання [211]. Функціонування даної системи ґрунтується на результатах оцінки загроз вчинення диверсій.

До суб’єктів ДСФЗ належать: Державна інспекція ядерного регулювання України, центральні та місцеві органи виконавчої влади, Національна гвардія України, Національна академія наук України щодо фізичного захисту, СБУ, а також ліцензіати, які беруть участь у забезпеченні фізичного захисту.

4. Національна система кібербезпеки (НСК). Згідно ст.8 Закону

України «Про основні засади забезпечення кібербезпеки України» [68] національна система кібербезпеки – «це сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури» [68].

Основними суб'єктами НСК є Держспецзв'язку, СБУ, НБУ, Національна поліція України, розвідувальні органи, Міністерство оборони України та Генеральний штаб ЗСУ. Координатором реалізації цієї Стратегії є робочий орган РНБО України – Національний координаційний центр кібербезпеки [242].

Важливим кроком у ампліфікації інституційної спроможності Національної системи кібербезпеки стало рішення РНБО України від 14.05.2021 р. «Про Стратегію кібербезпеки України» [268], яку ввів у дію Указ Президента України №447 від 14.05.2021 р. 30 грудня 2021 року, розглянувши проект Плану реалізації Стратегії кібербезпеки України, який був поданий Національним координаційним центром кібербезпеки, РНБО його схвалила та Указом Президента України № 37/2022 від 01.02.2022 р. було введено в дію. Головним тезисом зазначеної інституції є пріоритет у посиленні спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному динамічному середовищі. Гібридну агресію російської федерації проти України у кіберпросторі визначено першочерговою загрозою для критичної інфраструктури. Кіберпростір визнано одним з можливих театрів воєнних дій у якому посилюється тенденція зі створення кібервійськ. До прямих завдань останніх віднесено «забезпечення захисту критичної інформаційної інфраструктури від кібератак», а також «проведення

превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника» [268].

Основними напрямами державної політики у напрямку забезпечення інституційної спроможності Національної системи кібербезпеки визначено: створення захищеного національного сегмента кіберпростору; запобігання втручанню у внутрішні справи України з боку інших країн, боротьба з кіберзлочинністю та кібертероризмом, укріплення обороноздатності в кіберпросторі, посилення стійкості кіберзахисту, дотримання міжнародних зобов'язань щодо боротьби з кіберзлочинністю та кібертероризмом [268].

Продовжуючи аналізувати інституційну спроможність національної системи захисту критичної інфраструктури, варто провести оцінку ефективності кіберзахисту критичних об'єктів. З цією метою звернемо увагу на інструмент вимірювання NCSI, який застосовують для оцінки потенціалу кібербезпеки країни ЄС на основі розрахунку Індексу національної спроможності кіберзахисту (НСК). Модель розроблено Академією електронного управління (eGA) [157]. Дана організація є спільною ініціативою Уряду Естонії, Інституту відкритого суспільства (OSI) та Програми розвитку Організації Об'єднаних Націй. Основні функції даного інституту полягають у висвітленні проблем кібербезпеки, які потребують уваги уряду, і в допомозі у розбудові національного потенціалу кібербезпеки. NCSI – це інструмент для вимірювання та нарощування потенціалу національної кібербезпеки. NCSI вимірює готовність країн до запобігання реалізації фундаментальних кіберзагроз і готовність керувати кіберінцидентами, злочинами та масштабними кіберкризами. Фокус аналізу зосереджено на кіберпотужності національного рівня захисту об'єктів критичної інфраструктури та базується на ключових принципах:

– об'єднує результати всіх позитивно оцінених критеріїв;

– оцінка інституційної спроможності базується на чітко вимірних

аспектах – законодавстві, організаційній спроможності, політиках захисту, форматах міжсекторальної співпраці, технологіях та їх ефективності;

– відстежується прогрес держави у порівнянні з іншими країнами;

– дозволяє порівняти розвиток кібербезпеки країн із глобальним цифровим розвитком;

– аналіз універсальний та сумісний із законодавством ЄС щодо кібербезпеки [157].

Індекс НСК включає оцінку 12 профілів національних спроможностей кібербезпеки, які організовані у три групи: загальні спроможності кібербезпеки, базові спроможності та спроможності управління інцидентами та кризами. Вони вимірюються за допомогою загалом 46 індикаторів, заснованих на фактичних даних, які включають законодавство, створені організації, формати співпраці, навчальні програми, тренування тощо [157]. Індекс розраховується у 5 кроків:

1. Визначення кіберзагроз національного рівня..

2. Визначення заходів та можливостей кібербезпеки.

3. Вибір важливих та вимірних аспектів.

4. Розробка показників кібербезпеки.

5. Групування показників кібербезпеки.

Відзначимо, що у десятку зі 176 країн із найвищою інституційною спроможністю кібербезпеки входять Греція, Чехія, Естонія, Іспанія, Литва, Франція, Фінляндія, Данія, Нідерланди та Німеччина.

Індекс НСК базується на квадро-комплексі вимірників спроможності державної політики у сфері кібербезпеки критичної інфраструктури:

1. Спроможність чинного законодавства – дієвість та повнота нормативно-правової бази (законів, постанов, наказів та ін.).

2. Спроможність діючих підрозділів захисту – ефективність існуючих організацій, департаментів, служб та ін.

3. Спроможність формату міжсекторальної співпраці – наявність та ліквідність створених комітетів, робочих груп та ін.

4. Спроможні результати – дієвість державної політики, заходів,

технологій, веб-сайтів, програмного забезпечення та ін.

Загальну ієрархію набору показників розподілено на 3 категорії, 12 напрямків (табл.2.1) та 46 показників (Додаток А).

Таблиця 2.1

Дані спроможності державної політики кіберзахисту об'єктів критичної інфраструктури України у 2023 році

Категорія спроможності	Напрямок спроможності	Бал спроможності	
		фактичне значення	максимальне значення
Загальні показники кібербезпеки	Розробка політики кібербезпеки	7	7
	Аналіз кіберзагроз та інформація	4	5
	Освіта та професійний розвиток	8	9
	Внесок у глобальну кібербезпеку	2	6
Базові показники кібербезпеки	Захист цифрових сервісів	1	5
	Захист основних послуг	6	6
	Електронна ідентифікація та довірчі послуги	9	9
	Захист персональних даних	4	4
Показники управління інцидентами та кризи	Реагування на кіберінциденти	4	6
	Управління кіберкризою	3	5
	Боротьба з кіберзлочинністю	9	9
	Військові кібероперації	1	6

Джерело: розраховано за даними [157]

Оцінка індексу НСК показує відсоток, який країна отримала від максимального значення показників. Максимальна оцінка NCSI завжди дорівнює 100 (100%), незалежно від того, додано чи видалено індикатори.

$$\text{Індекс НСК} = \frac{\sum \text{балів спроможності} * 100\%}{\sum \text{Максимальне значення балів спроможності}} \qquad (2.1.)$$

Окрім оцінки Індексу НСК, таблиця індексів також показує рівень цифрового розвитку (РЦР) шляхом обрахунку Індексу РЦР, який розраховується відповідно до індексу розвитку інноваційних комп'ютерних технологій (Індекс ІКТ) та індексу стійкості мереж (Індекс СМ). Індекс РЦР – це середній відсоток, який країна отримала від максимального значення обох індексів (СМ+ІКТ).

$$\text{Індекс РЦР} = \frac{\text{Індекс СМ (\%)} + \text{Індекс ІКТ(\%)}}{2} \qquad (2.2.)$$

Ще один індикатор – різниця між Індексом НСК та індексом РЦР (табл. 2.2).

Таблиця 2.2

Світовий рейтинг спроможності державної політики кіберзахисту об'єктів критичної інфраструктури на основі Індексу НСК у 2023 році

Місце в рангу	**Країна**	**Індекс НСК**	**Індекс РЦР**	**Різниця**
1.	Бельгія	**94,81**	74.07	20.74
2.	Литва	**93,51**	67,34	26.17
3.	Естонія	**93,51**	75,59	17.92
4.	Чехія	**90,91**	69.21	21.70
5.	Німеччина	**90,91**	80.01	10.90
6.	Румунія	**89,61**	59,84	29.77
7.	Греція	**89,61**	64.02	25.59
8.	Португалія	**89,61**	68,46	21.15
9.	Великобританія	**89,61**	79,96	9,65
10.	Іспанія	**88.31**	72.21	16.10
24.	**Україна**	**75,32**	**55,96**	**19.36**

Джерело: сформовано за даними [157]

Вказаний індекс показує зв'язок між спроможністю кіберзахисту критичної інфраструктури та рівнем цифровізації суспільства. Позитивний показник показує, що розвиток кібербезпеки відповідає або випереджає рівень цифрового розвитку, що демонструє спроможність кіберзахисту. Негативний результат показує, що цифрове суспільство країни є більш розвиненим, ніж сфера кібербезпеки, що ставить під загрозу спроможність кіберзахисту критичної інфраструктури

Проведений аналіз показників спроможності національної системи захисту критичної інфраструктури в Україні на основі Індексу НСК у 2023 році, дозволило виявити наступні проблеми:

– освітні програми підготовки спеціалістів в країні не включають компетенції з кібербезпеки/комп'ютерної безпеки об'єктів критичної інфраструктури, а також відсутні спеціальності орієнтовані на захист об'єктів критичної інфраструктури вцілому;

– в Україні не розміщено жодного представництва регіональної або

міжнародної організації з кібербезпеки, та безпеки об’єктів критичної інфраструктури;

– Україна не брала участі у співфінансуванні або співорганізації жодного проєкту з розбудови потенціалу захисту критичної інфраструктури для іншої країни за останні 3 роки;

– відсутність компетентного наглядового органу за результативністю державної політики у сфері захисту критичної інфраструктури;

– Урядом не розроблено Плану врегулювання кризових ситуацій на випадок масштабних кіберінцидентів та аварій на об’єктах критичної інфраструктури, не врегульовано законодавством порядок залучення волонтерів у сферу кібербезпеки та захисту критичної інфраструктури;

– Збройні Сили України не проводили в країні навчання з кібероперацій або навчання з компонентом кібероперацій протягом останніх 3 років;

– не прийнято закон про створення та функціонування у системі Міністерства оборони України кібервійськ;

– у національній системі захисту критичної інфраструктури відсутні підрозділи кібероперацій, Збройні сили України досі не мають підрозділу кібервійська та кіберкомандування, який би спеціалізувався на плануванні та проведенні кібероперацій і спільних навчань з кіберполіцією із проведення кібероперацій;

– не сформовано перелік об’єктів критичної інформаційної інфраструктури та повільно проходить наповнення Реєстру об’єктів критичної інфраструктури;

– не розроблено дієву модель міжсекторальної співпраці у сфері захисту критичної інфраструктури та залучення стейкхолдерів на основі державно-приватного партнерства;

– брак фінансування, що не дозволяє державним інститутам у повній мірі займатися розробкою дієвих систем кіберзахисту, що вимагає залучення

аутсорсу;

– відсутність державного мультиплексу, що в умовах війни не дозволяє в повній мірі контролювати медіа простір;

– відсутність державної інстанції, відповідальної за аналіз, обробку даних про інциденти (кризи) на об'єктах критичної інфраструктури та її структурування з метою обміну досвідом та створення програм міжсекторального співробітництва у сфері стійкості та захисту критичної інфраструктури.

Проведений аналіз інституційно-правових особливостей національної системи захисту критичної інфраструктури підтвердив необхідність сфокусувати увагу на проблемі обширності суб'єктного складу, що детермінує низьку скоординованість режимів роботи, процедур і планів реагування на різні комплекси ризиків і загроз у сфері захисту критичної інфраструктури. Окрім цього, визначені у планах і положеннях процедури й механізми інтеракції між суб'єктами національних систем безпеки і кризового реагування є недостатньо відтренованими та апробованими у прецедентах масштабних та системних кризових явищ. Це можна пояснити слабкою розвинутістю до цього часу в країні практики міжвідомчих та міжсекторальних тренувань і навчань на рівнях, вищих ніж об'єктовий. Напрацьована база інституції у напрямку посилення інституційної спроможності передбачає застосування більш виваженого підходу до нормопроектувальної діяльності із використання сучасної юридичної техніки та залученням до даних питань фахівців-юристів. Зокрема розробка вимог та комплексний моніторинг рівня захищеності об'єктів критичної інфраструктури надасть можливість досягти повноти та всебічності інституційної спроможності у виконанні вимог нормативно-правової бази, що детермінує цілісність і системність державної політики у цій сфері. При цьому, вважаємо доцільним посилити увагу до превентивних заходів забезпечення стійкості критичної інфраструктури та доповнити ними Національний план захисту та забезпечення безпеки та

стійкості критичної інфраструктури. Тобто організаційно-правова структура Національний плану матиме на меті протидію усім видам загроз та ризиків і стане вагомим елементом сучасної національної системи захисту критичної інфраструктури.

2.3. Аналіз сучасної парадигми державної політики у сфері захисту критичної інфраструктури в умовах воєнного стану.

Нинішня державна політика у сфері захисту об'єктів критичної інфраструктури в умовах воєнного стану виступає не окремою проблемою, а є органічною складовою вирішення комплексного завдання: формування системної державної парадигми політики національної безпеки, в рамках якої чільне місце посідає питання функціонування монолітної системи безпеки критичної інфраструктури в умовах військової агресії рф. Підтвердження даного судження можемо віднайти у Концепції створення державної системи захисту критичної інфраструктури [230], де прямо відзначалася необхідність інтеграції системного підходу в напрямок розв'язання проблеми на загальнодержавному рівні.

Акцентуємо увагу, що в умовах воєнного стану дієвість національних векторів державної політики у сфері захисту об'єктів критичної інфраструктури в Україні в теоретичному плані не вивчено. В такому випадку для створення раціональних структур управління вкрай важливим є осягнути складність і глибину актуальних проблем України в період воєнного стану та підвищених ризиків терактів на об'єктах критичної інфраструктури і врахувати їх при конструюванні архітектури майбутньої державної безпекової політики. При цьому, як зазначає А. В. Бєлоусов, необхідним є «зважений погляд на стан суспільства, його можливості та перспективи, ресурси, резерви, потенціал і джерела зростання» [6, с. 230].

Нагадаємо, що у зв'язку з російською військовою агресією, Президент України, на підставі ч.1 п.20 ст.106 Конституції України [96] та Закону України «Про правовий режим воєнного стану» [71] 24 лютого 2022 року

підписав Указ, яким запровадив воєнний стан. Воєнний стан – це «особливий правовий режим, що вводиться в країні або в окремих її місцевостях у разі збройної агресії чи загрози нападу, небезпеки державній незалежності України, її територіальній цілісності та передбачає надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки, усунення загрози небезпеки державній незалежності України, її територіальній цілісності, а також тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень» [71].

Варто зазначити, що прояви російської агресії систематично ігнорує міжнародні конвенції, у тому числі породжує аномію у сферах критичної інфраструктури [247]. До прикладу, в умовах війни більша частина об’єктів критичної інфраструктури знаходиться під захистом Додаткового протоколу до Женевських конвенцій від 12.07.1949 р.. Документ не містить власне формулювання терміну «критична інфраструктура», однак у ньому зазначено, що «будь які цивільні об’єкти не повинні бути об’єктом нападу або репресалій» [39]. Окрім цього, документ забороняє знищувати або піддавати нападу чи виводити з ладу об’єкти, потрібні для виживання цивільного населення. Окрім цього, у Додатковому протоколі утверджено чіткий перелік споруд і установок, які заборонено піддавати нападам, оскільки вони містять приховану небезпеку (атомні електростанції, греблі, дамби). Отже, можемо зробити висновок, що оскільки об’єкти критичної інфраструктури в Україні цілком підпадають під юрисдикцію даного документу. Однак офіційні дані підтверджують, що за одну зі стратегічних цілей ворог обрав саме об’єкти цивільної критичної інфраструктури, розташовані у глибокому тилу у вигляді електропідстанцій, об’єктів гідроенергетики, теплової генерації та ін.. Дані факти спричинили примусове

переміщення та знищення цивільного населення. Станом на травень 2023 р. приблизно 6,2 мільйона людей покинули Україну як біженці, а 5,4 мільйона осіб перебувають усередині країни в статусі внутрішньопереміщених осіб. Окрім цього, у вересні 2022 року російська влада провела референдуми на тимчасово окупованих територіях Донецької, Луганської та Херсонської і Запорізької областей. В рамках незаконної анексії, було захоплено ряд критично важливих інфраструктурних об'єктів [148].

З початку війни в Україні росія повністю зруйнувала більш ніж 700 об'єктів критичної інфраструктури, завдаючи найбільше атак, спрямованих на знищення енергетичної інфраструктури шляхом систематичних групових ракетних ударів з рубежів пуску над Каспійським морем, акваторії Чорного моря, а також військової авіації, застосовуючи широкий арсенал ракет (Х-101, Х-555, Іскандер, Циркон, Онікс, Калібр, Торнадо, С-300 та ін.), а також бойових безпілотних дронів-камікадзе «Shahed 136» та Mohajer 6 [161].

Авіаудари по енергетичним потужностям України почалися 10 жовтня. Наймасовіший обстріл об'єктів енергосистеми України ворог здійснив 15 листопада 2022 р., випустивши по території України близько 100 ракет. При цьому окремі із них було спрямовано на інфраструктуру АЕС. Зафіксовано перше загальнонаціональне відключення електроенергії. Це при тому, що завдяки відпрацюванню ППО вдається знищувати близько 80% запущених росією ракет та дронів [165]. Перші удари по енергосистемі спричинили дефіцит потужності на рівні 20%, а вцілому на початок 2023 року енергетичний сектор зазнав зниження функціональності на 61%. Таким чином довоєнна потужність у 36 Гігават (ГВт) знизилася до 13,9 ГВт. Окрім цього, близько 10 ГВт знаходиться на територіях під тимчасовим військовим контролем російської федерації, 6 ГВт з яких надходить із Запорізької АЕС. У таких умовах оператори були змушені обмежувати постачання електроенергії, щоб забезпечити роботу системи [165]. За оцінками Світового банку [174] та ПРООН [173], понад 12 мільйонів українців постраждали внаслідок пошкодження джерел енергії , що призводить до нормування

електроенергії та опалення.

Подальші атаки на критичну інфраструктуру вплинули на роботу трьох атомних електростанцій (у Нетішині, Южноукраїнську та Вараші). Додатково, знаходячись під окупацією, під постійним ризиком аварії функціонує найбільша в Європі атомна електростанція – Запорізька. Встановлені факти «інфраструктурного тероризму» становлять загрозу не лише для постачання електроенергії [148], але, у разі руйнування 15 реакторів українських АЕС, населення України, а також і Європи опиниться в умовах глобальної ядерної катастрофи, в десятки разів потужнішої ніж аварія у квітні 1986 року на Чорнобильській АЕС.

Наступною за масштабом деструктивною ситуацією у критичній інфраструктурі України, став підрив 6 червня.2023 р. дамби Каховської ГЕС в Херсонській області. Це призвело до масового затоплення території країни на площі близько 180 км². Висота рівнів води сягала 5-6 метрів. Даний інфраструктурний об'єкт був джерелом питної води для 700 тис. людей та зрошувальних систем 584 тис га с.-г. угідь на півдні України [148]. Даний терористичний акт спричинив хвилю додаткових пошкоджень інших об'єктів критичної інфраструктури (комунального сектора, сільського господарства та ін..). Прямі збитки від підриву Каховської ГЕС оцінюються у більш ніж 2 млрд дол. США із яких на критичну інфраструктуру припадає близько 950 млн дол. США [148].

Підрив Каховської ГЕС завдав додаткових збитків енергетиці у $586 млн, за рахунок безповоротної втрати ще 334,8 МВт потужностей. Таким чином, загальні збитки енергетиці сягнули $624 млн. Збитки, завдані транспортній інфраструктурі, сягнули $311 млн. За оцінками KSE Institute [148], понад 290 км доріг постраждали від повені. Знищення посівів сільськогосподарських культур, поголів'я худоби та риби завдали збитків агросектору на $25 млн. Орієнтовна сума збитків, завданих навколишньому середовищу, оцінюється у $1,5 млрд. Міністерства захисту довкілля та природних ресурсів [166].

З початку війни в Україні пошкоджень зазнали 18 аеропортів і цивільних аеродромів, 344 мости та мостові переходи, а також понад 25 тисяч кілометрів автомобільних шляхів. Сфера освіти, за оцінками KSE Institute [148], на початок вересня 2023 р. отримала збитків близько 10.1 млрд дол США. Загальна кількість пошкоджених та зруйнованих освітніх об'єктів вже перевищила 3,5 тис. із яких – понад 1,7 тис. закладів середньої освіти, більше 1,0 тис. – дошкільної та 586 – вищої освіти. Зруйновано або пошкоджено 1223 медзаклади, з них – 384 лікарні та 352 амбулаторії. На вересень 2023 року зруйновано або пошкоджено війною близько 167,2 тис житлових об'єктів із яких 19,1 тис. багатоквартирних та 147,8 тис. приватних будинків, а також 350 гуртожитків. Найбільше пошкоджених об'єктів критичної інфраструктури зафіксовано у Донецькій, Харківській, Луганській, Запорізькій, Херсонській Дніпропетровській, Одеській та Миколаївській областях. Дані регіони найбільше постраждали з точки зору прямої шкоди цивільній та критичній інфраструктурі та економічних наслідків.

За підсумками 2022 року, за оцінками Світового банку, ВВП України скоротився на 29,2%, а рівень бідності зріс на 24,1%. Станом на 01.09.2023 р. загальна сума прямих задокументованих збитків, завдана критичній інфраструктурі України становила до $151,2 млрд., що більше на $700 млн, порівняно з червнем 2023 року [174].

Можемо дійти висновку, що всупереч міжнародним правилам війни, знищуючи цивільну критичну інфраструктуру України, агресор намагається маніпулювати морально-психологічним станом цивільного населення. Формуючи, тим самим, внутрішній страх потенційних проблем (відсутність взимку електроенергії, тепла, питної води, медичного обслуговування транспортного сполучення та ін.), намагається доповнити комплекс активних бойових дій та змусити українську владу прийняти свої умови.

Аналізуючи сучасну парадигму державної політики у сфері захисту критичної інфраструктури в умовах воєнного стану, варто звернути увагу на

працю О. Ю. Кондратенка, який досліджуючи зовнішню геоекономічну політику щодо України акцентує увагу на намірах рф спрямувати військову агресію, на підрив суверенітету та незалежності України, а також перетворення її на «буферну зону» безпеки відносно євроатлантичних інститутів [94, с. 15]. В. А. Ліпкан, аналізуючи дані умови, звертає увагу також на ідеологічне просування деструктивного простору політикою країни-агресора наративи концепції «failed state» [113, с. 272]. Дане припущення у своїх дослідженнях ще у 2000 році висвітлив З. К. Бжезінський, який резюмував що «…більша частина сучасної російської політичної еліти вважає Україну неправомірно утвореною державою; не лише незаконним, а й неприроднім державним утворенням...» [7, с.14]. Отже, можна зробити висновки, що спроба військової експансії рф території незалежної України було лише питанням часу. У даному випадку варто навести аргумент важливості забезпечення стійкості критичної інфраструктури, а саме думку Г. Ю. Зубка [86, с. 80], який, вивчаючи тематику інфраструктурної війни, наголошує, що руйнування критичної інфраструктури супротивника відкриває шлях до встановлення домінування над країною. Ці прояви генерують нові стратегічні виклики у сфері державної політики захисту критичної інфраструктури та закладають науковий дискурс щодо можливостей, інтелектуальних спроможностей, технічних засобів та власних сил і ресурсів спроможних інспірувати підвалини протидії інформаційним та ідеологічним загрозам.

Аналізуючи ретроспективу формування сучасної парадигми державної політики у сфері захисту критичної інфраструктури слід узагальнити аксіоматичні припущення стосовно фатальних стратегічних прорахунків, які були допущені у безпековій політиці незалежної України:

1. Прийняття без’ядерного статусу. Ще в Декларації про державний суверенітет 16 липня 1990 року [32] передбачалося, що Україна прагне позбутися ядерної зброї. 14 січня 1994 року було підписано Тристоронню заяву Президентів України, США та Росії (Леонідом Кравчуком, Біллом

Клінтоном і Борисом Єльциним), у якій було проголошено про те, що «всі ядерні боєзаряди будуть виведені з території України до Росії для цілей їх наступного розукомплектування у якомога коротший можливий час» [262]. 5 грудня 1994 року у Будапешті , між Україною, Росією, Великою Британією та США було укладено Меморандум про гарантії безпеки у зв'язку з приєднанням України до Договору про нерозповсюдження ядерної зброї. Документ передбачав гарантії безпеки для України у зв'язку з набуттям нею неядерного статусу [117].

2. Позиція нейтралітету та позаблоковий статус. Окрім без'ядерного статусу, Україна вирішила заявити ще й про нейтральність, позаблоковість і багатовекторність. Це все було виписано в Конституції 1996 року [96], а додатково у Законі України «Про засади внутрішньої і зовнішньої політики» № 2411-VI від 01.07.2010 р. було прописано що «Україна як європейська позаблокова держава здійснює відкриту зовнішню політику і прагне співробітництва з усіма заінтересованими партнерами, уникаючи залежності від окремих держав, груп держав чи міжнародних структур» [58]. Головними причинами запровадження позаблокового статусу України В. Т. Шатун [280] вбачає:

– низьку результативність політики України у євроінтеграційному векторі;

– політичний та економічний тиск росії;

– вплив проросійського політичного лобі на безпекову політику України;

– низька політична дієздатність і конкурентоспроможність української управлінської еліти;

– низький рівень суспільної підтримки курсу на євроатлантичну інтеграцію через брак і недоліки інформаційної політики держави.

3. Демілітаризація та штучна деградація обороноздатності суб'єктів системи забезпечення національної безпеки та захисту критичної інфраструктури.

4. Трансформація корупції на системоутворюючий чинник функціонування системи державної влади [83, с. 180].

5. Підписання «Угоди між Україною і Російською Федерацією про статус та умови перебування воєнної бази Чорноморського флоту Російської Федерації на території України» [264], що укладалася на 20 років.

6. Не були вирішені питання розмежування між Росією та Україною акваторії Азовського моря та проведення лінії державного кордону в Керченській протоці.

Саме ці прогалини у державній політиці національної безпеки на нашу думку сприяли стратегічному дисбалансу військових сил у геопросторовому позиціонуванні України як незалежної держави та детермінували формування стратегічних загроз для критичної інфраструктури.

Український стратегічний шлях передбачає її повноцінне приєднання («повернення») до західної цивілізації, інтеграцію до європейських та євроатлантичних структур. У геоекономічному контексті, попри всі труднощі, стратегічний курс України на вступ до ЄС покликаний забезпечити її економічне піднесення до рівня розвиненої високотехнологічної держави з достойним рівнем життя населення. Війна з росією фактично вирішує декілька важливих тактичних завдань у воєнній сфері:

1) знищення значних арсеналів застарілої радянської зброї;

2) знищення зброї країни-агресора;

3) постачання Україні в особливо великих розмірах надсучасної зброї за стандартами НАТО;

4) навчання персоналу щодо ефективного оперування сучасною зброєю, організацію підготовки, перепідготовки і підвищення кваліфікації щодо оперування сучасною зброєю;

5) оволодіння технікою і навичками ведення бою за стандартами НАТО.

Одним зі складників сучасної парадигми державної політики у сфері

захисту критичної інфраструктури в умовах правового режиму воєнного стану є напрямки протидії агресії рф. До таких напрямків варто віднести:

– мілітарний дискурс для України на порядку денному міжнародної спільноти;

– персональні та економічні санкції проти росії;

– політика «стримування» росії західним державам на чолі зі США що проявляється допомогою Україні фінансами, новітніми технологіями, військовим спорядженням та ін. [29, с. 73];

– ефективна стратегія інформаційної війни та забезпечення поширення у світі правдивої інформації про події, що відбуваються нині в країні;

– досягнення сумісності Збройних Сил із збройними силами держав – членів НАТО, розвиток спроможностей щодо отримання допомоги від іноземних партнерів та її надання іншим державам озброєння України та підготовка військових відповідно до стандартів НАТО [224, с. 345];

– створення дієвої системи територіальної оборони з використанням кращого досвіду країн з розвинутою територіальною обороною; розвиток військово-патріотичного виховання;

– забезпечення ефективності оборонного менеджменту, професійності та вмотивованості персоналу сил оборони, чисельності воєнного резерву, розвинутої військової інфраструктури, логістики та запасів матеріальних засобів;

– активні навчання й тренування представників інститутів державної влади, сил безпеки та оборони, зокрема за участі іноземних держав та НАТО, щодо комплексного реагування на різні загрози [224, с. 337].

Аналізуючи державну політику в сфері захисту критичної інфраструктури в умовах правового режиму воєнного стану, сліз зазначити, що задля посилення захисту критичної інфраструктури, військове командування у тандемі з військовими адміністраціями може змінювати охорону об’єктів життєзабезпечення населення та критичної інфраструктури, а також запроваджувати особливий режим їх роботи, вводити трудову

повинність для осіб не задіяних в оборонній сфері (з метою виконання робіт оборонного характеру для захисту критичної інфраструктури), ініціювати заборону діяльності громадських об'єднань, політичних партій та інших об'єднань якщо вона може порушити стійкість критичної інфраструктури [71].

У таких умовах порядок особливого режиму та роботи об'єктів критичної інфраструктури затверджуються Кабінетом Міністрів України. Однак, відзначимо, що у теорії державного управління не існує універсального інституційного шаблону, що визначало б стандартний алгоритм захисту критичної інфраструктури. Саме тому, завданням Уряду є формування власних автентичних протоколів, опираючись на аналіз поточної ситуації в країні крізь призму базових показників:

- основи конституційного ладу країни;
- каталог прогнозних і поточних критичних ризиків і загроз;
- кон'юнктура та структура економіки;
- етнічна культура нації та суспільно-політичний стан в країні;
- загальний інституційний досвід у державному управлінні.

Прислухаємось до наукового підходу вчених Д. С. Бірюкова та С. І. Кондратова [10, с. 76] стосовно архітектури державної політики захисту критичної інфраструктури, де вчені пропонують розвивати вектор державної політики у сфері захисту критичної інфраструктури у світлі дуальної моделі:

1. Модель, що базується на принципах стимулювання, саморегулювання та добровільності дотримання стандартів. Дана модель опирається на політику ліберального управління, та посилює участь стейкхолдерів інфраструктурних об'єктів, яким надається можливість докласти зусиль до процесу захисту критичної інфраструктури. Такі зусилля можуть бути як у дорадчій так і фізичній формі.

2. Модель, що базується на принципах обов'язковості та відповідальності. Головний зміст передбачає обов'язковість виконання правових норм в рамках державної політики у сфері захисту критичної

інфраструктури та супроводжується санкціями відносно операторів об’єктів критичної інфраструктури за порушення вимог безпеки.

Варто акцентувати увагу на поширеній у іноземних країн практиці інституційної інтегрції у державну політику комбінацій окремих елементів обох зазначених моделей. Такі перспективи у розбудові парадигми державної політики захисту критичної інфраструктури в Україні на основі світового досвіду вивчав учений Д. Г. Бобро [12, с. 7]. Нам імпонує перелік ключових кроків, які виокремив учений у цьому напрямі:

1. Конструювання автентичної інституційно-правової бази та її регулярне удосконалення.

2. Ідентифікація координуючого органу, як, наприклад, у США – Департамент внутрішньої безпеки (Department of Homeland Security), до складу якого включено 22 федеральних агентства із загальною чисельністю персоналу близько 170 тис. осіб.

3. Напрацювання методичних вказівок до формування реєстру об’єктів критичної інфраструктури, а також оцінки ризиків та загроз.

4. Створення планів оперативного реагування та систематична переоцінка їх дієвості. Наприклад, у США цим займається National infrastructure simulation and analysis center (Національний центр аналізу та імітаційного моделювання інфраструктури) [150].

5. Організація підготовки кадрового потенціалу в сфері захисту критичної інфраструктури.

6. Налагодження оперативної співпраці, інформаційного обміну та вивчення кращих практик.

7. Розвиток державно-приватного партнерства [14].

Реалізація в Україні парадигми державної політики у сфері захисту критичної інфраструктури в умовах правового режиму воєнного стану неможлива без розподілу специфічних функцій управління між спеціальними державними органами.

Це частково викликано тим, що сьогодні Україна зіткнулася із гострою

потребою оперативної адаптації векторів державної політики до умов протидії численним гібридним загрозам з боку країни агресора, котрі вона свідомо спрямовує на руйнацію суверенітету та територіальної цілісності держави. Аналізуючи досягнуті Україною успіхи у сучасній парадигмі державної політики у сфері захисту критичної інфраструктури, що формувалась в умовах воєнного стану, відзначимо створення власної архітектури комплексного аналітичного процесу забезпечення захисту об'єктів критичної інфраструктури, що включає:

– алгоритм ідентифікації секторів критичної інфраструктури;

– визначення спектру актуальних ризиків та загроз для об'єктів критичної інфраструктури;

– формування Реєстру об'єктів критичної інфраструктури;

– ідентифікацію суб'єктного складу із провадження державної політики у сфері захисту критичної інфраструктури;

– суттєву модернізацію інституційно-правового забезпечення державної політики у сфері захисту об'єктів критичної інфраструктури;

– розробку алгоритмів та протоколів вжиття відповідних заходів із усунення наслідків руйнувань об'єктів критичної інфраструктури

– формування системи захисту критичної інфраструктури.

Не зважаючи на позитивні зрушення, слушним вважаємо зауваження Г. Ю. Зубка [85, с. 170], який наголошує на певній інституційній недосконалості державної політики у розрізі забезпечення захисту об'єктів критичної інфраструктури саме в умовах воєнного стану в Україні. Учений акцентує увагу на її стратегічній розпорошеності та рандомності та локальній фрагментарності. Розділяємо позицію науковця, що дані проблеми виступають певним інституційним бар'єром до модернізації стратегії національної безпеки. Опираючись на даний аргумент, актуалізуємо квестію щодо розробки моделі ефективної взаємодії і міжсекторальної координації суб'єктів державної політики в сфері захисту критичної інфраструктури. Дану позицію можна підсилити на прикладі успішного досвіду світових

країн, де структурна дифузія систем реагування на загрози, ризики та небезпеки у сфері захисту критичної інфраструктури є пріоритетним елементом державної політики. Наприклад, нормативно-правова база США характеризує здатність таких систем взаємодіяти між собою терміном «функціональна сумісність» [164]. Даний предикат передбачає оптимальну здатність обладнання та персоналу окремих структур оперативно реагувати, отримувати та надавати послуги та організаційну підтримку при реагуванні на надзвичайні ситуації у сфері захисту об'єктів критичної інфраструктури, пріоритетно рівню їх критичності.

Категоризація критичності об'єкта критичної інфраструктури, є окремими важливим елементом державної політики, та визначається на основі аналізу рівня негативного впливу внаслідок порушення або припинення функціонування об'єкта інфраструктури [124].

Визначення рівня негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури (секторальні критерії) відбувається відповідно до рівня негативного впливу: катастрофічні наслідки (4 бали), критичні наслідки (3 бали), значні наслідки (2 бали), незначні наслідки (1 бал), надто малий (0 балів). Більшість показників ґрунтуються на однобічній кількісній характеристиці, що аналізує вплив порушення роботи критичного об'єкта на жителів відповідної території. Отже, це дає підстави стверджувати що дана методика розроблена відповідно до концепції людиноцентризму як антропологічної парадигми сучасної євроінтеграційної політики України. Відповідно до ідеології людиноцентризму або «людиноорієнтованої» ідеології, держава має «служити» інтересам громадян, тобто діяти заради і в ім'я приватних осіб шляхом всебічного забезпечення пріоритету їх прав, свобод та інтересів у публічній сфері [116, с. 161].

Аналіз реалізації адміністративно-правової доктрини людиноцентризму, проведений О. В. Гладкою свідчить, що людина володіє специфічним «соціальним тілом», яке базується на економічних,

антропологічних, духовно-етичних, аксіологічних засадах, що свідчить про специфічну культуру людини і суспільства [26, с. 61]. Це підтверджується аналізом визначення рівня негативного впливу у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури (міжсекторальні критерії), що диференційовані на категорії за Соціальною, суспільною Економічною, комунікативною та безпековою значущістю:

I. Соціальна значущість об'єкта критичної інфраструктури (заподіяння шкоди навколишньому природному середовищу, заподіяння шкоди життю та здоров'ю людей);

II. Суспільна значущість об'єкта критичної інфраструктури (припинення або порушення функціонування державних органів, негативний вплив на довіру людей до державних інституцій, шкода інтересам інших держав – партнерів України);

III. Економічна значущість об'єкта критичної інфраструктури (заподіяння збитків об'єкту інфраструктури, заподіяння збитків державному та місцевим бюджетам);

IV. Комунікативна (негативний вплив на безперервне та стійке функціонування іншого об'єкта інфраструктури, що забезпечує надання таких самих або інших послуг);

V. Безпекова значущість об'єкта критичної інфраструктури (припинення або порушення функціонування пунктів управління або ситуаційного центру, що оцінюється в їх значущості, зниження показників державного оборонного замовлення).

В межах сучасної парадигми державної політики в сфері захисту критичної інфраструктури в умовах правового режиму воєнного стану важливим кроком стало упорядкування процесу формування переліку суб'єктів, відповідальних за формування й реалізацію державної політики та секторів критичної інфраструктури у відповідних секторах національної

системи захисту критичної інфраструктури. Даний процес координує Кабінет Міністрів України, переглядаючи та змінюючи його виходячи визначених з критеріїв критичності. Ст. 4. Закону України «Про критичну інфраструктуру» [60] до життєво важливих послуг та функцій, порушення яких сприятиме виникненню негативних наслідків для національної безпеки України, визначає 17 позицій: урядування та надання найважливіших публічних послуг, охорона здоров'я, енергозабезпечення, , продовольче забезпечення, фармацевтична промисловість, водопостачання та водовідведення, виготовлення вакцин, інформаційні послуги, стале функціонування біолабораторій, транспортне забезпечення, електронні комунікації, фінансові послуги, оборона, правопорядок, державна безпека, здійснення правосуддя, цивільний захист населення та територій, тримання під вартою, служби порятунку, космічні технології та послуги, космічна і дослідницька діяльність, хімічна промисловість. Відповідно до зазначеного переліку, Постановою № 1109 визначено перелік секторів (підсекторів), основних послуг критичної інфраструктури, заключним у цей список було внесено агропромисловий комплекс у якості детермінанти продовольчого забезпечення держави. Таким чином станом на 1 листопада 2023 р. в Україні налічується 25 секторів критичної інфраструктури (Додаток Б) [78].

Важливим кроком у межах модернізації державної політики захисту критичної інфраструктури в умовах правового режиму воєнного стану стала спроба формування у системі Міністерства оборони України кібервійськ, що передбачено Указом Президента України №446 від 26.08.2021 р. «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави» [268]. Магістральною ціллю даної ініціативи стала необхідність захисту суверенітету держави, відсічі збройній агресії у кіберпросторі, забезпечення її обороноздатності та запобігання збройному конфлікту. Логічним завершенням процесу створення кібервійськ має стати розробка

законопроєкту «Про створення та функціонування у системі Міністерства оборони України кібервійськ». Однак станом на листопад 2023 року це питання ще залишається відкритим.

Звернемо увагу, що парадигми державної політики у сфері захисту критичної інфраструктури розвинених країн об'єднує актуалізація предикату стійкості критичної інфраструктури. Стійкість об'єкта критичної інфраструктури дослідники тлумачать як здатність ним виконувати задані функції не лише у нормальних умовах, але й запобігати виникненню на об'єкті аварій чи катастроф за настання надзвичайного стану [1, с. 234]. Тобто питання забезпечення стійкості критичної інфраструктури, є особливо актуальною в умовах воєнного стану, оскільки посилюється інтенсивність впливу надзвичайних ситуацій, що піддають критичну інфраструктуру ризику дестабілізації. С. І. Кондратов, О. М. Суходоля підтверджують дане припущення, наголошуючи, що проблемам забезпечення стійкості приділяється усе більше уваги відносно захисту. Таку діаметральність учені пояснюють тим, що в умовах війни, жодна відома система захисту не гарантує повноцінний захист від усього спектру загроз і небезпек [95, с. 20]. Відповідно стійкість критичної інфраструктури передбачає її здатність до готовності та акомодації відносно динамічних умов, а також здатність протистояти змінам і швидко регенерувати потужності після надзвичайних ситуацій. Отже, можна дійти висновку, що концепція стійкості є більш практичною та дієвішою. У даному напрямку Державна служба спеціального зв'язку та захисту інформації України вивчає директиви ЄС NIS 2 (EU 2022/2555) та RCE (EU 2022/2557) щодо стійкості критичної інфраструктури і співпрацює з країнами, які вже розпочали їх впровадження.

У законодавчо визначеному переліку С. І. Крук пропонує конкретизовані інформаційні, інформаційно-інструментальні загрози та загрози психологічні дії з території інших країн, спрямовані на порушення нормального функціонування систем державного і воєнного управління. Вітчизняне законодавство про безпеку має чітко розмежовувати

повноваження державних органів, насамперед, органів сектору безпеки, забезпечувати міжвідомчу координацію, зокрема за умов тривалої агресії проти України [101, с. 77].

Фундаментальне значення в ідентифікації позиції та ролі парадигми державної політики в сфері захисту критичної інфраструктури в умовах правового режиму воєнного стану, закріплено Конституцією України, положення якої проектуються у Законі України від 21.06.2018 № 2469-VIII «Про національну безпеку України» [62]. Його зміст спрямований на посилення ролі органів державної влади у механізмі розвитку оборонно-промислового комплексу України, складовими якого є «державно-приватне партнерство» та «міжнародна консультативна, фінансова та матеріально-технічна допомога» [62]. Роль державної влади у сфері захисту критичної інфраструктури в умовах правового режиму воєнного стану актуалізує також п.2 ч.1 ст.1 Закону України «Про критичну інфраструктуру» [60] у якій ідентифіковано послуги та функції, здійснення яких гарантується органами місцевого самоврядування та державної влади, суб'єктами господарювання, установами та організаціями будь-якої форми власності, переривання, збої або порушення надання яких спричиняє швидкі негативні наслідки для національної безпеки як атрибутив «життєво важливі функції та послуги». Тобто дані положення Закону спрямовані на створення національної системи забезпечення безпеки та стійкості функціонування критичної інфраструктури та здійснення життєво важливих функцій [60].

Зазначений аспект парадигми державної політики у сфері захисту критичної інфраструктури в умовах правового режиму воєнного стану урегульовується низкою механізмів та інструментів, описаними у попередніх розділах зокрема веденням Реєстру об'єктів критичної інфраструктури, паспортизацією об'єктів, розробкою планів захисту та планів взаємодії та ін. Такі заходи переважно орієнтовані на забезпечення безпеки конкретних об'єктів, що є складовою глобального завдання у векторі забезпечення стійкості критичної інфраструктури в умовах воєнного стану. Тобто в умовах

воєнного стану активується потреба у досягненні стійкості шляхом забезпечення спроможності окремих операторів критичної інфраструктури. Секторальні органи влади розробляють та затверджують плани підтримання життєво важливих функцій та взаємодії у випадку дизфункції об'єктів критичної інфраструктури (п.4 ст.19), місцеві органи виконавчої влади забезпечують розроблення та затвердження програм підвищення стійкості територіальних громад, місцевих планів взаємодії у кризовій ситуації залучених суб'єктів, планів відновлення функціонування критичної інфраструктури (ст.20). Такі плани є своєрідною угодою між стейкхолдерами, котрі залучаються до процесу захисту критичної інфраструктури [60].

Аналізуючи в умовах воєнного стану особливості сучасної державної політики у сфері захисту критичної інфраструктури, корисним вважаємо дослідження Г. Ю. Зубка [80, с. 172], який, вивчав наукові аспекти реалізації державної інфраструктурної політики. Опираючись на доктринальні погляди вченого, відзначимо декілька основоположних припущень:

По-перше, в умовах правового режиму воєнного стану державна політики у сфері захисту критичної інфраструктури існує в концептуальному та діяльнісному аспектах і здійснюється Президентом, Урядом, інститутами, відповідальними за реалізацію політики захисту критичної інфраструктури.

По-друге, як процесу в умовах правового режиму воєнного стану державній політиці у сфері захисту критичної інфраструктури, притаманна етапність: від плану, курсу дій до практичної реалізації безпекових заходів.

По-третє, в умовах правового режиму воєнного стану державна політики у сфері захисту критичної інфраструктури концентрує в собі суспільно значущі інтереси і потреби.

По-четверте, в умовах правового режиму воєнного стану державна політики у сфері захисту критичної інфраструктури є багатосуб'єктною.

Сформованість законодавчої бази в Україні передбачає механізми управління державою як у звичайних умовах, так і в умовах надзвичайного та

воєнного стану. Це значною мірою гарантує безперервність урядування, що є одним із ключових напрямів забезпечення національної безпеки і стійкості. Крім того, ухвалений 2021 р. Закон України «Про основи національного спротиву» [66] заклав підвалини організації територіальної оборони, яка відіграла важливу роль у забезпеченні захисту держави у нинішній війні. Зокрема, у такий спосіб було реалізовано принцип субсидіарності, який є одним із ключових у сфері формування національної стійкості. Це дозволило суттєво підвищити ефективність реагування на воєнні загрози на місцевому рівні й налагодити належне координування на всіх рівнях [224].

Зокрема в роботах, присвячених аналізу різноманітних аспектів захисту критичної інфраструктури йдеться передусім про внутрішній аспект. На наш погляд, така позиція вельми дискусійна, оскільки Україна обрала курс на європейську та євроатлантичну інтеграцію, що передбачає розвиток в умовах глобалізації світової спільноти. Відповідно до цього, вектор державної політики захисту критичної інфраструктури має розвиватися й реалізовуватися в міжнародному і транснаціональному безпекових контекстах [86]. Тобто Уряд має встигнути вбудуватися в нову архітектуру світу, зберігаючи власні національні інтереси, контроль над власним інфраструктурним комплексом та національною ідентичністю, в тому числі й монополію та розвиток та провадження штучного інтелекту, водночас враховуючи глобалізаційні загрози, в тому числі і щодо ролі та впливу інфраструктури на формування парадигми національної безпеки. Погодимось із думкою В. А. Ліпкана, який стверджує, що «сучасна парадигма безпеки в Україні є наслідком деструктивних результатів агресії рф та аксіом її геополітики таких як агресія, анексія, тероризм, сепаратизм» [113, с. 271], що варто вважати основоположним системоутворюючими елементами адаптації державної політики захисту критичної інфраструктури. Слушною вважаємо пропозицію Г. Ю. Зубка, який пропонує політику України у цій сфері адаптувати за такими напрямами: зменшення інвестиційно-інноваційних ризиків; поліпшення

економічних, правових та організаційних умов діяльності іноземних інвесторів; активізацію механізмів концесії, угод про розподіл продукції, лізингу; використання потенціалу інститутів спільного інвестування [81, с. 220]. Аналіз алгоритмів відпрацьованих дій суб'єктами реагування на кризові ситуації внаслідок руйнування енергетичної інфраструктури України, можемо узагальнити методичний підхід до розробки концепції забезпечення стійкості системи критичної інфраструктури (рис. 2.1).

Враховуючи напрацювання у цьому напрямку О. М. Суходолі [255] та у відповідності до визначених Законом України «Про критичну інфраструктуру» [60] режимів функціонування критичної інфраструктури можемо узагальнити базові заходи реагування в межах квадрокомлексу режимів на об'єктовому рівні:

1. Штатний режим – передбачає розробку превентивного плану захисту, зокрема, розробку паспорта безпеки, відпрацюванні заходів зі попередження загроз, планування заходів зі зниження ризиків, планування заходів із мінімізації потенційної шкоди; застосування заходів з підвищення технічної стійкості, навчання персоналу.

2. Режим готовності та запобігання – передбачає розробку планів оперативної готовності. Основним документом є Акт оцінки стану захищеності об'єкта критичної інфраструктури, на основі якого здійснюється розробка планів захисту об'єкта та протидії проектним загрозам, оцінка стану аварійної готовності, тренування персоналу.

3. Режим реагування – заходи реагування на подію з метою повернення до первинних параметрів функціонування. Розробляються плани реагування, аварійної ситуації, взаємодії на випадок диверсії, протидії кіберзагрозам, безперервності ведення виконання функцій.

4. Режим відновлення – повернення до штатного режиму функціонування та урахування помилок попередніх режимів. Передбачає розробку планів відновлення, диверсифікації, резервування, посилення майбутньої стійкості, нових технологічних можливостей.

Рис. 2.1 Концепція забезпечення стійкості системи критичної інфраструктури

Джерело: розроблено автором на основі [113],[255]

Слушною вважаємо також пропозицію О. М. Суходолі [255, с. 3], який розподіляє заходи державної політики у сфері забезпечення стійкості системи критичної інфраструктури під час реагування на загрози порушення функціонування критичної інфраструктури на заходи «аварійного реагування» (першочергові дії реагування по припиненню деструктивного впливу загроз) та заходи «пом'якшення впливу загроз» на функціональність критичних об'єктів та рівень їх функціональності.

Важливим тригером у формуванні ефективної парадигми державної політики у сфері захисту критичної інфраструктури в умовах правового режиму воєнного стану стало ухвалення Урядом 19 вересня 2023 року розробленого Адміністрацією Держспецзв'язку «Національного плану захисту та забезпечення безпеки та стійкості критичної

інфраструктури» [228]. Інституція визначає стратегічні цілі, завдання та заходи для суб'єктів національної системи захисту критичної інфраструктури, серед яких: уточнення завдань та повноважень суб'єктів захисту критичної інфраструктури, удосконалення законодавства, що регламентує їхню діяльність; забезпечення проведення моніторингу; проведення оцінки ризиків і загроз критичній інфраструктурі; визначення порядку взаємодії суб'єктів захисту у кризових ситуаціях; забезпечення функціонування системи обміну інформацією; посилення стійкості; розроблення програм щодо роботи з громадами та підтримки населення на випадок кризових ситуацій; налагодження міжнародної співпраці.

Отже, адекватна модель загроз об'єкта критичної інфраструктури (рис.2.2) має включати портрет потенційного порушника, модель об'єкта та модель обстановки. Зважаючи на зазначене, модель загроз можна представити відповідно до підходу «all hazards approach» враховуючи загрози диверсифікованого походження: природного, техногенного, соціально-політичного, військового, кібернетичного, диверсійного, економічного, терористичного та колаборантного. Завдячуючи процесу моделювання формується модель загроз, що включає перелік можливих небезпек для критичного об'єкта, що впливають на його стале функціонування [95, с. 20]. Варто акцентувати увагу, що 15 березня 2022 року Кримінальний кодекс України було доповнено статтею 111-1 «Колабораційна діяльність» [99], де розтлумачено інтенцію «колабораціонізм», відповідно, колабораційну загрозу можемо трактувати, як небезпеки, що походять від громадян держави, які співпрацюють із ворогом з метою забезпечення реалізації його інтересів та заподіяння шкоди.

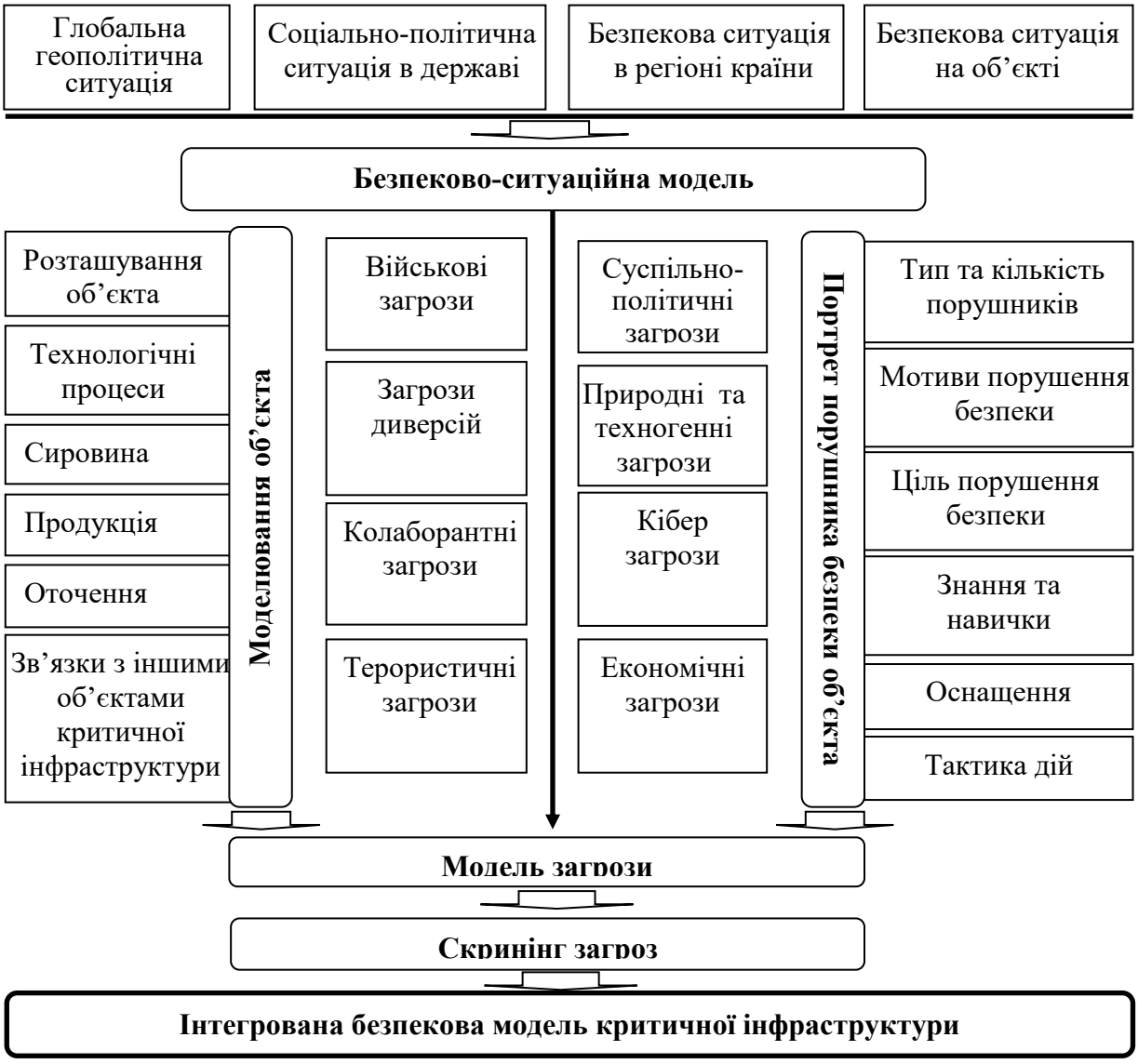


Рис. 2.2. Формат інтегрованої безпекової моделі критичної інфраструктури

Джерело:узагальнено на основі [14], [95], [99]

Теорії взаємовідносин між вищими органами державної влади в умовах надзвичайних ситуацій, де чітко розмежовується характер загрози. Якщо ця загроза зовнішня – за її подолання чи попередження відповідає глава держави, якщо внутрішня – уряд. Тому конституційні приписи мають бути розкриті в нормах спеціальних законів, де повинна бути чітко відображена послідовність дій всіх органів влади та посадових осіб.

Якщо в умовах воєнного стану Президент стає ключовою фігурою в прийнятті рішень, то в умовах надзвичайного стану чи надзвичайної екологічної ситуації повсякденне керівництво управлінням ресурсами та

подоланням таких подій бере на себе уряд, а Президент здійснює тільки функцію запуску заходів, передбачених у таких випадках, а саме, оголошення відповідного стану. Для уникнення протистоянь між Президентом та Прем'єром служить єдина площадка для прийняття рішень – Рада національної безпеки та оборони.

Структурно-логічна схема функціонування суб'єктів державної системи БСКІ (Додаток В) ілюструє процес організації системи управління та координації, а також відображає суб'єктів та основні завдання якими вони опікуються. Формалізаційним інструментом у функціонуванні державної системи БСКІ виступає Національний план захисту критичної інфраструктури, який зафіксує завдання, послідовність дій та механізм координації всіх залучених суб'єктів у різних режимах функціонування державної системи.

Органи державної влади та місцевого самоврядування в умовах надзвичайного і воєнного стану продовжують виконувати свої конституційні повноваження, опираючись на законодавство України. Зокрема, регламентовано механізми координації та міжвідомчої взаємодії на територіальних рівнях під час запровадження зазначених правових режимів. Реалізація заходів із впровадження дії надзвичайного стану покладається на органи виконавчої влади, органи місцевого самоврядування та відповідні військові командування. Також вони у співпраці з військовим командуванням організовують контроль за додержанням конституційних прав і свобод громадян, забезпеченням громадського порядку, громадської безпеки, захисту інтересів держави. Координація діяльності органів виконавчої влади та місцевого самоврядування, воєнного командування, підприємств, установ і організацій в умовах надзвичайного стану в частині, що не належить до повноважень РНБО України, покладається на КМУ. Для координації дії з питань підтримання правопорядку і забезпечення безпеки громадян на відповідній території на місцях можуть створюватися оперативні штаби, до складу яких можуть включатися представники СБУ, Національної поліції,

Військової служби правопорядку у ЗСУ, центральних органів виконавчої влади, що реалізують державну політику у сфері цивільного захисту, місцевого самоврядування на чолі з комендантами територій та місцевих органів виконавчої влади.

Важливим кроком у розвитку державної політики стало рішення Президента України, який 17.10. 2023 р. своїм Указом ввів у дію рішення РНБО «Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій» [271], яке орієнтовано на посилення захисту об'єктів критичної інфраструктури в умовах воєнного стану. Основні положення даного рішення передбачають посилення інженерного та фізичного протидронового захисту об'єктів критичної інфраструктури;. у разі виникнення надзвичайних ситуацій підвищити якість захисту та евакуації працівників об'єктів критичної інфраструктури; створення резеру обладнання та запасних частин для оперативного відновлення пошкоджених об'єктів; створення страхового фонду документації та критичних баз даних на захищених ресурсах; забезпечення об'єктів критичної інфраструктури резервними джерелами електроживлення; відпрацювання систем оповіщення населення про виникнення надзвичайної ситуації; затвердження Плану заходів з відновлення об'єктів критичної інфраструктури, що були зруйновані та/або пошкоджені внаслідок збройної агресії рф проти України; розробку та затвердження Плану енергетичної стійкості України; доповнення секторальних переліків об'єктів критичної інфраструктури, розташованими на тимчасово окупованій території України, та включити їх до Реєстру; утворення структурних підрозділів з питань захисту критичної інфраструктури; розробку та затвердження за категоріями об'єктів критичної інфраструктури; забезпечити запровадження системи взаємодії та інформаційного обміну між суб'єктами національної системи захисту критичної інфраструктури; вжити заходів із посилення бойової спроможності мобільних вогневих груп які здійснюють оборону об'єктів критичної

інфраструктури; підготовку методичних рекомендацій для органів місцевого самоврядування та місцевих органів виконавчої влади стосовно розробки та затвердження місцевих програм забезпечення стійкості та безпеки критичної інфраструктури; унеможливлення поширення інформації про об'єкти критичної інфраструктури; запровадження Міністерством оборони України навчальних програм та курсів підвищення кваліфікації з радіоелектронної боротьби та розвідки для військовослужбовців, залучених до забезпечення захисту і оборони об'єктів критичної інфраструктури [271].

Отже, варто відзначити, що сучасний етап реформування сектору безпеки і оборони України можна охарактеризувати як період активного формування мультиплікованої державної системи захисту критичної інфраструктури. Цьому сприяє наявність повноцінних систем захисту та кризового реагування. Практичної реалізації даного вектору державної політики можна досягнути за рахунок переходу до більш чіткого рівня координації дій та симбіозу, що передбачає узгодження основних параметрів функціонування зазначених систем реагування. До даної системи обов'язково має входити вектор превентивного та антикризового управління ризиками та загрозами за участю стейкхолдерів об'єктів критичної інфраструктури із розробкою спеціальних галузевих планів що застосовуватимуться у сфері їх захисту та не обмежуватиметься лише національним рівнем. Даний модуль сприятиме забезпеченню стійкості критичної інфраструктури та протидії стратегічним загрозам і ризикам на національному й міжнародному рівнях.

Висновки до розділу 2

1. Визначено, що інституційно праве регулювання є один із проявів правового впливу органів державної влади за допомогою інституційних засобів правової дійсності, які реалізують регуляторну силу права, а механізм інституційно-правового регулювання розглядаються як комплекс цих засобів, які пов'язані між собою та сприяють досягненню визначеної

мети правовим регулюванням. Екстрапольовано трактування інституційно-правового регулювання реалізації державної політики у сфері захисту критичної інфраструктури як систему організаційно-управлінських і правових заходів, що реалізовують інститути державної влади, за допомогою яких реалізується цілеспрямований (з метою максимізації безпеки об'єктів критичної інфраструктури) адміністративний вплив на суспільні відносини орієнтовані на запобігання диференційованим ризикам, загрозам і небезпекам об'єктам критичної інфраструктури основані на тріаді людина-суспільство-держава.

2. Проведений скринінг нормативно-правової бази у сфері захисту критичної політики, що формує магістральну основу інституційно-правового механізму державної політики. Узагальнено спектр основоположних інституцій, які структурують архітектуру безпекової парадигми об'єктів критичної інфраструктури. Досліджено спектр ключових інститутів державної влади у механізмі інституційно-правового регулювання провадження державної політики у сфері захисту критичної інфраструктури і їх основних функцій, серед яких визначено Президента України, Раду національної безпеки та оборони, Кабінет Міністрів України, Верховну Раду України, Уповноважений орган у сфері захисту критичної інфраструктури, Секторальні та функціональні органи в сфері захисту критичної інфраструктури, Державну службу захисту критичної інфраструктури та забезпечення національної системи стійкості, операторів критичної інфраструктури. У практичній реалізації архітектури національної безпеки ідентифіковано комплекс автономних державних систем захисту критичної інфраструктури.

3. Доведено, що реалізація державної політики у сферах захисту критичної інфраструктури інспірує еманацію інституційно-правових заходів реалізовуваних органами державної влади, серед яких відзначено привенційну значимість таких новелизацій, як внесення відомостей про об'єкт критичної інфраструктури до Реєстру об'єктів критичної

інфраструктури. Аналіз сучасних аспектів світового розвитку дав підстави констатувати масштабні зміни геополітичних інтересів у сфері перерозподілу територій та світових ресурсів, що у свою чергу, детермінує боротьбу за центри впливу на найбільш важливі об'єкти критичної інфраструктури, що призводить до безпрецедентних фактів порушення територіальної цілісності та інституціональної належності країн із слабкою системою державної політики захисту та обороноздатності.

4. Проаналізовано рівень інституційної спроможності національної системи захисту критичної інфраструктури у розрізі спроможностей структурних, організаційних, технічних систем та окремих індивідів, що включає розвиток навичок і компетенцій на всіх рівнях провадження державної політики у сфері захисту критичної інфраструктури крізь діоптрій процесних інституцій, що включає правила, процедури, засоби, інструменти, методи, організацію і ресурси. Виокремлено тріаду базових індикаторів інституційної спроможності системи національного захисту критичної інфраструктури: внутрішня синхронізація складових інституційної системи, зовнішня комплементарність складових інституційної системи, конгруентність внутрішніх та зовнішніх складових інституційної системи.

5. Головними суб'єктами інституційної спроможності забезпечення державної політики у сфері захисту критичної інфраструктури визначено органи публічної влади, котрі не проводять власних наукових досліджень, а знання, необхідні для реалізації даної діяльності, отримують лише в закладах вищої освіти та спеціалізованих установах підвищення кваліфікації, на основі чого формується їх рівень компетентності. Отже, однією із фундаментальних детермінант інституційної спроможності національної системи захисту критичної інфраструктури є спектр компетенцій, якими повинні володіти фахівці та оператори у даній галузі, а також наукова складова їх забезпечення, що обумовлюється наявністю

відповідних освітньо-професійних та освітньо-наукових програм у закладах вищої освіти держави.

6. Встановлено, що експліцитність інституційної спроможності національної системи захисту критичної інфраструктури імплікує комплементарність ряду паралельно функціонуючих систем: Єдиної державної системи запобігання, реагування й припинення терористичних актів та мінімізації їх наслідків, Національної системи кібербезпеки, Єдиної державної системи цивільного захисту, Державної системи фізичного захисту. На основі аналізу інституційної спроможності національної системи кібербезпеки, апробовано розрахунок Індексу національної спроможності кіберзахисту (НСК), який базується на квадро-комплексі вимірників спроможності державної політики у сфері кібербезпеки критичної інфраструктури, спроможності чинного законодавства, спроможності діючих підрозділів захисту, спроможності формату міжсекторальної співпраця та спроможних результатів.

7. Проведений аналіз показників спроможності національної системи захисту критичної інфраструктури в Україні дозволив виявити ряд проблемних питань, зокрема: освітні програми в країні не включають компетенції з кібербезпеки об’єктів критичної інфраструктури, а також відсутні спеціальності орієнтовані на захист об’єктів критичної інфраструктури вцілому, відсутність компетентного наглядового органу за результативністю державної політики у сфері захисту критичної інфраструктури, не розроблено План врегулювання кризових ситуацій на випадок масштабних кіберінцидентів та аварій на об’єктах критичної інфраструктури, не врегульовано законодавством порядок залучення волонтерів у сферу кібербезпеки та захисту критичної інфраструктури.

8. З’ясовано, що сучасна політика у сфері захисту критичної інфраструктури реалізується в умовах воєнного стану та безперервної російської військової агресії. Ворог систематично порушує міжнародні конвенції та інші інституції у сфері захисту життєво-важливих потреб

цивільного населення, які чітко забороняють атакувати, виводити з ладу чи знищувати об’єкти критичної інфраструктури. Встановлено, що Україна сьогодні зіштовхнулась із потребою переулаштування своєї державної політики відповідно до необхідності протидії численним інструментам гібридної війни з боку ворога, які він спрямовує на руйнацію суверенітету та територіальної цілісності країни. Обгрунтовано, що в умовах військової агресії, елементом стратегії ворога є сплановане руйнування об’єктів життєво-важливої інфраструктури, з метою маніпулювання морально-психологічним станом цивільного населення,

9. Аналіз сучасних аспектів державна політики у сфері захисту критичної інфраструктури в умовах правового режиму воєнного стану в Україні, надав підстави стверджувати, що сучасний захист об’єктів критичної інфраструктури забезпечується за рахунок комплексного аналітичного процесу, архітектура якого сформована на основі ідентифікації критичних секторів, створенні Реєстру об’єктів критичної інфраструктури, формуванні суб’єктного складу державної політики у сфері захисту критичної інфраструктури, визначенні актуальних загроз для критичних об’єктів, удосконалення інституційного забезпечення державної політики у цій сфері, формування системи захисту об’єктів критичної інфраструктури, вжиття відповідних заходів із подолання наслідків руйнувань. Акцентовано увагу, що політики у сфері захисту критичної інфраструктури розвинених країн об’єднує актуалізація предикату стійкості відносно питань захисту. Це пояснюється тим, що в умовах війни, жодна із наявних систем захисту не гарантує безумовний захист від усіх загроз і небезпек. Стійкість об’єкта критичної інфраструктури трактовано як його здатність виконувати задані функції не лише в нормальних умовах, але й здатність запобігати виникненню аварій та катастроф на об’єкті в умовах настання надзвичайного стану, тобто передбачає здатність до акомодації відносно динамічних умов, а також швидко регенерувати потужності після деструктивних явищ.

10. Узагальнено методичний підхід до розробки концептуальних засад

захисту критичної інфраструктури на основі забезпечення стійкості у штатному режимі, режимі готовності та запобігання, режимі реагування та режимі відновлення. На основі цього, структуровано формат інтегрованої безпекової моделі критичної інфраструктури, що передбачає створення безпеково-ситуаційної моделі у якості фідбеку до моделі проєктної загрози. Остання створюється відповідно до спроєктованого портрету порушника безпеки об’єкта та особливостей самого об’єкта із урахуванням потенційного переліку проєктних загроз.

РОЗДІЛ 3.
УДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

3.1. Міжнародний досвід реалізації державної політики у сфері захисту критичної інфраструктури.

Сучасна воєнно-політична ситуація у світі породжує додаткові бінарні ризики у сфері найважливіших безпекових пріоритетів держави. У такому випадку управління системними ризиками вимагає посилення симбіозу державних та міжнародних інститутів у сфері політики захисту критично важливих об'єктів. Це у свою чергу мотивує вектор державної політики країн до пошуку нових засобів та методів спостереження, ідентифікації та нейтралізації потенційних загроз, або мінімізації їх наслідків. У даному випадку слушною вважаємо думку С. С. Теленика, щодо критичної інфраструктури як об'єкту адміністративно-правового регулювання [258, с. 185]. За переконанням ученого, модель діяльності у даному напрямку «має ґрунтуватися на нормативній базі, програмно-стратегічних документах, напрацьованому досвіді та найкращих прикладах правового регулювання аналогічних інститутів у зарубіжних країнах» [258, с. 185]. Тут стає корисним аналіз та вивчення передових підходів країн світу до конструювання і реалізації державної політики у сфері захисту критичної інфраструктури. Зокрема, особливу увагу пропонуємо звернути на досвід державних превентивних механізмів управління ризиками та загрозами. Особливу увагу слід звернути на практику провідних країн світу, що вирізняється корельованістю у системах захисту, розширенням ситуаційної обізнаності та оперативного контролю стейкхолдерів, а також інституційною структурованістю мультипліканд безпекових механізмів.

Аналізуючи зарубіжний досвід, перш за все слід відзначити, що кожна держава, яка реалізує автентичну парадигму захисту критичної інфраструктури чітко визначає певний сегмент, реєстр відповідних об'єктів,

складові системи та необхідні ресурси. Кількість таких критичних секторів різниться в кожній країні, залежно від можливостей (ресурсів), додаткових інститутів захисту (наприклад приватних компаній), що можуть бути залученні до реалізації державної політики у сфері захисту критичної інфраструктури. Кожен сектор критичної інфраструктури може бути закріплений за одним (іноді кількома) державними органами та установами (агентствами), на які покладено завдання, в тому числі щодо підготовки кадрів і населення до забезпечення безпеки стратегічної від специфічних для цього сектора загроз і ризиків, відповідно до їх пробільності [141, с. 145].

Аналізуючи досвід США у цьому напрямку, варто відзначити, що на національному рівні ключову роль із реалізації державної політики у сфері безпеки критичної інфраструктури покладено на Офіс захисту інфраструктури (Office of Infrastructure Protection). Таку інституцію було утворено з метою забезпечення загального управління і координації національних зусиль захисту критичних об'єктів, фокусуючи увагу на управлінні ризиками та забезпеченні стійкості критичної інфраструктури, співпрацюючи з усіма стейкхолдерами даного процесу [83, с. 215].

Звернемо також увагу, що у США у якості уповноваженого органу у сфері захисту критичної інфраструктури діє Агентство з кібербезпеки та стійкості критичної інфраструктури (CISA) [155]. У його структурі функціонує Міжвідомчий комітет безпеки, який комунікує з державними партнерами, компаніями та громадами на всіх рівнях, з метою забезпечення навчання та інші ресурси та інструменти, пов'язані з безпекою критичної інфраструктури. Особливістю даного інституту є те, що його зусилля сфокусовано на посиленні обізнаності максимально широкої спільноти стейкхолдерів про необхідність підтримки безпеки та стійкості критичної інфраструктури та активізації їхніх спільних дій. CISA виконує життєво важливу роль у інформаційному обміні з партнерами як з державного, так і приватного секторів, що має ключове значення для гарантування безпеки та стійкості нації. Державний та приватний сектори налагодили партнерські

відносини в структурі галузевої координаційної ради, щоб спільно нести відповідальність за мінімізацію ризиків та збоїв у роботі критичної інфраструктури. Експерти CISA з предметних питань також організовують навчання присвячене безпеці критичної інфраструктури за допомогою диверсифікованих засобів, включаючи віртуальне навчання під керівництвом інструктора, незалежні навчальні курси та аудиторні заняття [155]. Тобто, агенція CISA відповідальна і за кіберзахист, і за захист критичної інфраструктури. Можемо зробити висновок, що Україна, запозичила досвід американської моделі, опираючись на досвід ЄС. Українська система захисту критичної інфраструктури відповідає новій Директиві ЄС 2557 щодо стійкості. Унікальність української системи кібербезпеки та захисту критичної інфраструктури варто відзначити у її адаптивності та еластичності, що дозволило під час повномасштабного вторгнення рф в Україну продемонструвати можливості до оперативного вдосконалення відповідно до новітніх загроз та кооперуватися для посилення національної безпеки.

Важливу роль у системі захисту критичної інфраструктури США виконує стратегічний документ – Національний план захисту інфраструктури 2013 (NIPP 2013) [329], розроблений Департаментом внутрішньої безпеки США. Він визначає підходи до захисту критичної інфраструктури країни від актів тероризму та інших небезпек. Цей план включає в себе координацію дій між федеральними, місцевими та приватними суб'єктами, а також визначає пріоритети та стратегії для ефективного захисту інфраструктури. Основний тезис, який прослідковується у NIPP 2013 проголошує, що «національне благополуччя залежить від безпечної та стійкої критичної інфраструктури» [329]. Метою NIPP 2013 є розвиток державно-приварного партнерства для забезпечення безпеки та стійкості критичної інфраструктури. Для досягнення цієї мети партнери з критичної інфраструктури повинні колективно визначити національні пріоритети, формулювати чіткі цілі, зменшити ризик, виміряти прогрес, і адаптуватися на основі зворотного зв'язку та мінливого середовища. До ключових положень

NIPP 2013 варто віднести:

1. Визначення та класифікація секторів критичної інфраструктури.

2. Оцінка та управління ризиками критичної інфраструктури з метою пом’якшення потенційних загроз.

3. Розвиток державно-приватного партнерства та координації між різними державними установами, організаціями приватного сектору, державними та місцевими органами влади для захисту критичної інфраструктури.

4. Обмін інформацією та кібербезпека, що сприяє комунікаціям у сфері апроксимації найкращих практик для посилення кібербезпеки та загального захисту критичної інфраструктури.

5. Опис стратегій реагування на інциденти та швидкого відновлення після збоїв у критичній інфраструктурі.

6. Визнає ключову роль і знання власників і операторів критичної інфраструктури.

7. Об’єднує зусилля всіх рівнів уряду, приватного та некомерційного секторів, забезпечуючи інклюзивне партнерство, рамки та визнання унікального досвіду та здібностей, які кожен стейкхолдер докладає до національних зусиль захисту критичної інфраструктури [329].

На сучасному етапі доктрина національної безпеки США розвивається зі зміщенням фокусу уваги Уряду у напрямку обґрунтування інституційних конструкцій із фіксацією у федеральному законодавстві, президентських указах та директивах особливого статусу для об’єктів критичної інфраструктури у сфері національної безпеки. Перелік критично значимих секторів, закріплено Національною стратегією внутрішньої безпеки [332] серед яких закріплено: телекомунікації, енергетику, банківсько-фінансовий сектор, транспортну інфраструктуру, водопостачання, служби екстреної допомоги та забезпечення роботи органів влади, охорону здоров’я, хімічну індустрію, поштову службу та перевезення, оборонно-промисловий комплекс, агросектор та харчову промисловість [164]. Зазначений документ

також обґрунтовує фундаментальні вектори колективних дій федеральної та місцевої влади у умовах посилення комунікації із приватним сектором у процесі оперативного та стратегічного державного управління в сфері захисту об'єктів критичної інфраструктури.

Відзначимо ще один не менш важливий документ – Президентську політичну директиву «Безпека та стійкість критичної інфраструктури» [338]. Ця директива регламентує архітектуру процесу координації зусиль між урядовими установами, організаціями приватного сектору та іншими стейкхолдерами для визначення та фіксації пріоритетів захисту критичної інфраструктури, оцінки вразливостей і розробки планів та програм для зменшення ризиків і підвищення її стійкості. Він підкреслює важливість інформаційного фідбеку, державно-приватного партнерства та стратегій управління ризиками для захисту критичної інфраструктури від фізичних і кіберзагроз. У документі прослідковується тріада стратегічних імператив, яким керуються федеральні органи влади та оператори критичної інфраструктури у своїй діяльності:

1) синхронізація функціональних зв'язків Федерального уряду для сприяння національній єдності при докладанні зусиль для посилення безпеки та стійкості критичної інфраструктури;

2) забезпечення ефективного обміну інформацією шляхом визначення базових даних і системних вимог;

3) впровадження функції інтеграції та аналізу для інформування щодо планування та операційних рішень стосовно критичної інфраструктури [315].

Варто згадати ще одну важливу інституцію, яка доповнює попередні – «Національну стратегію фізичного захисту критичної інфраструктури та найважливіших об'єктів» США [333]. У ній закріплено підходи до державного регулювання захисту критичних об'єктів на основі принципу «спільної відповідальності» всіх уповноважених суб'єктів як на міжурядовому рівні (федерація – штати – місцеві органи влади та

управління), так і всередині міжвідомчого-секторального сегменту, включаючи зв'язку «регулятор – приватні бізнес-структури», у власності або управлінні яких знаходяться об'єкти критичної інфраструктури. В межах даного інституційного конструкту визначено основні групи загроз:

– прямої інфраструктурної дії, що мають наростаючий (cascading) ефект та ведуть до руйнування об'єктів критичної інфраструктури внаслідок прямої атаки чи іншого впливу на ключові системи;

– непрямої інфраструктурної дії, здатна викликати збій, дезорганізацію роботи, в тому числі і за допомогою створення негативних соціальних ефектів;

– загрози використання конкретних об'єктів або їх елементів як засіб для ураження інших цілей.

Актуальним до вивчення в Україні вважаємо регламентований зазначеним нормативним актом спектр повноважень федерального уряду США сфері забезпечення захисту об'єктів критичної інфраструктури. До них включено регулювання, координацію взаємодії та забезпечення інституційної підтримки, що ґрунтується на секторальній сформатованій схемі, де за кожен критично важливий сектор відповідає окремий орган виконавчої влади, іменований як «провідне агентство» (lead agency). Також Національною стратегію фізичного захисту критичної інфраструктури та найважливіших об'єктів США визначені всі параметри підходів до регулювання об'єктів критичної інфраструктури: ідентифікація цих об'єктів по кожному сектору, їх категоризація, визначення можливих видів загроз сектору, стандартизація вимог захисту, уніфікація зведених геопросторових даних, організація механізмів обміну інформацією, включаючи дані під грифом секретності, визначення інструментів захисту персоналу, пов'язаного з роботою на об'єктах критичної інфраструктури та деякі інші. Інституцією також було визначено відповідні напрямки фундаментальних наукових досліджень та технічного пошуку, орієнтовані на пошук нових рішень у сфері створення ефективних моделей регулювання та захисту критичної

інфраструктури [314].

Парадигма внутрішньої та національної безпеки США також встановлює нові параметри обмеження допуску іноземних інвесторів у сферу критичної інфраструктури [163, с. 134]. Дані обмеження ставлять важливі завдання перед законодавчими органами, які беруть участь у підготовці законодавчої бази щодо модернізації процесу аналізу ризиків, пов'язаних з іноземним інвестуванням у сфери дотичні до критично значимих об'єктів [307]. Важливо зазначити, що Розвідувальне співтовариство США разом із Міністерством оборони негайно запропонували низку інституційних рішень, спрямованих на посилення правил щодо регулювання іноземних інвестицій в об'єкти критичної інфраструктури, а також на введення ряду радикальніших положень про контроль іноземних інвесторів у економіці США в цілому. Основі положення зазначених пропозицій вимагають, щоб іноземні інвестиції проходили процедуру ретельного оцінювання крізь призму відповідності інтересам забезпечення національної безпеки у їхньому традиційному розумінні. Уповноваженими органами влади, відповідальними за ці рішення проводиться розслідування по можливостях, цілях та намірах країни-інвестора встановити контроль над об'єктом інвестування. При цьому було визначено, що країни, які викликають особливе занепокоєння (country of special concern) або підозру, але оголосили про наміри придбання критичних технологій або критичної інфраструктури США, не повинні отримати погодження на даний правочин. Конгрес вказав також на те, що обов'язково проводиться розслідування потенційних наслідків такої угоди для національної безпеки США, якщо вона призводить до встановлення кумулятивного контролю (cumulative control) через нещодавні угоди іноземного уряду або іноземної особи, що вже відбулися, щодо будь-якого певного виду критичної інфраструктури, енергетичних активів, критичних матеріалів чи критичних технологій. Очевидно, що ключові положення даних пропозицій передбачають стратегічний комплекс превентивних заходів для унеможливлення внутрішньої дестабілізації стійкості критичної

інфраструктури, що свідчить про активну безпекову політику.

Звернемо також увагу, що у своїй діяльності Офіс захисту інфраструктури США робить значний акцент на підготовку персоналу та його навчання із питань захисту об'єктів критичної інфраструктури за профілем їх діяльності (хімічна промисловість, енергетика, комерційний сектор, гідротехнічні споруди та ін.). З цією метою відповідними експертами проводяться семінари щодо захисту критичної інфраструктури, де персонал інформують про сучасні тенденції, проблеми, загрози відносно критичної інфраструктури, а також знайомлять із передовим досвідом та засобами укріплення стійкості об'єктів. Таким чином відбувається формування секторальних систем підготовки персоналу та населення до підвищення безпеки критичної інфраструктури та формування у них відповідних компетентностей.

Відзначимо, що суттєвим інституційним проривом у сфері захисту критичної інфраструктури стало прийняття 15 листопада 2021 року Закону про інвестиції в інфраструктуру та робочі місця [316], який долучив до даного процесу також Управління науково-технічної політики (OSTP). Основна місія даного інституту передбачає співпрацю з федеральними департаментами, агентствами та Конгресом для створення спільної візії та єдиних стратегій, чітких планів, зваженої державної політики та ефективних рішень на основі наукового обґрунтування. OSTP також посилює взаємодію із зовнішніми партнерами, включаючи промисловість, благодійні організації та громадянське суспільство, державні, місцеві та територіальні органи влади. Діяльність OSTP орієнтована також на покращення розуміння впливу надзвичайних подій на критичну інфраструктуру та стимулювання дослідницької діяльності для надання практичної, керованої даними, конкретної та дієвої інформації, концепцій, методів, технологій, а також інструменти для власників і операторів критичної інфраструктури щодо потенційного пом'якшення впливу та відновлення після подій [178]. Зазначеним вище законом регламентовано спільні дії OSTP та Міністерства

внутрішньої безпеки (Department of Homeland Security – DHS) у напрямку проведення досліджень, розробки, тестування та оцінки критичної інфраструктури на її стійкість. На підтримку Закону OSTP розробила стратегічну структуру та план витрат на підтримку безпеки та стійкості критичної інфраструктури, а також створила Програму дослідження безпеки та стійкості критичної інфраструктури (CISRR) для керування широким спектром пов'язаних заходів, що проводяться OSTP для вирішення проблем критичної інфраструктури. Окрім цього Законом «Про інвестиції в інфраструктуру та робочі місця» передбачено до 2026 року фінансування у розмірі 550 млрд дол. США на нові інфраструктурні ініціативи, серед яких: ремонт і реконструкція доріг і мостів (110 млрд дол.), модернізація та обслуговування пасажирських і вантажних залізничних систем (66 млрд дол.), оновлення ліній електропередач, запобігання виходу з ладу елементів електромереж та забезпечення збільшення частки відновних джерел енергії (65 млрд дол.), розширення широкосмугового зв'язку в сільській місцевості та малозабезпечених громадах (65 млрд дол.), забезпечення населення чистою питною водою, включаючи заміну свинцевих труб і боротьбу із забрудненням вод свинцем та іншими хімікатами (55 млрд дол.), захист інфраструктури від фізичних атак, кібертероризму та погодних катаклізмів (55 млрд дол.), оновлення громадського транспорту, створення нових автобусних маршрутів і підвищення доступності для людей похилого віку та інвалідів (39 млрд дол.), модернізація та розширення американських аеропортів, диспетчерських веж і систем контролю (25 млрд дол.), прибирання територій Суперфонду та забудованих територій, покинутих шахт і старих нафтових і газових свердловин (21 млрд дол.), портову інфраструктуру та викиди вантажівок у портах (17 млрд дол.), забезпечення безпечних зон на дорогах, пішоходах, трубопроводах та інших (11 млрд дол.), інфраструктуру водопостачання Заходу країни, включаючи розвиток зрошення та протидії посухам (8 млрд дол.), розвиток загальнонаціональної мережі зарядних станцій для електромобілів (7,5 млрд дол.), електричні

шкільні автобуси, переважно для малозабезпечених, сільських та племінних громад (5 млрд дол.) [303]. Отже, зазначений інвестиційний пакет покликаний модернізувати застарілі елементи критичної інфраструктури та посилити її стійкість.

Аналізуючи практику реагування на інцидент або надзвичайну ситуацію на об'єктах китичної інфраструктури США відбувається чітка координації між DHS та власниками й операторами критичної інфраструктури. Даним процесом опікується Національний координаційний центр інфраструктури (National Infrastructure Coordinating Center – NICC), що є національним центром для підтримки безпеки та стійкості активів фізичної критичної інфраструктури. NICC активно співпрацює з федеральними департаментами та агенціями, а також стейкхолдерами з числа приватного сектору для моніторингу потенціалу, розвитку та поточних регіональних і національних операцій у секторах критичної інфраструктури країни [142].

Президентська політична Директива 21 (Presidential Policy Directive 21) [338] підкреслює роль національних фізичних і кіберкоординаційних центрів у забезпеченні успішних результатів безпеки та стійкості критичної інфраструктури. Національний центр інтеграції кібербезпеки та комунікацій (National Cybersecurity and. Communications Integration Center – NCCIC) визначається провідною організацією з кібербезпеки та комунікацій у структурі DHS. Він виконує функції національного центру критичної кіберінфраструктури, координує та синхронізує процес реагування, пом'якшення та відновлення у разі значних кібер-інцидентів шляхом регулярної координації з правоохоронними органами, розвідувальним співтовариством, міжнародними комп'ютерними групами готовності до надзвичайних ситуацій, внутрішніми центрами обміну та аналізу інформації і стейкхолдерами критичної інфраструктури, для обміну інформацією та спільного реагування на інциденти [142]. По суті, NCCIC захищає та аналізує дані для інформування про заходи щодо запобігання,

захисту, пом’якшення, реагування та відновлення кіберінфраструктури.

Центри NICC та NCCIC, разом із інтегрованою функцією аналізу, формують механізми обміну інформацією (ситуаційну обізнаність) у секторах критичної інфраструктури на основі комунікації, надаючи інформацію з більшою глибиною, широтою та контекстом. Власники та оператори критичної інфраструктури отримують інформацію безпосередньо з центрів, але також часто отримують інформацію через свої відповідні Секторальні агентства (Sector-Specific Agencies – SSA) або інші сторони, такі як регіональні кластери, центри обміну та аналізу інформації (Information sharing and analysis centers – ISAC), центри синтезу та ін.

Варто також відзначити, що у США в сфері захисту критичної інфраструктури важливу роль відіграють також інтернет ресурси, зокрема створено Інформаційну мережу внутрішньої безпеки – критична інфраструктура (Homeland Security Information Network – Critical Infrastructure – HSIN-CI). HSIN-CI забезпечує безпечний мережевий обмін інформацією, що охоплює весь спектр інтересів стейкхолдерів критичної інфраструктури, котрі можуть отримати вільний доступ до Інформаційної мережі внутрішньої безпеки. HSIN-CI також може сприяти численним видам обміну інформацією та координації, включаючи повідомлення про підозрілу діяльність, вебінари, спільні конференції та ін. Наповненням HSIN-CI опікується NICC, котрий публікує дані по критичній інфраструктурі, що включають звіти про інциденти, дані про загрози, моделювання впливу, оцінки загальної вразливості об’єктів, потенційні захисні та превентивні заходи, забезпечуючи при цьому зручність доступу до необхідної інформації. Окремі, більш масштабні сектори та під сектори, самостійно керують власними інформаційними порталами в рамках HSIN-CI. [149].

Щоб забезпечити широкий обмін важливою інформацією, NICC також отримує та надає інформацію через інші портали. Наприклад, створено Портал команди комп’ютерної готовності до надзвичайних ситуацій

Сполучених Штатів (United States Computer Emergency Readiness Team – US-CERT) і Команди реагування на надзвичайні ситуації промислових систем керування (ICS-CERT). NCCIC надає безпечну веб-платформу для спільної роботи системи з обміну конфіденційною інформацією щодо забезпечення кібербезпеки, фізичного захисту, депферності, превентивного реагування та регенерації із залученням приватного сектору, уряду і міжнародних партнерів. Він надає партнерам доступ до двох компонентів захищеного порталу, які містять інформацію про кіберіндикатори, інциденти та перелік відомого зловмисного програмного забезпечення, що може використовуватись проти систем критичної інфраструктури:

– Cobalt Compartment – інформаційний центр безпеки корпоративних систем.

– Відділ систем керування (The Control System Compartment) – містить матеріали про промислові системи керування, обмежені власниками та операторами активів систем керування [156].

Секторальні та міжгалузеві структури включають:

– Галузеві координаційні ради (Sector Coordinating Councils – SCCs) – самоорганізовані, самокеровані та самоврядні ради стейкхолдерів, що складаються з власників, операторів та їхніх представників, які взаємодіють у широкому діапазоні галузевих стратегій, політики, діяльності та безпекових питань. SCCs служать основними точками співпраці між урядом і власниками (операторами) об’єктів критичної інфраструктури та приватного сектору для координації та планування політики безпеки та стійкості критичної інфраструктури.

– Міжгалузева рада критичної інфраструктури – рада стейкхолдерів, що складається з голів і заступників голів SCCs, координує міжсекторальні питання, ініціативи та взаємозалежності для підтримки безпеки та стійкості критичної інфраструктури.

– Урядові координаційні ради (GCC) – складаються з представників різних рівнів влади (включно з федеральним), відповідно до робочого

ландшафту кожного окремого сектору, ці ради забезпечують міжвідомчу, міжурядову та міжюрисдикційну координацію всередині та між секторах і співпрацювати з SCCs на основі державно-приватного партнерства.

– Федеральна рада вищого керівництва (FSLC) – складається з вищих посадових осіб з SSA та інших федеральних департаментів та агентств, які відіграють роль у забезпеченні безпеки та стійкості критичної інфраструктури, FSLC сприяє комунікації та координації у сфері безпеки та стійкості критичної інфраструктури на федеральному рівні.

– Координаційна рада державного, місцевого та територіального уряду (SLTTGCC) – складається з представників серед державних установ. SLTTGCC сприяє залученню партнерів з безпеки та стійкості до національної критичної інфраструктури та забезпечує організаційну структуру для координації між державними та місцевими рівнями юрисдикції в розробці та реалізації урядових стратегій та програм.

– Координаційна рада регіонального кластеру (RC3) – включає регіональні групи та коаліції по всій країні у різноманітних ініціативах з підвищення безпеки та стійкості критичної інфраструктури в державному та приватному секторах [149].

Аналізуючи лаконічний огляд основних інституційно-правових аспектів розвитку державної політики у сфері захисту критичної інфраструктури США, можемо узагальнити кращі практики, актуальні до вивчення та інтерпретації в Україні, зокрема, варто узагальнити основні кроки для формування концепції безпеки та стійкості критичної інфраструктури:

1. Встановити основні цілі та завдання концепції;

2. Проаналізувати існуючий закордонний досвід та визначити приклади відповідних планів або програм безпеки та стійкості критичної інфраструктури, елементи яких можуть бути трансплантовані у інституційно-правову структуру державної політики України;

3. Закріпити перспективи адаптації визначених практик за конкретними секторами критичної інфраструктури;

4. Ідентифікувати перелік стейкхолдерів об’єктів критичної інфраструктури у відповідних секторах;

5. Закріпити інституційні ролі та обов’язки визначених стейкхолдерів;

6. Встановити механізми координації та комунікації між державними інститутами, операторами (власниками) об’єктів критичної інфраструктури та їх стейкхолдерами;

7. Створити систему ризик-менеджменту, розробити алгоритми спільних дій, встановити перелік індикаторів та провести на їх основі оцінювання дієвості таких заходів;

8. Розробити плани проведення спільних міжсекторальних навчань та тренувань;

9. Встановити чіткі часові регламенти зазначених дій та забезпечити їх дотримання;

10. Пропагувати необхідність розширення кола стейкхолдерів та дотримання зазначених концептуальних положень.

Ці кроки гарантують, що в разі реального інциденту кожен знатиме свою роль і що робити.

Розглянемо також досвід ЄС у напрямку реалізації державної політики захисту критичної інфраструктури. Щоб зменшити вразливість даних об’єктів, Європейська комісія запустила Європейську програму захисту критичної інфраструктури (European Programme for Critical Infrastructure Protection – EPCIP). Це пакет заходів, спрямований на покращення захисту критичної інфраструктури усіх держав ЄС у відповідних секторах діяльності. Однією із наймасштабніших є ініціатива ЄС щодо захисту критичної інформаційної інфраструктури (Critical Information Infrastructure Protection – CIP), котра спрямована на посилення безпеки та стійкості життєво важливих інфраструктур інформаційно-комунікаційного спрямування [293].

Одним із заходів, передбачених для сприяння реалізації EPCIP стало створення Комісії мережевого інформаційного попередження критичної інфраструктури (Commission of a Critical Infrastructure Warning Information

Network – CIWIN), що спрямована на надання допомоги державам-членам і Європейській комісії в обміні інформацією про спільні загрози, вразливості та відповідні заходи та стратегії для зменшення ризику на підтримку CIP. Мережа CIWIN була розроблена як захищена загальнодоступна інформаційно-комунікаційна система, що належить Комісії, яка пропонує визнаним членам спільноти CIP ЄС можливість обмінюватися та обговорювати інформацію, дослідження та передову практику в усіх державах-членах ЄС і обговорювати пов'язану з CIP інформацію. Портал CIWIN почав роботу у січні 2013 року.

Із проведеного аналізу закордонного досвіду помітно, що спільним знаменником державної політики у даному напрямку є вектор орієнтований на забезпечення стійкості критичної інфраструктури. У загальному розумінні R. Cantelmi пропонує даний феномен розглядати, виходячи із хронологічної послідовності дій «до, під час і після» надзвичайної події, яка дестабілізує роботу критичної інфраструктури [289]. Таким чином, можна припустити, що даний конструкт включає у себе цикл антикризового управління. Отже, у розрізі «стійкість критичної інфраструктури» характеризується стадійністю. T. W. Coombs пропонує розглядати три стадії даного процесу: докризову, кризову і посткризову. Докризовий період включає в себе підготовку до можливої кризи шляхом аналізу ризиків, розробки планів дій та впровадження профілактичних заходів. Кризовий період включає в себе реагування на кризову ситуацію, управління кризовими подіями та мінімізацію збитків. Посткризовий період включає в себе оцінку наслідків кризи, відновлення діяльності критичної інфраструктури та впровадження заходів для запобігання подібним ситуаціям у майбутньому [294. с. 198].

Отже, приділяючи увагу таким питанням, як надійність і здатність витримувати або протистояти дестабілізуючим факторам. Варто також припустити факт, що порушення в роботі критичних об'єктів час від часу неминуче відбуватимуться, що потребує посилення їх абсорбційних та адаптаційних можливостей.

Аналізуючи змістовне наповнення теоретизування «стійкість», звернемось до словника Управління ООН зі зменшення ризику стихійних лих (UNDRR) у якому дана дефініція ідентифікується як «здатність системи, громади або суспільства, що піддаються впливу небезпеки, протистояти, поглинати, адаптуватися та відновлюватися від наслідків небезпеки своєчасно та ефективно, в тому числі шляхом збереження та відновлення своїх основних базових структур та функцій» [351]. Стійкість системи критичної інфраструктури іноземні учені трактують як здатність протидіяти, адаптуватися та швидко відновлюватися після потенційно деструктивної події [342. с. 25].

Актуалізація феномену стійкості критичної інфраструктури знаходить пояснення у проєкті Critical Entities Resilience Directive 2022 року (Директива CER) [301] це питання у зазначеному документі належним чином відзначене: «необхідно докорінно змінити нинішній підхід із захисту конкретних активів на посилення стійкості критично важливих об'єктів». У цьому контексті «стійкість» означає здатність запобігати, протистояти, пом'якшувати, абсорбувати, пристосовуватися та відновлюватися після інциденту, який порушує або може порушити роботу критично важливого об'єкта. Насправді це досить добре відповідає основному визначенню в літературі з питань стійкості критичної інфраструктури. Зміну вектору безпекової парадигми ЄС можна пояснити зростанням кількості держав-членів, які усе більше усвідомлюють важливість ідеї стійкості, в якій захист не є основою стабільності роботи критичної інфраструктури, а однією зі складових поряд із запобіганням і пом'якшенням ризиків та відновленням. Виходячи з цього, Європейська Комісія у своїй пропозиції дійшла висновку, що необхідно забезпечити «більш комплексний підхід до забезпечення стійкості критично важливих об'єктів у низці секторів у всьому Європейському Союзі» [297].

Погоджуємось із думкою О.Суходолі [254, с. 2], який стверджує що основна ціль політики ЄС щодо забезпечення стійкості критичної інфраструктури полягає у підвищенні спроможності держав-членів

гарантувати безперебійність надання основних життєво важливих послуг підтримки суспільних функцій, громадського здоров'я, економічної діяльності та безпеки навколишнього середовища на внутрішньому ринку ЄС. Директива CER відводить особливе місце розбудові спроможності ЄС та держав-членів бути підготовленими до виникнення кризових ситуацій.

Варто відмітити, що Директива CER стала основоположною інституцією на шляху стратегічного зміцнення безпеки критичної інфраструктури ЄС крізь призму її стійкості. Із цією метою документ передбачає імплементацію державами-членами ЄС наступних заходів:

– ухвалення стратегій підвищення стійкості критичних об'єктів;

– розробку на національному рівні у визначених Директивою CER секторах вимоги до проведення ризик-аналізу стійкості на об'єктах критичної інфраструктури;

– зобов'язання операторів критичних об'єктів до розробки та ратифікації планів стійкості технічних, безпекових та організаційних заходів відповідно до визначеного рівня загроз;

– організація груп стійкості операторів критичної інфраструктури у якості консультативно-координаційного механізму діяльності Єврокомісії;

– створення дорадчого інституту з метою допомогти операторам критичних об'єктів оцінити дієвість вжитих заходів забезпечення стійкості;

– призначення уповноважених координаційних органів для забезпечення взаємодії між державами-членами ЄС, Єврокомісією, інститутами та операторами критичних об'єктів ЄС з метою оцінювання стану імплементації положень Директиви CER;

– підготовка методичних та інструктивних матеріалів для проведення колективних навчань, консультування, запровадження програм підвищення кваліфікації персоналу операторів критичної інфраструктури [254, с. 3], [301].

У профілі реалізації державної політики в напрямку ініціалізації

стійкості критичної інфраструктури варто узагальнити тріаду її тригерів:

1. Соціальна стійкість – сфокусована на оцінюванні впливу дестабілізації об'єктів на життєво важливі суспільні функції для населення громади. Соціальний вимір стійкості складається із заходів, спеціально розроблених для зменшення ступеня негативних наслідків для постраждалих від дизфункції критичної інфраструктури громад. Подібним чином, економічний вимір соціальної стійкості відноситься до здатності зменшувати як прямі, так і непрямі економічні втрати в результаті кризових ситуацій [122, с. 55].

2. Організаційна стійкість – визначається у ефективності антикризового управління та організаційному рівні превентивних заходів, проявляється у готовності до кризової ситуації та ранньому її попередженні, а також спроможності до оперативного реагування та ефективність комунікації. Організаційний вимір стійкості стосується спроможності організацій, які керують критично важливими об'єктами та несуть відповідальність за виконання критично важливих функцій, пов'язаних із кризовими ситуаціями, приймати рішення та вживати заходів, які сприяють досягненню властивостей стійкості, описаних вище, тобто допомагають досягти більшої надійності, резервування, винахідливості та швидкості [23, с. 3].

3. Технологічна стійкість – стосується самого об'єкта критичної інфраструктури, його адаптивності, надійності, еластичності та здатності до відновлення. Вимір технологічної стійкості стосується здатності фізичних систем (включно з їх компонентами, взаємозв'язками та взаємодіями) працювати на прийнятному (бажаному рівні) під час кризової ситуації [290, с. 720].

Зазначені складові формують «трикутник стійкості», що є базовим індикатором для оцінки. Максимізація стійкості обернено пропорційна зменшенню площі трикутника в усіх його вимірах, що дозволяє довше витримувати стрес, швидше адаптуватися і оперативніше відновлюватися. Зазначені сфери стійкості, очевидно, взаємопов'язані у поєднанні з іншими

супутніми сферами, наприклад, екологічною або психологічною.

Успішним вважаємо досвід Німеччини, де безпека об'єктів критичної інфраструктури є колективним завданням стейкхолдерів, уряду, операторів та громадянського суспільства. Серед основоположних принципів державної політики захисту критичної інфраструктури можемо відзначити паритетну співпрацю держави з промисловістю і бізнесом та дієвість і пропорційність вжитих заходів для підвищення рівня стійкості [331].

Зазначимо, що одні з перших політичних дій щодо захисту критичної інфраструктури були здійснені саме в Німеччині. У 1997 році з ініціативи Федерального міністерства внутрішніх справ (BMI) створено міжвідомчу робочу групу як інституційну одиницю захисту критичної інфраструктури – «UP KRITIS». Це державно-приватна співпраця між операторами критичної інфраструктури їх асоціаціями а також відповідними державними органами. Дана група об'єднує дев'ять із десяти секторів критичної інфраструктури (за виключенням сектору державного управління) та охоплює федеральний, державний і місцевий рівні [177]. Організація служить для підготовки до інцидентів безпеки та перебоїв і запобігання їм на критичних об'єктах шляхом обміну інформацією та думками щодо фундаментальних основ стійкості критичної інфраструктури. Серед основних учасників варто відзначити Федеральне міністерство внутрішніх справ і громадськості, Федеральне відомство з інформаційної безпеки, Федерального відомства цивільного захисту та ліквідації наслідків катастроф, представників Сектору утилізації побутових відходів, Сектору харчування, Сектору фінансів та страхування, Водного сектору, Сектору транспорту, Сектору інформаційних технологій і телекомунікацій, Сектору охорони здоров'я, Енергетичного сектору а також представники бізнесу, які утворюють Економічну консультативну раду [177].

Ключовими інституціями у сфері захисту критичної інфраструктури Німеччини є:

1. Закон про підвищення безпеки систем інформаційних технологій

(Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme). Федеральний уряд робить внесок у те, щоб IT-системи та цифрові інфраструктури Німеччини стали одними з найбезпечніших, зокрема, у сфері критичної інфраструктури. Закон вимагає, щоб оператори критичних інфраструктур забезпечували належний захист їхніх інформаційних систем від кіберзагроз [358].

2. Закон про Федеральне відомство з інформаційної безпеки (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik – BSI). Закон регулює сферу інформаційної безпеки в Німеччині через Федеральне відомство BSI, що відповідає за захист інформаційних систем державних і некомерційних організацій від кібератак, зломів та інших загроз. BSI займається розробкою стандартів безпеки, проведенням досліджень та аналізу загроз, наданням консультацій та підтримки організацій у сфері інформаційної безпеки [305].

3. Національна стратегія захисту критичної інфраструктури (Nationale Strategie zum Schutz Kritischer Infrastrukturen – NSKR). NSKR стратегія була розроблена з метою забезпечення безпеки та стійкості важливих секторів, таких як енергетика, транспорт, телекомунікації, фінанси та інші, від різних загроз, включаючи кібератаки. Визначає основні принципи та завдання захисту критичних інфраструктур, включаючи електроенергетику, транспорт, телекомунікації та інші сектори. Вона також передбачає регулярну інвентаризацію та класифікацію критичних об’єктів, а також розробку заходів для їх захисту. Вона також встановлює роль та відповідальність різних органів і організацій, які займаються захистом критичних інфраструктур [334].

Важливим у державній політиці Німеччини є урахування міжгалузевого підходу, який стає необхідним там, де внаслідок просторової близькості різних інфраструктурних об’єктів зосередження уваги на окремих галузевих правилах безпеки є недостатньо або може перешкодити виробленню ефективного управлінського рішення. Однією з інституцій міжгалузевого реагування на небезпеки, тісно пов’язані із захистом критичної

інфраструктури, є Стратегія кібербезпеки [299] У ній основна увага приділяється загрозам, що походять від кіберпростору у різних секторах. Також варто відзначити «Стратегію Німеччини щодо адаптації до зміни клімату» [309] у якій велику роль відведено цілому ряду різних явищ зі спектру природних небезпек та заходів відповідної протидії. «Стратегія безпеки вантажних перевезень та логістики» [347] є прикладом галузевого стратегічного документа, який безпосередньо відноситься до захисту критичної інфраструктури та стратегії KRITIS. Вона визначає значимість захисту критично важливих інфраструктур для вантажних перевезень та логістики.

Відповідно до Польської практики, основну роль у розбудові системи захисту критичної інфраструктури відіграє Урядовий центр безпеки (Rządowe Centrum Bezpieczeństwa – RCB) [153]. Урядовий центр безпеки регулює процес запобігання кризовим ситуаціям, а в разі їх виникнення координує заходи з мінімізації їх наслідків. Центр оцінює ризик загроз національній безпеці, уніфікуючи сприйняття загроз окремими міністерствами. Тим самим він підвищує спроможність відповідних служб та органів державного управління справлятися зі складними ситуаціями у секторах критичної інфраструктури. У штат RCB входять цивільні експерти, офіцери та солдати Війська Польського. Основними завданнями RCB є:

– підтримка Урядової Групи Кризового Регулювання (Rządowego Zespołu Zarządzania Kryzysowego – RZZK), яка є міжміністерською консультативною групою, що формує думку та відповідає за ініціювання і координацію кризового управління;

– моніторинг та проведення аналізу загроз на основі даних, отриманих від усіх кризових центрів, що діють у державному управлінні;

– цілодобове чергування, що забезпечує обіг інформації в Національному центрі управління кризами, який у разі загрози запускає процедуру врегулювання, а також приймає та поширює сигнали, що передаються НАТО, ЄС та ООН;

– застереження від загроз та публікація інформації в соціальних мережах (Twitter, Facebook, Instagram) та у ЗМІ;

– нагляд за захистом національної та європейської критичної інфраструктури;

– створення планів, звітів, аналізів та рекомендацій щодо загроз національній безпеці та прогнозів кризових ситуацій;

– створення Національного плану врегулювання кризових ситуацій (Krajowego Planu Zarządzania Kryzysowego), що визначає напрямки цивільного планування на центральному та провінційному рівнях;

– створення звіту про загрози національній безпеці – національна стратегія оцінки ризиків та зменшення ризиків стихійних лих;

– постійне чергування з підвищення обороноздатності держави.

Урядовий центр безпеки готує Національну програму захисту критичної інфраструктури (Narodowy Program Ochrony Infrastruktury Krytycznej – NPOIK) та співпрацює з операторами й адміністрацією критичних об'єктів. На основі детальних критеріїв, що є конфіденційним додатком до NPOIK, директор RCB у співпраці з відповідними міністрами, відповідальними за системи критичної інфраструктури, спільно готують єдиний перелік об'єктів, установок, пристроїв і послуг, включених до критичної інфраструктури, розділяючи їх на системи [328].

Важливим інститутом у системі державної політики захисту критичної інфраструктури Польщі є згадувана вище Урядова Група Кризового Регулювання – RZZK [154], створення якої передбачено ст. 8. Ustawa «O zarządzaniu kryzysowym» [354]. RZZK є польською державною організацією, відповідальною за управління кризовими ситуаціями та надання допомоги населенню під час надзвичайних подій. Його завдання включає розробку та впровадження планів дій для запобігання, реагування та ліквідації кризових ситуацій. Інститут координує дії різних державних служб і організацій у разі виникнення кризової ситуації, такої як природні катастрофи, техногенні

аварії, терористичні акти тощо. Вони також займаються попередженням та освітою населення щодо поведінки під час кризових ситуацій. Отже, серед основних функцій даної організації варто визначити:

– відповідальність за координацію зусиль різних урядових та неурядових організацій у випадках кризових ситуацій;

– планування та підготовку до кризових ситуацій, сприяння розробці планів, процедур та стратегій для відповіді на кризові ситуації;

– взаємодія з іншими органами та міжнародними партнерами, шляхом налагодження співпраці державних та місцевих органів із міжнародними організаціями для обміну інформацією та ресурсами у випадках криз;

– забезпечення збору, аналізу та поширення інформації про поточні кризові ситуації та важливі рекомендації громадськості.

Важливо звернути увагу на перспективний для України досвід Польщі у ролі, яку відіграють у системі захисту критичної інфраструктури та кризового управління воєводи. Відповідно до чинних правових актів, завданням воєвод та їх організаційних підрозділів, відповідальних за врегулювання кризових ситуацій на об’єктах критичної інфраструктури у воєводському управлінні визначено:

– організацію виконання завдань у сфері захисту критичної інфраструктури, що пов’язано із розташуванням на території воєводства критичних об’єктів, у тому числі включення цих завдань до воєводських планів стратегічного управління;

– збір та обробку інформації щодо критичної інфраструктури, розташованої на території воєводств;

– надання необхідної інформації про критичну інфраструктуру у воєводстві компетентному органу публічного управління, який діє у цій сфері, якщо є потреба, що випливає з плану управління кризою;

– узгодження планів операторів по захисту критичної інфраструктури.

Воєводський рівень є перехідною точкою між системним та

територіальним підходом до завдань у сфері захисту критичної інфраструктури, а підпорядковані воєводам служби, охорона та інспекції є важливим елементом планування на випадок порушення функціонування критичних об'єктів, розташованих на території воєводства. У зв'язку із зазначеним, воєводи, прагнучи досягти цілей Програми NPOIK [328], зокрема:

– організовують та керують регіональним форумом захисту критичної інфраструктури та беруть участь у механізмі її захисту в межах, визначених у Програмі;

– беруть участь у процесі оцінки ризиків кризової ситуації в країні, спричиненої ураженням або дисфункцію об'єктів критичної інфраструктури, розташованих на території воєводства, шляхом підготовки та оновлення Часткового звіту про загрози національній безпеці (Częściowy raport o zagrożeniach bezpieczeństwa narodowego), який вони готують для потреб Національного плану врегулювання кризових ситуацій (Krajowego Planu Zarządzania Kryzysowego) [320];

– співпрацюють з воєводськими, повітовими та міськими урядами у виконанні завдань у сфері врегулювання криз та цивільного планування, що випливають із компетенції воєводського самоврядування;

– співпрацюють з операторами критичної інфраструктури та суб'єктами, компетентними у питаннях захисту та підтримки їх діяльності, спрямованої на досягнення цілей NPOIK [328].

Комплекс безпекових заходів в межах державної політики охарактеризованих країн корелює із загальноєвропейською інституцією – European Programme for Critical Infrastructure Protection (EPCIP). Даний документ є ініціативою Європейського Союзу, націленою на забезпечення протекції критичної інфраструктури в Європі. EPCIP була започаткована ще у 2006 році, маючи на меті максимізацію рівня безпеки та стійкості критичних інфраструктур. Основні принципи зазначеної Програми включають оцінку ризиків, розуміння загроз, застосування заходів безпеки,

міжсекторальну співпрацю та рефлексію між країнами у напрямку модернізації заходів реагування на інциденти та регенерацію роботи після них на об'єктах критичної інфраструктури [293].

Магістральною віссю державної політики у сфері захисту критичної інфраструктури у ЄС є Директива від 8 грудня 2008 року Council directive 2008/114/EC «On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection» (Щодо ідентифікації та позначення європейських критичних інфраструктур та оцінки необхідності покращення їх захисту). Вона встановлює процедуру ідентифікації та маркування європейських об'єктів критичних інфраструктур (ECI) і загальний підхід до оцінки потреб у покращенні їх захисту. Документ передбачає створення Комісії щодо покращення захисту ECI. Директива також зобов'язує власників (операторів) ECI готувати плани безпеки і призначати офіцерів зв'язку з безпекою, що зв'язують власника/оператора з національним органом, відповідальним за захист критичної інфраструктури. Інституція також визначає пріоритетність участі приватного сектору в нагляді та управлінні ризиками, плануванні безпекових заходів та відновленні після надзвичайної ситуації [301].

У системі захисту критичної інфраструктури ЄС існує поняття «Critical Infrastructure Protection Point» (CIP Point), що передбачає точку зв'язку, визначену для обміну інформацією та координації з питань захисту критичної інфраструктури. У тому числі відбувається інформаційний реверс стосовно загроз, ризиків та інцидентів, а також координація спільних дій для запобігання та реагування на події, які можуть загрожувати критичній інфраструктурі. Ці CIP точки використовуються для налаштування партнерства між країнами-членами ЄС, Європейською Комісією та іншими стейкхолдерами у сфері захисту критичної інфраструктури. Органи та структури CIP Points може визначати кожна країна-член ЄС, враховуючи свої особливості та потреби [140, с. 153].

Спільні дії державної політики стійкості, що були описані вище,

передбачають наявність стратегічних вказівок, які описують основну філософію дій та досвід вирішення усіх важливих питань щодо безпеки критичної інфраструктури з посиланням на всі відомі ризики. На цій основі можна спроєктувати відповідні підцілі, які, у свою чергу, будуть конкретизовані в концепціях, планах, програмах та віддзеркалюватимуться в них. Зусилля держави у цій сфері мають бути орієнтовані на забезпечення та посилення рівня захищеності критичної інфраструктури за допомогою відповідних заходів, архітектуру яких пропонуємо узагальнити у відповідному квадро-комплексі (рис 3.1).

Рис.3.1. Квадро-комплекс забезпечення стійкості критичної інфраструктури

Джерело:[242, с. 106]

Аналізуючи досвід країн ЄС у забезпеченні досягнення балансу описаного «трикутника стійкості» варто узагальнити ключові позиції, на яких варто акцентувати увагу у напрямку проекції даного досвіду у площину державної політики України у сфері забезпечення стійкості критичної інфраструктури:

– аналіз та оцінка ризиків і загроз – процес визначення та оцінювання потенційних загроз та ризиків, які можуть вплинути на важливі системи та об’єкти, необхідні для функціонування суспільства та економіки. Цей процес

допомагає забезпечити стійкість та надійність критичної інфраструктури в умовах загроз;

– превентивність – на основі заздалегідь виявлених існуючих ризиків та загроз здійснення профілактичних дій, що дозволить уникнути серйозних збоїв у роботі критично-важливих інфраструктурних об'єктів;

– імплементація – втілення комплексу рішень ефективного управління в кризових і надзвичайних ситуаціях, що дозволить мінімізувати їх наслідки;

– апроксимація досвіду – посилення захисту критичної інфраструктури на базі стратифікації отриманого досвіду та систематичного аналізу ризиків і загроз інцидентів, що уже мали місце в країні або за її межами. На основі набутого досвіду спільно з відповідними операторами та міжнародними партнерами формуються стандарти захисту [242, с. 107].

Послідовна реалізація зазначеного квадро-комплексу у вигляді циклу управління ризиками та загрозам гарантуватиме необхідну захисній системі пролонговану ефективність, яка підвищить компетенцію відповідних інститутів у галузі безпеки об'єктів критичної інфраструктури (рис. 3.2).

Таким чином, можемо визначити кілька елементів стійкості критичної інфраструктури, а саме: передбачення потенційних порушень (для оцінки, планування та підготовки), здатність поглинати (витримувати удари/тиск або пристосовуватися до несподіванок), здатність адаптуватися (продовжувати функціонувати або надавати послуги в новій ситуації) і здатність швидко відновлюватися після значних порушень або ситуацій.

З іншого боку, стійкість критичної інфраструктури визначається трьома ключовими характеристиками:

– надійністю (здатність підтримувати діяльність та функції в умовах НС, наприклад, стійкий дизайн, заміна системи та інші фактори);

– винахідливістю (вміла підготовка до реагування на НС, наприклад, безперервність бізнесу, навчання, управління ланцюгами поставок та інші фактори);

– швидким відновленням (поверненням або відновленням нормальної роботи в найкоротші терміни після НС, наприклад, екстрені операції, негайні дії з відновлення та інші фактори) [242, с. 109].

Рис. 3.2. Модель забезпечення стійкості критичної інфраструктури

Джерело: узагальнено автором на основі [185],[343]

На основі проведеного дослідження закордонного досвіду інституційно-правових особливостей реалізації державної політики в сфері захисту критичної інфраструктури у контексті розбудови її стійкості та опираючись на результати досліджень, можна підсумувати наступні особливості:

– у більшості країн ЄС спостерігається низький рівень концептуальної та термінологічної ідентифікації та визначення критичної інфраструктури в основних політичних і нормативних документах;

– окрім держав, які ратифікували закони про критичну інфраструктуру, інші не мають офіційної національної ідентифікації об’єктів як основи для розробки політики та заходів з розбудови стійкості та інклюзивності;

– у більшості країн ЄС аспекти систем критичної інфраструктури включені в існуючі нормативні та планові документи;

– національні органи управління з питань надзвичайних ситуацій роблять вирішальний внесок у захист критичної інфраструктури разом з іншими суб'єктами на національному та місцевому рівнях, займаючи ключову позицію у врегулюванні мультиризикових, мульти-загрозливих чи міжсекторальних ситуацій дизфункції критичної інфраструктури;

– об'єкти критичної інфраструктури отримали особливу увагу у зв'язку зі змінами національної інвестиційної політики деяких країн, яка у свою чергу відіграє велику роль у різних національних стратегіях захисту;

– більшість країн мають плани щодо захисту критичної інфраструктури, мають систему ідентифікації таких об'єктів, визначають потенційну шкоду та наслідки від дестабілізації критичної інфраструктури, ідентифікують джерела ризиків;

– у більшості країн приймають державні стратегії управління ризиками до захисту критичної інфраструктури, які включають базові заходи: запобігання, підготовленість, відповідь та відновлення;

– політика у сфері захисту критичної інфраструктури більшості країн орієнтована на розвиток потенціалу інвестиційної активності у сферу захисту критичної інфраструктури, забезпечуючи паритетну роль державних і приватних операторів критичної інфраструктури та бізнес-структур (як внутрішніх так і іноземних), з метою посилення стійкості критичної інфраструктури, охопивши максимальний спектр національних інтересів;

– значна роль відведена ідентифікації стейкхолдерів захисту об'єктів критичної інфраструктури у сфері приватного бізнесу та розвиток відносин на основі державно-приватного партнерства та кластеризації;

– приділяється увага розвитку освіти у напрямку підготовки спеціалістів у сфері захисту критичної інфраструктури;

– активізується інформаційний реверс між стейкхолдерами безпеки та стійкості об'єктів критичної інфраструктури, у напрямку акумуляції дієвого досвіду протидії загрозам та ризикам, створення та підтримки зручних

систем комунікації, захисту інформаційної конфіденційності власників та операторів, кіберзахисту;

– розробка програм безпеки та стійкості критичної інфраструктури стартує із постановки цілей і завдань на національному, регіональному, місцевому, галузевому чи організаційному рівні, повинна віддзеркалювати існуюче робоче середовище, культурні цінності, переконання та опиратися на існуючі відносини, зусилля та політику [311].

На основі результатів оціночного огляду закордонного досвіду у сфері державної політики, варто узагальнити концептуальні положення вектору посилення стійкості критичної інфраструктури на загальнодержавному і регіональному рівнях:

– удосконалення політичної та інституційно-правової бази, яка дозволить всебічно розбудовувати діяльність з підвищення стійкості, включаючи інтеграцію в існуючі або прийняття нових транснаціональних програм та стратегій;

– розвиток кадрового потенціалу, що передбачає формування відповідних компетентностей у ключових стейкхолдерів, представників державної влади, відповідальних за формування політики та прийняття рішень у сфері захисту критичної інфраструктури, операторів, експертів, професіоналів та громадян;

– перегляд секторів критичної інфраструктури на основі аналізу досвіду, досліджень і розробок відповідно до національних контекстів і пріоритетів передових країнах світу;

– інтегрована оцінка ризиків та загроз, моделювання, оперативне планування та розробка сценаріїв превентивних та поточних дій у разі надзвичайних ситуацій на об’єктах критичної інфраструктури;

– забезпечення міжсекторальної координації та співпраці, а також створення партнерств зі стейкхолдерами, національними, місцевими органами влади і власниками та операторами критичних об’єктів на основі

державно-приватного партнерства;

– посилення ресурсного забезпечення стійкості критичної інфраструктури.

3.2. Інституційні перетворення у напрямку підвищення ефективності державної політики захисту критичної інфраструктури.

Як зазначалося раніше, у питаннях захисту об'єктів критичної інфраструктури розвинутих держав прослідковується актуалізація 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» [318, с. 291]. 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 регенерувати порушену функціональну спроможність. При цьому, питанням забезпечення стійкості опікується усе більше науковців у порівнянні з проблемами захисту [242, с. 105]. Дану тезу підтверджують і закордонні дослідники, наголошуючи, що колективне опікування національною стратегією оборони та безпеки є обов'язковою умовою стійкості нації.

Основоположним напрямком інституційних перетворень вчені пропонують окрім відповідних міністерств, залучати до реалізації стратегії стійкості критичної інфраструктури інших учасників, без яких неможливо уявити врегулювання кризових ситуацій [1, с. 112], [95, с. 25]. 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.

Зазначимо, що кожний державний інститут або відомство, забезпечуючи розробку та впровадження політики безпеки критичної інфраструктури, має чітко розуміти спектр потенційних ризиків та загроз для підпорядкованих йому інфраструктурних об'єктів, оперуючи відповідним набором ресурсів та інструментів. Солідарні із судженням учених Д. С. Бірюкова та С. І. Кондратова [9, с. 109], що інститутам державної безпекової політики варто взяти до уваги діаметральні світоглядні наукові доробки, які повинні передувати практичній частині інституційних перетворень в межах реалізації державної політики захисту та забезпечення стійкості критичної інфраструктури. Серед таких перетворень науковці пропонують виділити:

– секторальна біфуркація об'єктів критичної інфраструктури на місцевому, регіональному та національному рівнях;

– комплексний підхід до ідентифікації релевантних секторальних загроз та ризиків для об'єктів критичної інфраструктури;

– аналіз ступеня вразливості різних секторів критичної інфраструктури до окремих загроз та ризиків;

– оцінка загроз та ризиків дестабілізації або повного руйнування окремих секторів критичної інфраструктури;

– розробка відповідних превентивних заходів на основі функціонування системи захисту критичної інфраструктури.

Загалом, можна стверджувати, що в основі даних підходів лежить виконання мероприємств стратегічного планування державними інститутами, з метою уникнення нових і зниження впливу відомих ризиків та загроз об'єктам критичної інфраструктури. Кінцевим продуктом даного процесу

мають стати управлінські рішення на загальнодержавному, регіональному та місцевому рівнях, орієнтовані на реалізацію комплексу заходів із ідентифікації потенційних ризиків, удосконалення інституційно-правових параметрів управління загрозами і ризиками, інвестування в заходи підвищення ефективності оперативного реагування на загрози та відновлення після надзвичайних ситуацій [282, с. 78].

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 [329]. 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, що у країнах ЄС на зміну парадигмі захисту

приходить парадигма резильєнтності, що явно простежується у спеціальних публікаціях NIST [335], публікаціях MITRE [325] і в розробленні стандартів ISO [317]. На загальному рівні це також знаходить своє відображення в останніх директивах Ради ЄС, що визначають нові пріоритети в забезпеченні безпеки об'єктів критичної інфраструктури. С. І. Пирожков, Н. В. Хамітов, аналізуючи семантичний зміст терміну «резильєнтність» ототожнюють його із життєстійкістю та здатністю відновлюватися [186, с. 48]. Відповідно у напрямку забезпечення захисту критичної інфраструктури з позиції сучасної міжнародної практики, вважаємо доцільним вживати саме термін «резильєнтність критичної інфраструктури». Науковці трактують даний предикат як здатність суб'єкта міжнародних відносин протидіяти гібридним загрозам.

Отже, 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 [330]. Мотиви даної ініціативи можемо відзначити:

– у потребі систематизації та ідентифікації ризиків, за допомогою якого можна заповнити сліпі зони у захисті критичної інфраструктури;

– у необхідності комплексної готовності до різних типів ризиків відповідно до загального набору критеріїв;

– у необхідності досягнення консенсусу між секторальними органами захисту критичної інфраструктури та інвесторами щодо пріоритетів інвестування у заходах з управління ризиками;

– у необхідності краще зрозуміти зв'язки між різними типами ризиків, з метою розробки міжсекторальних планів протидії ризикам та ліквідації наслідків.

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) [176] Подібний підхід використовується й у США. Він ґрунтується на аналізі вразливостей, загроз та наслідків. При цьому ризики критичній інфраструктурі оцінюються на основі експертних оцінок за 5-бальною шкалою, а інколи за 3-бальною – від мінімального до катастрофічного рівня [305, с. 260].

Диференціювання діяльності об'єктів критичної інфраструктури та їх приналежності до різних галузей ілюструє багатоаспектність проблем аналізу ризиків в управлінні безпекою. Особливість критичного ризик-аналізу визначимо також у тому, що аналізуються потенційно шкодочинні наслідки,

що можуть виникнути в наслідок збоїв, дестабілізації технологічних систем, або помилок персоналу об'єкту. Враховуючи це, варто приділити окрему увагу складовій «управління критичними ризиками», як головній складовій державної політики забезпечення безпеки та резильєнтності критичної інфраструктури. Зауважимо, що дану тезу слід розглянути також під кутом зору адміністрування, як сфери компетенції органів державної влади. У даному випадку звернемось до фундаментального дослідження даного поняття ученими О. Я. Лазор та О. Д. Лазор [109, с. 116], які відстоюють позицію, що процес адміністрування включає консультативно-дорадчу та організаційно-розпорядчу діяльність органів державної влади. Отже, адміністрування з позиції державного управління варто характеризувати з точки зору підпорядкованості законам, узгодженості інтересів учасників процесу та відповідальності за стан керованих систем. Розширимо межі уявлення про дану категорію теорією В. В. Овчарука [138, с. 116] який визначає її як управлінську діяльність, функцію менеджменту, вид менеджменту або стиль управління. Отже, дійдемо висновку, що процес управління критичними ризиками слід проводити із позиції синхронізації публічного адміністрування та менеджменту. Доречним у даному випадку вважаємо розширення структури державної політики у сфері захисту та резильєнтності критичної інфраструктури предикатом «критичний ризик-менеджмент». Це дозволить посилити складову захисту як державних критичних об'єктів, так і приватних. Слушним у даному розумінні вважаємо позицію вчених В. О. Мусієнка та М. Е. Зінченка, які тлумачать поняття ризик-менеджмент як «процес прийняття та виконання управлінських рішень, спрямованих на зменшення ступеня ймовірності виникнення результату несприятливого характеру та мінімізацію можливих втрат, які викликані його реалізацією» [118, с. 103]. Доцільно трактувати систему критичного ризик-менеджменту в межах забезпечення резильєнтності критичної інфраструктури як частину системного підходу до прийняття управлінських рішень [88, с. 55]. Отже, вважаємо доцільним сприймати

критичний ризик-менеджмент як спектр процедур і практичних заходів, націлених на вирішенні завдань з профілактики і зниження рівня потенційних ризиків та загроз виникнення критичних ситуацій, що загрожують стійкості функціонування об'єктів критичної інфраструктури, зниження потенційних втрат та інших негативних наслідків. По суті, мова йде про застосування превентивних заходів для унеможливлення виникнення надзвичайних ситуацій на життєво-важливих об'єктах та планові заходи щодо мінімізації та ліквідації негативних наслідків за умов їх виникнення. Оскільки, як зазначалося вище, управління ризиками у структурі державно політики захисту критичної інфраструктури відбувається в умовах неясності, в основі варто розглядати методи прогнозування і соціальний та технічний аналіз під час оцінки ризику (рис 3.3.). Відповідно до схеми, зазначимо, що захист критичної інфраструктури має базуватися на механізмах державного управління та оцінці критичних ризиків. Аналіз ризику та вразливості є основними методами та важливими інструментами для проведення проактивного та ефективного управління безпекою [327, с. 455].

Середовище державного управління для створення дієвого захисту критичної інфраструктури повинно містити модуль ризик-менеджменту, який базується на відпрацюванні альтернатив з використанням результатів оцінки ризиків, аналізу ризиків та прогнозування наслідків для їх мінімізації. Тобто, даний процес передбачає реалізацію багатокритеріальних задач, які передують прийняттю рішення в умовах невизначеності. Оцінка ризику є базовим у дослідженнях і розробці заходів ризик-менеджменту згідно з алгоритмом дій із детекції небезпек, оцінки загроз та вразливості критичного об'єкта. В свою чергу це вимагає створення додаткового алгоритму, що дозволить змоделювати обставини надзвичайної ситуації і в подальшому допоможе керівництву і працівникам критичних об'єктів адаптуватись до них у реальності. Отже, інтеграція ризик-менеджменту в архітектуру державної політики забезпечить реалізацію механізму управління загрозами та їх ідентифікації на об'єктах критичної інфраструктури.

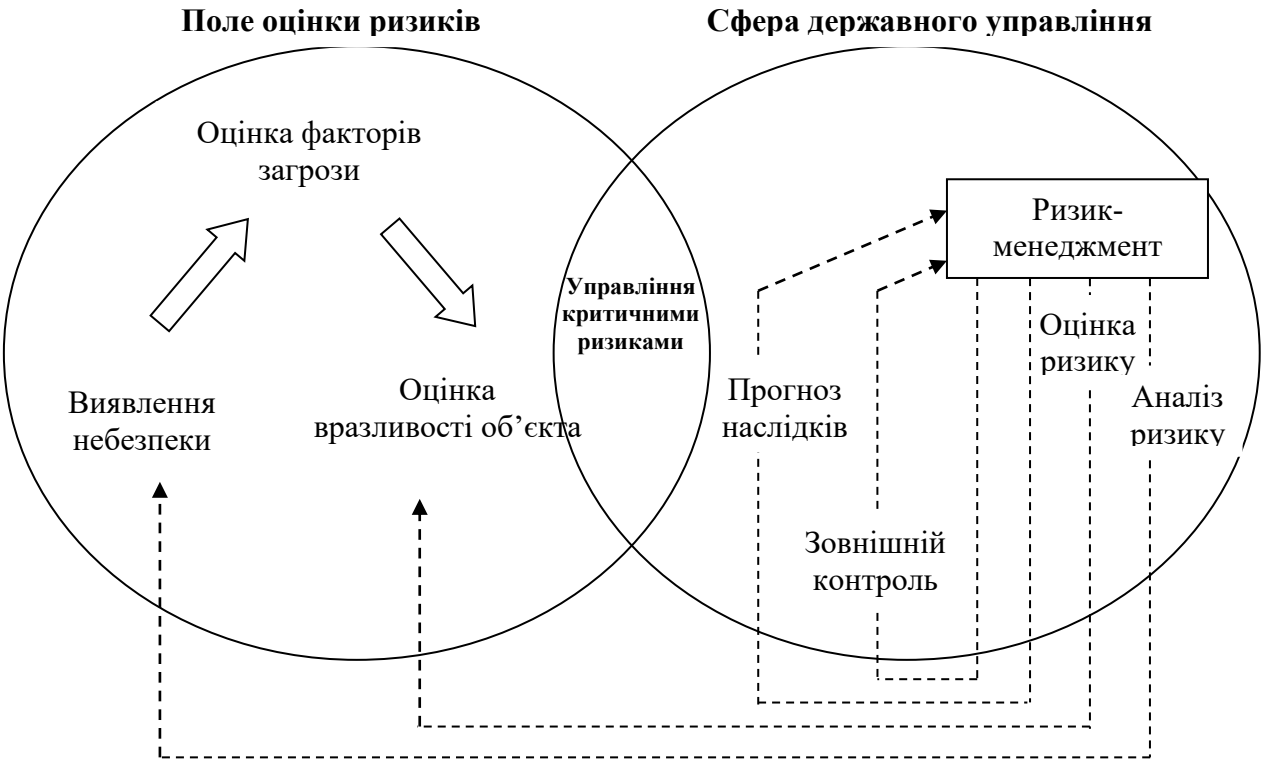


Рис. 3.3. Алгоритм забезпечення критичного ризик-менеджменту як складової державної політики резильєнтності критичної інфраструктури

Джерело: розроблено автором [282, с. 79]

Для просторово-часових характеристик описаного алгоритму виникнення ризикової ситуації критично важливого об'єкту можна використати напрацювання учених В. В. Вітлінського та Г. І. Великоіваненко [225, с. 345], які пропонують використовувати наступні критерії:

– зрозуміле визначення загроз, які можуть детермінувати ризикову ситуацію;

– імовірність виникнення такої ситуації;

– рівень зниження деструктивних наслідків після її виникнення.

Подібна схема задовольняє логіку наукового дослідження забезпечення захисту критичної інфраструктури через механізми адміністративно-правового регулювання в умовах невизначеності. Доречною у даному дослідженні вважаємо думку учених О. Є. Кузьміна, М. Є. Адамів та О. Г. Мельника [103, с. 75], які наголошують, що при інтенсивному зростанні

дефіциту інформаційно-часових ресурсів при обґрунтуванні управлінських рішень, активізується загроза неадекватного тлумачення поточних умов діяльності критичної інфраструктури, що відбиваються на латентності такого рішення. Виходом із даної ситуації вчені вбачають інтеграцію антисипативного управління, орієнтованого на прогнозування потенційних ризиків внутрішнього та зовнішнього середовища. Слід зазначити, що притаманна результатам невизначеність у процесі прийняття рішення інспірує необхідність прогнозування його наслідків, що можна підкріпити вірогіднісною моделлю, на основі застосування методів розпливчастих множин які не піддаються строгій формалізації і мають логіко-аналітичний характер (у нашому випадку – критичний ризик-менеджмент). Основуючись на результатах досліджень учених С. В. Козловського [92, с. 350], С. А. Олизаренка, А. В. Перепелиці та В. А. Капранова [139, с. 42] можна стверджувати, що саме для таких задач доцільно використовувати теорію нечіткої логіки у якості засобу структурування та моделювання для управлінських когнітивних методів і моделей із застосуванням інженерії наукових знань та штучного інтелекту.

Загальна методика моделювання на основі нечіткої логіки, акомодована під умови забезпечення безпеки критичної інфраструктури, має передбачати поетапне розв’язання таких задач: препарація основних детермінант впливу на критичну інфраструктуру та інтеракції між ними; визначення і формалізацію лінгвістичних оцінок факторів; побудову нечіткої бази знань про взаємозв’язки між факторами [115, с. 201]. Прислухаємось до І. Г. Фадєєвої [305, с. 260], котра пропонує декілька алгоритмів систем нечіткого умовиводу, опис яких заснований на поділі вихідного процесу на ряд послідовних етапів:

1. Формування бази даних правил нечіткого висновку системи.
2. Фазифікація вхідних змінних.
3. Агрегація підумов у нечітких умовах правил дії.
4. Активізація або композиція підвисновків в правила нечіткі умови-дія.
5. Накопичення висновків нечіткої умови правила дії.

6. Дефазифікація вихідних змінних.

Отже, при формуванні алгоритму, оператор критичного об’єкту буде аналізувати поточну ситуацію, порівнюючи її з раніше розробленими шаблонами критеріальних факторів, які є ознаками надзвичайної ситуації. Відповідно, описану алгоритмізацію нечітких висновків у межах кризового ризик-менеджменту можна застосовувати у ситуаціях, відносно стабільних та у вузький проміжок часу при мінімальному об’ємі ситуаційної інформації, а формалізовані алгоритмічні узагальнення підходять для прийняття екстрених управлінських рішень на об’єктах критичної інфраструктури, що робить даний процес актуальним в умовах війни [282, с. 75].

У напрямку інституційних перетворень ключовим вважаємо також розробку узагальнених критеріїв та алгоритмів для оцінки резильєнтності. Даний напрям є актуальним рішенням для перетворення феномену резильєнтності в оперативні інструменти у сфері захисту критичної інфраструктури. Іноземні учені Yang Z., Barroca B. потенціал резильєнтності критичної інфраструктури оцінюють в залежності від спроможності квадро-комплексу складових країни: соціально-економічної системи, державних установ, навчально-наукового забезпечення та техніко-інфраструктурної системи [356].

Зазначені складові резильєнтності є потенційно важливими для операційної реалізації державної політики у сфері захисту об’єктів критичної інфраструктури, що в розрізі передбачає елементи «наслідків» та «впливу», які деталізуються в межах конкретної ситуації уже у формі «дія» чи «зусилля». Дані елементи можуть бути інтерпретовані у вигляді витрат, вигод, збитків, побічних ефектів, які необхідно враховувати при практичному управлінні в межах конкретної ситуації на об’єктах критичної інфраструктури. Концептуальний сценарій резильєнтності зобразимо на рис. 3.4, як дуальність основних аспектів резильєнтності – «наслідок» і «дія». Зображений сценарій резильєнтності об’єктів критичної інфраструктури ілюструє алгоритм «як небезпека впливає на систему», і підкреслює дві

умови цього явища:

1) вплив загрози (подія) викликає деструктивні наслідки в постраждалій системі або її компонентах;

2) постраждала система застосовує дії для протистояння, сприйняття, пристосування, адаптації, трансформації, відновлення та навчання відносно загрози.

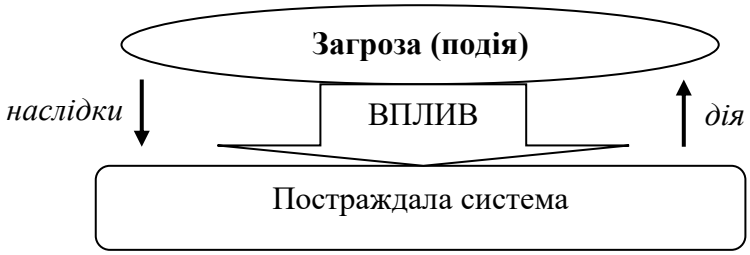


Рис. 3.4. Концептуальний сценарій резильєнтності об’єктів критичної інфраструктури

Джерело: розроблено автором

Слушною у продовжені даного вектору дослідження вважаємо також теорію норвезьких вчених K.Øien та L.Bodsberg [346, с. 17] у якій вони виділяють чотири ключові атрибути «дії» у напрямку досягнення резильєнтності об’єктів критичних інфраструктур – «аналіз ризиків/загроз», «передбачення/підготовка», «проходження/витримка», «реагування/ відновлення» та «адаптація/навчання». Учені також підтверджують запропоновану вище тезу, щодо інтеграції до концептуального сценарію резильєнтності ризик-менеджменту, заснованого на наслідках дій, метою виконання яких є мінімізація їх деструктивного впливу. Відповідно, оцінка наслідків може бути використана для обґрунтування дій. Наслідки певного сценарію досягнення резильєнтності можуть бути використані як досвід для покращення потенційних дій. Крім того, ефективність окремих дій можна оцінити за рівнем зменшення наслідків майбутніх сценаріїв резильєнтності. Отже, оцінка наслідків дій є ірраціональним і безперервним процесом.

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. 3.5).

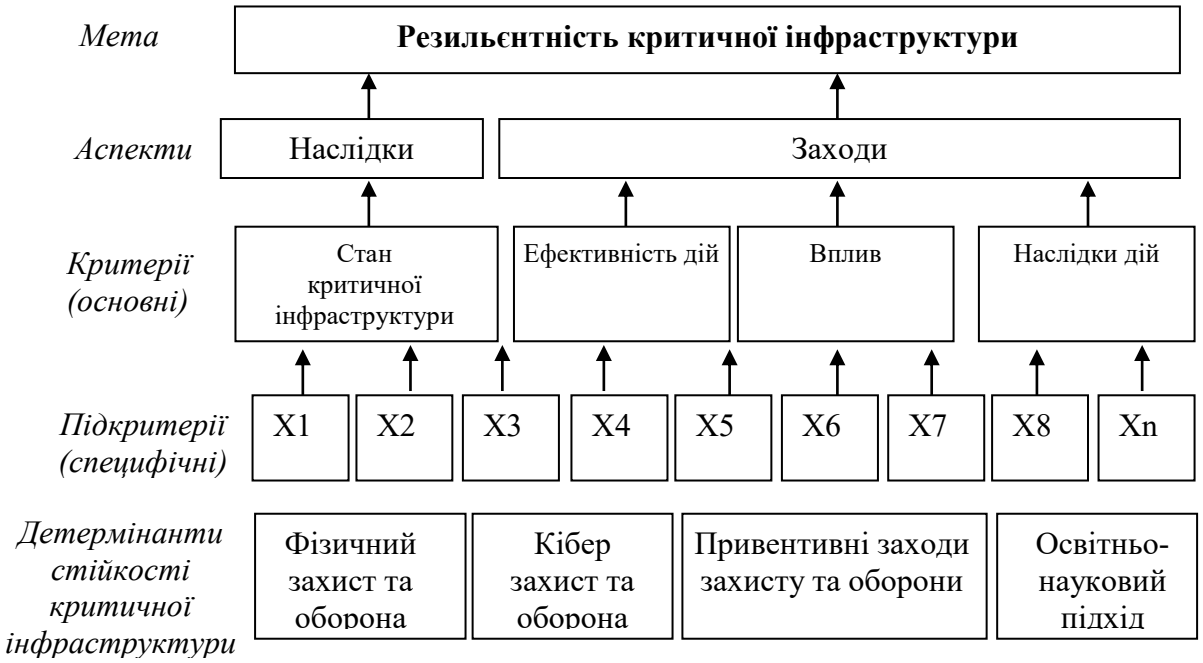


Рис. 3.5. Структурно-логічна схема забезпечення стійкості критичної інфраструктури в межах реалізації державої політики

Джерело: розроблено автором

Структурно-логічну схему забезпечення резильєнтності критичної інфраструктури в межах реалізації державої 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 здійснення суб’єктами у сфері розробки та реалізації державної політики їх унікальних функцій які повинні реалізовуватися державними управлінськими інститутами. Опираючись на проведений аналіз даного вектору у попередніх розділах роботи, погоджуємось із вченими С. І. Кондратовим та О. М. Суходолею [95, с. 26], які вбачають проблему у тому, що відповідальність за захист критично-важливих об’єктів покладається на різні відомства і міністерства, котрі забезпечують функціонування відповідних систем. Одночасно кожна із систем оперує унікальними наборами загроз та ризиків, які вона контролює, унікальні режими функціонування у різних безпекових умовах, унікальні плани і процедури реагування, викладені із застосуванням відомчої термінології і понятійного апарату. Зокрема, визначені у планах і положеннях процедури і механізми комунікації між існуючими національними системами безпеки і кризового реагування переважно є недостатньо апробованими та відпрацьованими у випадках масштабних кризових ситуацій. Це можна пояснити слабко розвинутою практикою міжвідомчих навчань [244, с. 115]. 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 (рис.3.6).

Варто розмежувати рівень загроз на об’єктові, секторальні, національні

та наднаціональні. Відповідно до проєктних загроз потребує розмежування сфери їх відповідальності за наступними секторами:

І. Міжнародний рівень – посилювати координацію з НАТО, діалогу та співпраці між Єврокомісією, Центром координації реагування на надзвичайні ситуації (ERCC), Агентства Європейського Союзу зі співробітництва правоохоронних органів (EUROPOL), Європейського центру компетенції з кібербезпеки (ECCC) застосування механізму «раннього попередження» (UCPM) та ін.

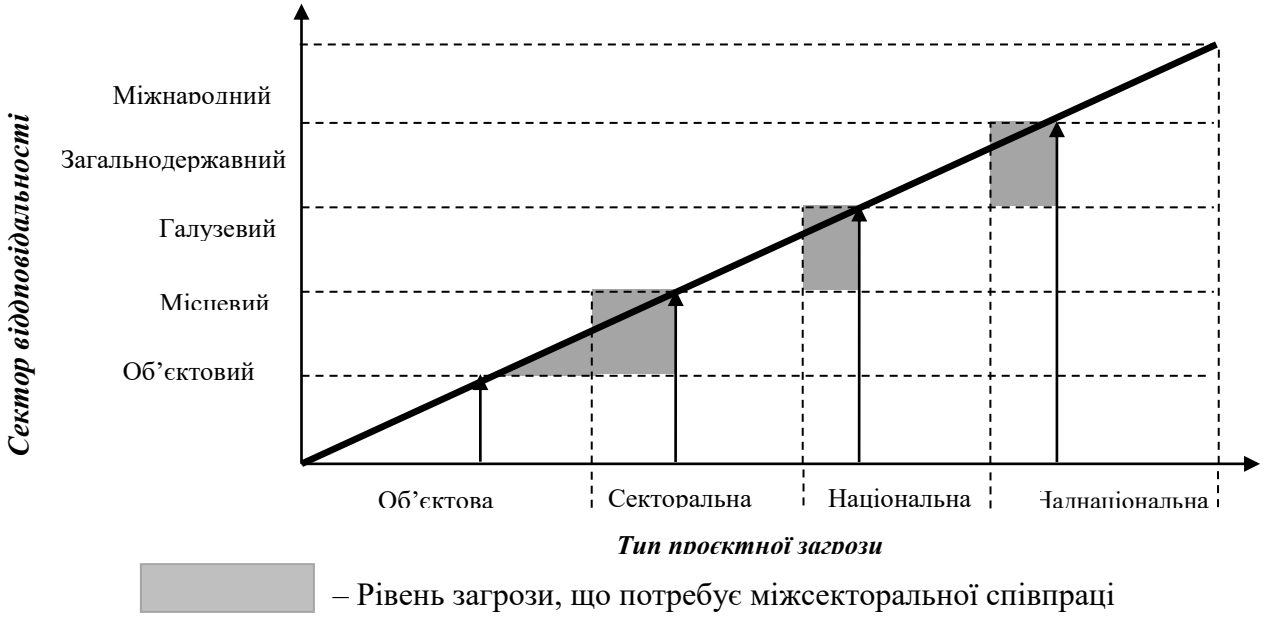


Рис. 3.6. Розподіл відповідальності за типами проєктної загрози

Джерело: узагальнено автором на основі [60], [289, с. 25]

ІІ. Загальнодержавний рівень – реалізується Кабінетом Міністрів України, Національним банком України, органами державної влади згідно розподілу повноважень уповноваженим органом у сфері захисту критичної інфраструктури та іншими державними та центральними органами виконавчої влади.

ІІІ. Регіональний та галузевий рівні – здійснюється центральними та місцевими органами виконавчої влади, яких призначено відповідальними за формування й реалізацію державної політики у сфері захисту об'єктів критичної інфраструктури.

ІV. Місцевий рівень – координується органами місцевого

самоврядування, місцевими органами виконавчої влади, а в умовах воєнного стану – військово-цивільними адміністраціями в межах повноважень.

V. Об’єктовий рівень – здійснюється безпосередньо операторами критичної інфраструктури.

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 тренувань і навчань з оперативного реагування на кризові ситуації на критичних об’єктах з метою посилення рівня міжвідомчої комунікації для превенції загроз. Доцільно проводити дані заходи із обов’язковим залученням представників Національної гвардії, СБУ, Державної прикордонної служби, Національної поліції, ЗСУ, Держслужби з надзвичайних ситуацій, а також представників органів виконавчої влади та місцевого самоврядування, Департаментів цивільного захисту і операторів об’єктів критичної інфраструктури. Дану пропозицію можна віднести до категорії антикризових превентивних заходів державного управління у сфері захисту життєво-важливих об’єктів критичної інфраструктури.

Зобразимо основні положення зазначених міжсекторальних навчань у формі імітаційної моделі навчального сценарію превентивного захисту об’єктів критичної інфраструктури (рис. 3.7).

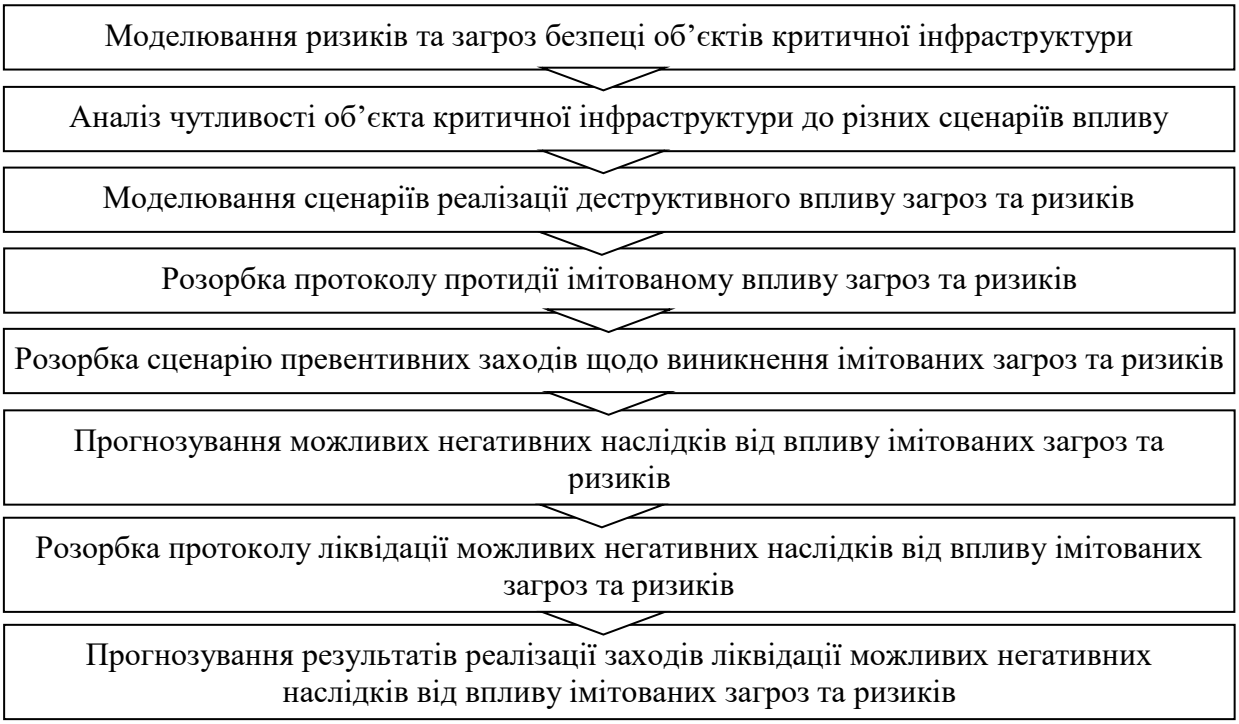


Рис. 3.7. Імітаційна модель навчального сценарію міжсекторальних навчань із превентивного захисту об’єктів критичної інфраструктури

Джерело: узагальнено автором

Дану пропозицію підтримує Г. І. Зубко [83, с. 345], пропонуючи деталізацію описаного навчального сценарію та включити до нього:

– диференціація 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.

Звернемо увагу, що сьогодні одним із найбільш поширених видів зброї дистанційного ураження об'єктів критичної інфраструктури є кіберзброя. Це «кіберзасіб ведення війни, який за конструкцією, поточним або передбачуваним використанням становить загрозу для життя і здоров'я людей, здатен до виведення з ладу або порушення функціонування, пошкодження чи знищення критично важливих об'єктів інфраструктури та призводить до наслідків, які кваліфікуються як кібератака» [270]. Даний факт в умовах цифрового суспільства особливо актуалізує модуль цифровізованого навчання, що передбачатиме посилення заходів кібербезпеки. Також в умовах воєнного стану в Україні із метою посилення резильєнтності критичної інфраструктури та протидії кіберзброї варто в межах інституційних перетворень завершити ініціативу РНБО та Президента України із формування кібервійська. Відповідно до положень Стратегії кібербезпеки України від 27.01.2016 р, зазначена національна система «має забезпечити взаємодію з питань кібербезпеки органів державної влади і місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури» [269].

Продовжуючи дослідження перспектив інституційних перетворень у напрямку підвищення ефективності захисту та резильєнтності критичної інфраструктури, звернемо увагу на дослідження М. Б. Домарацького, який зазначає, що уряди окремих держав розробляють спеціальні галузеві плани

превентивного захисту критичної інфраструктури. Дані документи будуються на аналітичних результатах у напрямках:

– атрибуції секторів критичної інфраструктури стратифіковано за місцевим, регіональним та національним рівнями;

– ідентифікації критичних ризиків та потенційних загроз для об'єктів критичної інфраструктури;

– вивчення вразливості окремих секторів критичної інфраструктури;

– моніторинг ризиків дестабілізації функціонування критично-важливих галузей у разі виведення з ладу або руйнування окремих об'єктів критичної інфраструктури;

– створення відповідних превентивних сценаріїв, у процесі формування системи захисту об'єктів критичної інфраструктури [40, с. 83].

Особливої уваги вимагає тема організації управління у кризових і надзвичайних ситуаціях. При цьому значно зростає складність задач управління, які потрібно вирішувати в умовах високої невизначеності розвитку ситуації, нестачі достовірної інформації і наявності недостовірної інформації, яка поширюється засобами масової інформації. Звичайно, це потребує методик, програм і технічних засобів систем управління, насамперед в інтересах підвищення оперативності прийняття рішень, їх ефективності і контролю виконання. Складність вирішення цих завдань пов'язана з необхідністю координації та інтеграції діяльності широкого кола найрізноманітніших структур. Така робота має органічно вписуватися в єдину систему аналітичного забезпечення органів державної влади, бути скоординованою в рамках діяльності єдиної державної системи.

Одним із ключових векторів державної політики із підвищення резильєнтності об'єктів критичної інфраструктури учені [355, с. 8], [306, с. 5] виділяють формування монолітної державної системи, націленої на гарантування безпеки населення та критичних об'єктів, виконуючи наступні завдання:

– удосконалювати нормативно-правову базу щодо посилення

відповідальності суб’єктів за порушення встановлених правил, норм, вимог, невиконання необхідних робіт, які призвели до збитків;

– розподіляти повноваження, відповідальність і сфери взаємодії органів державної влади з власниками і операторами критичної інфраструктури;

– координувати науково-технічну політику в сфері створення інновацій у секторі технологій безпеки критичної інфраструктури;

– створити об’єднану систему моніторингу стану захищеності та безпеки об’єктів критичної інфраструктури;

– сформувати постійно діючу систему попередження та знешкодження загроз для об’єктів критичної інфраструктури;

– створити систему дозвільного характеру діяльності об’єктів критичної інфраструктури незалежно від форм власності;

– реалізовувати заходи із наповнення загальноукраїнського Реєстру об’єктів критичної інфраструктури диференціюючи критерії за ступенем потенційної терористичної уразливості об’єктів;

– розробка засобів і методів захисту і контролю доступу сторонніх осіб до об’єктів критичної інфраструктури;

– удосконалення системи відбору, допуску, підготовки та атестації керівників і фахівців на об’єктах критичної інфраструктури;

– розробка методики оцінки мір безпеки на об’єктах критичної інфраструктури.

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 макросистеми [355, с. 9], [306, с. 10].

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 резильєнтності, спрямованої на побудову спроможностей реагування на випередження, а не на ліквідацію наслідків основаної на теорії кризового реагування [253, с. 112]. 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 [254, с. 5]. Варто також звернути увагу на дослідження О. О. Резнікової [223, с. 6] яка опублікувала загальне бачення Концепції забезпечення національної стійкості. 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 реагування на кризові ситуації і загрози та планування для координованих дій державних органів.

5. Створити двосторонні канали комунікацій органів державної і місцевої влади з населенням утворити постійно діючі механізми взаємодії органів державної влади та місцевого самоврядування, приватного бізнесу, неурядових організацій 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 комунікації державних органів влади та місцевого самоврядування, приватного бізнесу, неурядових організацій, та міжнародних партнерів з питань забезпечення резильєнтності критичної інфраструктури.

9. Обов’язковість здійснення систематичних міжвідомчих та міжсекторальних тренувань і навчань за участю цивільного населення з

метою посилення рівня готовності до реагування на широкий спектр загроз, посилення стійкості громад, а також економічної та суспільної стійкості [223, с. 7].

В межах зазначеної ініціативи, особливої уваги вимагає блок науково-освітнього забезпечення резильєнтності критичної інфраструктури. Відповідно до Стратегічного оборонного бюлетеня України, значення освіти є одним із ключових напрямів реалізації безпекової політики. У документі визначено основні вимоги і даному напрямку:

– набуття центральними органами виконавчої влади, іншими державними органами необхідних компетентностей щодо задоволення потреб оборони держави і захисту її території від можливої агресії та ефективного управління оборонними ресурсами;

– розвиток компетентностей сил оборони в контексті підготовки до всебічного забезпечення всеохоплюючої оборони України [270].

Актуальність даного вектору підтверджено у Концепції створення державної системи захисту критичної інфраструктури, схваленій Розпорядженням КМУ № 1009-р від 06.12.2017 р. [230], де одним зі шляхів розв'язання проблеми забезпечення захисту критичної інфраструктури визначено «створення системи підготовки та перепідготовки кадрів у сфері захисту критичної інфраструктури та встановлення вимог до планування проведення навчань (тренувань) та заходів щодо захисту критичної інфраструктури» [230]. На цьому також наголошено у Законі України «Про критичну інфраструктуру» [60], п.4, п.5 ст. 25 визначено необхідність: «створення системи підготовки кадрів для сфери захисту критичної інфраструктури» [60] (п.4), «підвищення комплексних знань, навичок і умінь персоналу та керівного складу операторів критичної інфраструктури, персоналу суб'єктів господарювання, які провадять діяльність, пов'язану із забезпеченням безпеки об'єктів критичної інфраструктури, з питань реагування на кризові ситуації на таких об'єктах» [60] (п.5). Значимість наукової складової підкреслено у п.6 ст. 25 , що передбачає «залучення

експертного потенціалу наукових установ, професійних та громадських об’єднань до підготовки галузевих проектів та нормативно-правових актів у сфері захисту критичної інфраструктури» [60]. Однак, аналізуючи Стандарт вищої освіти України за спеціальністю 281 Публічне управління та адміністрування за СВО бакалавра, серед компетенцій фахівця немає жодної, яка б передбачала підготовку до управління безпекою критичної інфраструктури. А у Стандарті даної спеціальності СВО магістра міститься лише одна – СК06. «Здатність здійснювати професійну діяльність з урахуванням потреб забезпечення національної безпеки України», однак вона носить досить загальний характер [129], [130]. У перспективах вирішення даної проблеми слушною вважаємо пропозицію Г. Ю. Зубка [83, с. 367], який пропонує внести зміни до чинного Класифікатора професій та Стандарту вищої освіти України спеціальності 281 Публічне управління та адміністрування в частині доповнення компетентностей орієнтованих на управлінське забезпечення національної системи безпеки об’єктів критичної інфраструктури. Це, у свою чергу, дозволить посилити інституційну спроможність у цій сфері і формування ефективної системи підготовки публічних службовців і працівників державних установ, підприємств і відомств та приватного сектора. Стратегією в питанні державної служби та управління людськими ресурсами передбачено необхідність впровадження сучасної цілісної, мобільної та гнучкої системи професійного навчання державних службовців з розвиненою інфраструктурою та належним ресурсним забезпеченням, що орієнтована на розвиток компетентностей і потреби в професійному розвитку державних службовців [77]. Також варто зазначити, що відповідно до (ст. 49) Закону України «Про Державну службу» [57] передбачено наявність індивідуальних програм підвищення рівня професійної компетентності державного службовця, які складають службовець разом із відомчою службою управління персоналом. Центральним органом виконавчої влади з формування та реалізації державної політики у сфері державної служби є Національне агентство

України з питань державної служби [168], яке відповідно до покладених на нього завдань сприяє розвитку системи закладів освіти надає освітні послуги з підготовки, спеціалізації та підвищення кваліфікації державних службовців. До даних програм також доречно включити блок із підвищення кваліфікації у напрямку забезпечення захисту критичної інфраструктури. Також в Україні існує низка наукових та науково-дослідних організацій, що потенційно спроможні зробити належний внесок у створення та функціонування відповідної системи надання необхідних компетенцій у сфері захисту критичної інфраструктури: провідні класичні університети, заклади освіти системи правоохоронних і силових структур, навчальні заклади та науково-дослідні установи.

Отже, внесення змін до чинного Класифікатора є першим кроком до розбудови як самої національної системи безпеки стратегічної інфраструктури, так і інституційної спроможності у цій сфері. Також до системи підготовки кадрів і населення, окрім перелічених, необхідно буде залучити інші галузеві установи, що мають профільну компетенцію у відповідному секторі, а також залучати експертні спільноти.

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 [350, с. 55]. 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 на наступних напрямках:

– розвиток воєнно-політичного діалогу між Україною та ЄС з

широкого спектру питань спільної глобальної політики забезпечення стійкості критичної інфраструктури;

– підготовка українських фахівців у сфері забезпечення стійкості критичної інфраструктури;

– досягнення взаємосумісності визначених силових підрозділів для участі у спільних навчаннях та операціях

– посилення технологічної інтеграції об’єктів критичної інфраструктури.

Отже, на сучасному етапі удосконалення державної політики у сфері захисту критичної інфраструктури варто сфокусувати інституційні перетворення у точці забезпечення її резильєнтності на основі чинних національних систем безпеки, захисту та кризового реагування за умов еволюції рівня координації дій до якісно нового рівня та взаємодії між ними. Вкрай важливим питанням є врегулювання публічно-приватної взаємодії у формі кластерного підходу до забезпечення захисту об’єктів критичної інфраструктури диференційовано за відповідними сферами. При чому має бути визначено не тільки сфери застосування, принципи, правові засади, форми здійснення та об’єкти критичної інфраструктури, які можуть бути передані у власність приватному партнеру, а також особливості співуправління окремими об’єктами та специфіка партнерської взаємодії тими об’єктами, які належать до сфер національної безпеки з державною монополією.

3.3. Кластерний підхід до забезпечення захисту критичної інфраструктури в умовах воєнного стану в Україні.

Проведені дослідження у сфері державної політики безпеки дають підстави дійти висновку, що Україні вдалося створити унікальну систему захисту об’єктів критичної інфраструктури, комбінуючи різноманітні тактичні прийоми із використанням радянських засобів протиповітряної оборони та сучасних видів озброєння передових країн світу. Створено із

використанням цифрових технологій та мобільних додатків унікальну систему сповіщення населення в режимі реального часу а також моніторингу, фіксації та передачі оперативної інформації. Ефективність продемонструвала також використання проти ворожих повітряних цілей зенітно-ракетних комплексів, винищувачів, розміщення мобільних ударних груп та візуальних постів спостереження. Однак, підтримуємо позицію учених, котрі вважають сучасну модель державного управління в сфері захисту об'єктів критичної інфраструктури реактивною, тобто орієнтованою на вирішення проблем, а не на їх попередження. При цьому, як показують результати аналізу світового досвіду, неможливо досягнути прийнятного рівня безпеки та резильєнтності за відсутності дієвої системи превентивного захисту від проєктних ризиків та загроз [83, с. 213]. Це ставить перед нашою державою дилему зміни загальної парадигми державної політики у цій сфері в умовах зростання військово-терористичної загрози у нашій державі. Як фідбек на вимоги сьогодення, цей вектор передбачатиме розробку стратегії протидії техногенному та інфраструктурному тероризму, інтегруючи нову функцію, пов'язану з необхідністю синхронізації в екстремальних ситуаціях державних служб, приватного сектору та операторів (власників критичних об'єктів), що набуває превентивного значення в умовах постійної ескалації складності сучасних загроз (гібридна війна, техногенний тероризм та ін.). Крім того, в умовах активних бойових дій, у геометричній прогресії зростають ризики випадкового нанесення ударів по об'єктах критичної інфраструктури (у т.ч. ядерним та хімічним). Водночас, враховуючи значну кількість потенційних об'єктів терористичних атак, цілком можливим є свідомі атаки ворога на ядерні об'єкти, з метою дестабілізації суспільства.

Нагальною потребою державної політики резильєнтності критичної інфраструктури є інституційне закріплення питань взаємодії систем захисту. У даному напрямку корисним є досвід США, що інтегрує процес визначення заходів і реального досвіду захисту від загроз і небезпек в сталому режимі. Відповідальність за захист у сталому режимі покладається на спільноту

окремих осіб, домогосподарства, органи влади всіх рівнів, приватний некомерційний сектор, власників і операторів критичної інфраструктури та бізнес. Рекомендується використовувати сталий режим координації для визначення основних сил і засобів, необхідних для виконання місії із забезпечення захисту (рис.3.8).

Рис. 3.8. Сталий режим захисту критичної інфраструктури

Джерело: [158]

Сталий режим захисту вимагає децентралізованого управління ризиками для ефективного виконання завдань. Як національна модель координації між різними партнерами, організаціями та зацікавленими сторонами у сфері захисту, стабільна координація діяльності у сфері захисту спирається на існуючі координаційні структури для обміну інформацією та підтримки обґрунтованої та адаптивної діяльності місії у сфері захисту. Захист є безперервним процесом і вимагає адаптивної моделі організаційного навчання та міжвідомчої координації.

На основі проаналізованого вище досвіду США та країн ЄС, варто обґрунтувати пропозицію щодо законодавчого закріплення механізму спільного захисту критичної інфраструктури. Пропонуємо розглянути інноваційну ідею концепції кластерного підходу до забезпечення резильєнтності критичної інфраструктури в умовах правового режиму воєнного стану в Україні на основі створення Кластерів резильєнтності критичної інфраструктури (КРКІ). Головна ідея даного концепту полягає у

створенні навколо важливих інфраструктурних об’єктів кластерних інтеграційних об’єднань, які будуть спроможні забезпечити синергію безпекових заходів реалізованих в межах співпраці державних інститутів влади, систем захисту та реагування, самих інфраструктурних об’єктів та їх стейкхолдерів [75] (рис. 3.9).

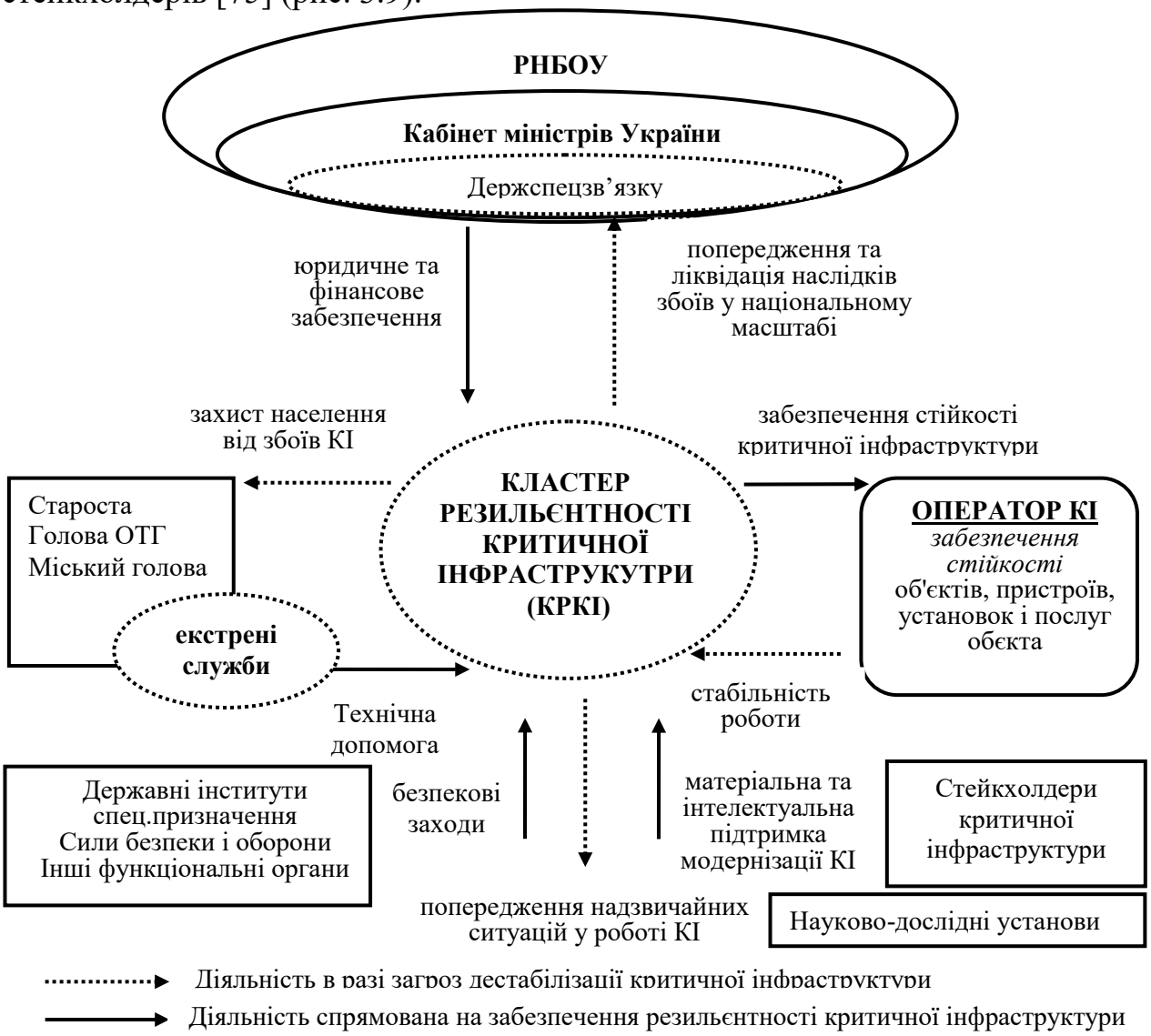


Рис. 3.9. Модель кластерного підходу до забезпечення резильєнтності критичної інфраструктури в Україні

Джерело: розробка автора

Більшість вітчизняних науковців у діагностуванні феномену «кластер» дійшли висновку, що його основними індикаторами є інноваційність, географічна близькість, незалежність учасників та їх спільний інтерес. У нашому випадку, спільним інтересом слід вважати безперебійність

функціонування об’єктів критичної інфраструктури. Важливо зазначити, що кластер впливає не лише на функціональність самих об’єктів, але і на регіон у якому він функціонує. Відповідно, ефекти від створення кластера резильєнтності критичної інфраструктури проявляється у синергії дій його учасників за рахунок: анти тригерних ефектів, ефектів охоплення, масштабу, зниження безпекових витрат, накопичення знань та інновацій, ефекту інвестиційних переваг протидії ризикам, ефект колективного використання інфраструктурних об’єктів, превентивний ефект [248, с. 165].

Інфраструктурні об’єкти в даному проєкті варто розглядати як тригери на основі яких зароджуються конкурентні переваги членів кластера, що присвоює їм статус «стейкхолдера». Цю дефініцію вперше обґрунтував у 1984 р. Е. Фріман у своїй праці «Стратегічне управління: роль зацікавлених сторін» [308, с. 19]. Інтерпретуючи крізь призму пропонованого кластерного підходу трактування Е. Фріманом сутності інтенції «стейкхолдер», можемо дійти висновку, що його зміст передбачає окремих суб’єктів зацікавлених результатами роботи критичної інфраструктури, що є складовими її внутрішнього або зовнішнього середовища та здійснюють певний внесок у поліпшення роботи та захист об’єктів критичної інфраструктури. Колективне використання стейкхолдерами результатів роботи об’єктів критичної інфраструктури дасть змогу зменшити витрати та підвищити економічну вигоду за рахунок мінімізації ризиків дестабілізації роботи. При цьому, кластер, що успішно розвивається стає привабливим для залучення нових учасників.

Європейська практика кластерного підходу засвідчила, що це складні та динамічні структури, які здатні посилити економічне зростання за рахунок використання інноваційного потенціалу регіону. До того ж, в нинішніх умовах правового режиму воєнного стану такі потужні та стабільні об’єднання змогли б швидко рефлексувати на зміну безпекового середовища та переорієнтуватися на виробництво необхідної продукції для потреб ЗСУ та посилення систем захисту. Відзначимо, що кластери в світі стають потужним

інструментом для втілення передових інновацій, діджиталізації, нових сучасних бізнес-моделей, ресурсоефективних технологій, формування засад інклюзивної соціальної креативної економіки та ін..

Підтвердити дієвість та релевантність подібної кластерної ініціативи можемо на прикладі досвіду ЄС, де Директива CER передбачає «розвиток скоординованої міжгалузевої та багатонаціональної оперативної співпраці у сфері захисту критичної інфраструктури від гібридних загроз, не порушуючи при цьому головних принципів ринкового лібералізму» [301]. Отже, сучасний європейський механізм державного управління у сфері захисту критичної інфраструктури закладає у основу доктрину лібералізму, що прагне забезпечити індивідуальну свободу та рівність перед законом. Це природно призводить до розвитку державно-приватного партнерства чи інших багаторівневих моделей управління, що уникають механізму примусу. Зокрема це також представлено у Директиві CER (ст. 9-19), де передбачено, що «регулювання з боку держави передбачає підтримку приватних компаній, які опікуються посиленням стійкості критичної інфраструктури шляхом передачі матеріалів, методологій та навчання персоналу» [301]. Тобто, можемо дійти висновку, що вектор посилення колективності в державній політиці захисту життєво важливих об’єктів у країнах ЄС базується на заходах мотивації, а не примусу. Реальний приклад можемо розглянути в Нідерландах, де існує формат «округів безпеки», який уособлює механізм комунікації органів державної й місцевої влади із неурядовими організаціями та бізнесом щодо питань забезпечення національної стійкості. Перш за все він орієнтований на посилення стійкості місцевих громад до надзвичайних та кризових ситуацій. Округ безпеки передбачає об’єднання спроможностей кількох територіальних громад зі створенням спільного органу управління та з метою забезпечення ефективної взаємодії. Відповідна співпраця територіальних громад здійснюється на основі меморандумів про співробітництво. Місцеві муніципалітети територіально консолідовані в округи безпеки з урахуванням специфіки їх категорії ризиків і загроз та

особливостей безпекового середовища на окремій території держав, зокрема на її кордонах із сусідніми країнами – Бельгією та Німеччиною. Цього досягають через інтеграцію єдиної системи забезпечення безпеки та стійкості, інтеграції ресурсів, посилення спроможностей та їх раціональної експлуатації, підтримання максимального рівня готовності. Важливе значення має налагодження належної взаємодії муніципалітетів та місцевих громад, сил і засобів служб оперативного реагування (протипожежних, протиповеневих, рятувальних, епідеміологічних, невідкладної допомоги, медичних, екологічних, поліцейських та ін.), інститутів антикризового управління, інформаційного, логістичного, консалтингового забезпечення округів, волонтерських організацій і приватних підприємств, територіальних підрозділів державних органів – перш за все сил реагування у вигляді берегової охорони, органів управління та безпеки у галузі водного господарства, армії і флоту та спеціальних служб. Науково-методичний супровід діяльності округів безпеки Нідерландів здійснює Нідерландський інститут громадської безпеки (Nederlands Instituut Publieke Veiligheid – NIPV) [43] Він являє собою інститут громадських знань, який об'єднує та посилює стійкість регіонів безпеки, центрального уряду і партнерів у кризових ситуаціях за допомогою проведення досліджень, освіти, консультування та інформаційної підтримки. NIPV діє як експертний центр, коли мова йде про високоякісні знання щодо управління кризовими ситуаціями. Інститут проводить прикладні дослідження в цій галузі, систематизує науковий і практичний досвід, надає експертну допомогу щодо придбання та експлуатації оперативно-технічних засобів, створює курси професійної підготовки спеціалістів відповідного рівня, створює методичні рекомендації щодо планування у сфері антикризового управління, а також методики, довідники, керівні документи щодо дій округів безпеки в умовах звичайної діяльності та кризових явищ, і розвитку стійкості громад включно [151].

Варто також відзначити факт функціонування Європейського кластеру

безпеки критичних інфраструктур (ECSCI). Основною метою даної організації є дослідницька діяльність орієнтована на створення синергії та сприяння генерації проривних рішень для розв'язання проблем безпеки та захисту критичної інфраструктури за допомогою міжпроєктної співпраці та інновацій. Діяльність відбувається із висвітленням різних підходів до кластерних проєктів організовуючи національні й міжнародні семінари, міжнародні конференції за участю представників промисловості, політиків, науковців та представників Європейської Комісії [145]. Ще однією ініціативою ЄС, яка варта уваги у забезпеченні резильєнтності критичної інфраструктури, є служба науки та знань Європейської комісії, Об'єднаний дослідницький центр (European Commission's Joint Research Centre – JRC) [146] – спільний науково-дослідницький центр Європейської комісії, який забезпечує незалежні наукові та технічні підтримку для розроблення, виконання та моніторингу політики ЄС. У сфері критичної інфраструктури дана платформа передбачає функціонування Європейської довідкової мережі захисту критичної інфраструктури (ERNCIP, n.d.), робота якої організована в тематичних групах критичної інфраструктури (наприклад, авіація, промисловість, продовольча безпека та ін.), які об'єднують сотні дослідників та експертів різних країн, які працюють у відповідних наукових колах або компетентних державних органах [145]. Отже, можна стверджувати, що політика держави має зосереджуватись на посиленні ролі приватного сектору у захисті та фінансуванні критичної інфраструктури, шляхом реалізації проєктів зі створення кластерів резильєнтності критичної інфраструктури, а також посилення ролі науково-інтелектуального потенціалу країни.

Особливої уваги вимагає науково-інформаційне забезпечення в межах функціонування КРКІ. Приклад ефективної комунікації можемо знайти в ЄС, де функціонують Центри обміну інформацією та аналізу (Information Sharing and Analysis Centers – ISACs). Це некомерційні організації, які створюють централізований ресурс для збору інформації про основні загрози, їх причини та інциденти, що стосуються безпеки критичної інфраструктури. Дані центри

діють на умовах публічно-приватного партнерства, забезпечуючи реверсний обмін аналітичними даними, знаннями та досвідом між приватним і державним секторами. ISAC або подібні ініціативи існують у більшості країн-членів ЄС. ISAC глибоко інтегруються в інформаційний простір свого сектору, транспортуючи важливу інформацію до відповідних суб'єктів захисту [147]. У більш розширеному форматі дана структура існує також у США, де функціонує Real Estate Information Sharing and Analysis Center (RE-ISAC). Роль Real Estate ISAC полягає в підтримці місії захисту критичної інфраструктури власників і операторів шляхом надання інформації про потенційні антропогенні інциденти та стихійні лиха, щоб вони могли визначити потенційні ризики, пом'якшити їх, наскільки це можливо та ефективно реагувати [152].

Модель кластерного підходу до забезпечення резильєнтності критичної інфраструктури в Україні також здатна забезпечити значні перспективи до організації міжсекторального навчання та підвищення кваліфікації на основі обміну інформацією, досвідом та залученням науково-дослідницьких установ. Підтвердження перспективності даного напрямку та його практичну реалізацію можемо знайти у досвіді США [164], де дана модель проведення комплексу навчальних (тренінгових) заходів реалізуються у вигляді:

– семінарів (Seminars) та воркшопів (Workshops) – передбачають активну форму залучення кола зацікавлених сторін до вивчення окремих проблем у сфері захисту критичної інфраструктури, їх обговорення, роз'яснення інноваційних підходів, новітніх правил та процедур реагування;

– «настільних вправ» (Tabletop Exercises, TTX) – забезпечують активне аудиторне обговорення, теоретичне відпрацювання способів реагування на певні абстрактні події, дискусії стосовно дієвості стандартних регламентів, планів та протоколів дій відповідальних суб'єктів на проєктні загрози та ризики на об'єктах критичної інфраструктури. Фактично даний вид навчання передбачає оцінку ефективності інституційно-правовго забезпечення захисту критичної інфраструктури а не дій операторів чи безпекових служб;

– фокусне навчання (Drills) – проводиться в реальному часі із залученням безпосередніх учасників, сил та засобів сфери захисту критичної інфраструктури в мінімальному обсязі, який регламентується функціональною спрямованістю заходу. Даний вид навчання націлений на аудит спроможності кадрового складу відповідних служб у стандартних надзвичайних ситуаціях на об'єктах критичної інфраструктури (наприклад пожежна евакуація);

– повномасштабні тренування (Full-Scale Exercises) – проводяться в реальному часі та в умовах детальної імітації нестандартної надзвичайної ситуації до яких залучаються усі сили та засоби реагування у повному складі.

Аналізуючи досвід США та інших країн НАТО у сфері розширення компетентностей кадрового складу сфери захисту критичної інфраструктури можна виділити наступні підходи до сфери між секторальних навчань і тренувань:

1) залежно від масштабу охоплення секторів критичної інфраструктури, процес тренувань та навчання можна поділити на міжнаціональне, загальнодержавне, регіональне та територіальне, секторальне, кластерне та об'єктове;

2) залежно від залучених до процесу тренувань на навчання сил, ресурсів та суб'єктів захисту, а також складеності та масштабності завдань, що відпрацьовуються, їх можна поділити на командно-штабні та тактико-спеціальні;

3) процедури навчань і тренувань дозволяють отримати комплексну оцінку спроможності державної політики у сфері безпеки критичної інфраструктури та стану готовності сил реагування на кризові ситуації.

Перекладаючи досвід США з питань формування та розвитку системи підготовки персоналу з питань забезпечення безпеки та стійкості стратегічної інфраструктури на українські реалії, варто зосередити увагу на таких аспектах, як нормативно-правове та організаційне забезпечення такої системи особливо в умовах здійснення реформи державного управління,

ініційованої Стратегією реформування державного управління України на 2022-2025 роки [227].

Отже, відповідно до проведеного вище аналізу, у сфері захисту критичної інфраструктури потребують уточнення питання, що стосуються підготовки кадрів, підвищення компетентностей та залучення експертного потенціалу з питань її захисту та забезпечення резильєнтності. Така підготовка має відбуватися на принципах системності та систематичності відповідно до кадрових потреб цільових інститутів профільними закладами освіти та експертними організаціями і науково-дослідними установами.

Основними механізмами моделі кластерного підходу до забезпечення резильєнтності критичної інфраструктури в Україні варто передбачити:

– розробку й реалізацію загальнодержавних, регіональних та місцевих програм підтримки та мотивування створення кластерів резильєнтності критичної інфраструктури з інтегрованими захисними механізмами;

– ініціювання організації галузевих та міжгалузевих асоціацій, об’єднань та громадських організацій, спеціалізованих фондів з дифузії об’єктів критичної інфраструктури до бізнес-середовища;

– формування спроможних кластерів резильєнтності критичної інфраструктури.

Отже, можемо зробити висновок, що кластери резильєнтності критичної інфраструктури – це інноваційний формат публічного управління в сфері забезпечення безпеки, стійкості й економічного розвитку регіонів, який передбачає об’єднання спроможностей територіальних громад, інститутів публічного управління, наукових установ, об’єктів критичної інфраструктури та їх стейкхолдерів шляхом створення спільного об’єднання з метою координації і розширення взаємодії. Як свідчить міжнародна практика, сутністю цього явища є встановлення довгострокових стратегічних відносин у реалізації суспільно значущих проєктів між приватним сектором, публічною владою та об’єктами критичної інфраструктури. В умовах України, зазначена ініціатива стає можливою до практичного втілення в

межах реалізації проєктів «державно-приватного партнерства», яке передбачено у відповідному Законі України [55]. У зазначеному нормативному акті явище державно-приватного партнерства трактується як «співробітництво між державою Україна, Автономною Республікою Крим, територіальними громадами в особі відповідних державних органів, що згідно із Законом України «Про управління об'єктами державної власності» здійснюють управління об'єктами державної власності, органів місцевого самоврядування, Національною академією наук України, національних галузевих академій наук (державних партнерів) та юридичними особами, крім державних та комунальних підприємств, установ, організацій (приватних партнерів), що здійснюється на основі договору в порядку, встановленому цим Законом та іншими законодавчими актами, та відповідає ознакам державно-приватного партнерства» [55]. Серед таких ознак:

1) створення та/або будівництво (нове будівництво, реконструкція, реставрація, капітальний ремонт та технічне переоснащення) об'єкта державно-приватного партнерства та/або управління (користування, експлуатація, технічне обслуговування) таким об'єктом;

2) довготривалість відносин (від 5 до 50 років);

3) передача приватному партнеру частини ризиків у процесі здійснення державно-приватного партнерства;

4) внесення приватним партнером інвестицій в об'єкт державно-приватного партнерства [55].

Отже, можемо дійти висновку що термін «державно-приватне партнерство» носить широкий спектр сфер застосування, серед яких можна виокремити наступні сфери дотичні до критичної інфраструктури:

– генерація, транспортування і постачання теплової енергії та перерозподіл і постачання природного газу;

– будівництво та експлуатація доріг, автострад, залізниць, мостів, шляхових естакад, злітно-посадкових смуг на аеродромах, морських і річкових портів та їх інфраструктури, тунелів і метрополітенів;

– збір, очищення та розподіл води;

– забезпечення функціонування меліоративних систем;

– виробництво, розподілення та постачання електричної енергії.

Зауважимо, що зазначений список не охоплює усі сектори критичної інфраструктури, що обмежує можливості застосування його норм до формування кластерів резильєнтності в усіх сферах критичної інфраструктури, а також залучати інші недержавні організації сфери публічного управління. Відповідно вирішення даної дилеми потребує ухвалення окремого закону чи внесення відповідних змін до чинних законів у сфері захисту та резильєнтності критичної інфраструктури. Реалізація цього завдання в умовах воєнного стану та військового вторгнення рф передбачає налагодження тісної співпраці і створення дієвих організаційних механізмів на загальнодержавному, а також локальному місцевому та регіональному рівнях. Зокрема на низових рівнях слід забезпечити первинне реагування на ризики, загрози і кризові ситуації. Таким чином оперативність, ефективність та превентивність заходів реагування на подібні явища дозволить попередити деструктивний вплив на критичну інфраструктуру. Створення стабільних форматів взаємодії органів державної і місцевої влади, підприємств та організацій, інститутів самоорганізації населення, науково-дослідних установ із об’єктами критичної інфраструктури на регіональному і локальному рівнях є умовою ефективності провадження державної політики у сфері забезпечення безпеки та резильєнтності критичної інфраструктури. Головною умовою має стати посилення превентивних заходів, що дозволить трансформувати модель державного управління у сфері захисту критичної інфраструктури із реактивної у активну фазу.

Юридично базові відносини в межах функціонування кластеру резильєнтності критичної інфраструктури пропонуємо врегулювати відповідно до ст. 1130. ЦКУ, яка передбачає заключення договору «Про спільну діяльність» [276], згідно якого сторони зобов’язані «спільно діяти без створення юридичної особи для досягнення певної мети, що не суперечить законодавству» [276]. Договір про спільну діяльність можуть оформляти підприємства, спеціалізовані як на окремих товарах (послугах), так і окремих

технологічних процесах. За договором простого товариства учасники беруть зобов'язання об'єднати свої вклади для досягнення спільної мети, наприклад, спільного будівництва об'єкту критичної інфраструктури, необхідного усім учасникам. У зазначених договорах можуть брати участь як приватні, так і державні суб'єкти, а також некомерційні організації. Тобто, дана організація передбачає колективне інвестування у необхідне обладнання для функціонування критичної інфраструктури та її резильєнтності.

З метою розвитку нормативно-правового поля адаптації моделі кластерного підходу до забезпечення резильєнтності критичної інфраструктури в Україні, прислухаємось до пропозицій учених О.Ю. Носова та Т. В.Черничко, які наголошують, що з цією метою слід сформувати методичні рекомендації щодо реалізації кластерної політики та створення кластерів резильєнтності критичної інфраструктури [137, с. 24]. За основу можна взяти Закон України «Про стимулювання розвитку регіонів» [74], який визначає правові, економічні та організаційні засади реалізації державної регіональної політики щодо стимулювання розвитку регіонів та подолання депресивності територій із внесенням відповідних змін. У даному контексті стимулювання розвитку регіонів могло би також здійснюватись на засадах моделі кластерного підходу до забезпечення резильєнтності критичної інфраструктури в Україні. Зазначена модель відповідає напрямкам державної регіональної політики, зазначеної у Законі України № 2389-IX від 09.07.2022 р. «Про внесення змін до деяких законодавчих актів України щодо засад державної регіональної політики та політики відновлення регіонів і територій» [54] зокрема відповідає наступним положенням:

– включає вектори відновлення регіонів і територій, що постраждали внаслідок збройної агресії проти України, в соціальному, гуманітарному, економічному, екологічному, безпековому та просторовому вимірах;

– передбачає адаптацію регіональної економіки та суспільства для посилення стійкості територіальних громад до безпекових викликів;

– створює ефективний механізм представництва інтересів мікросередовища на загальнонаціональному рівні.

Важливим є розробка алгоритму створення територіального кластеру резильєнтності критичної інфраструктури, який можемо зобразити на основі інтерпретації проаналізованого закордонного досвіду та інституційно-правового поля України (рис.3.10).

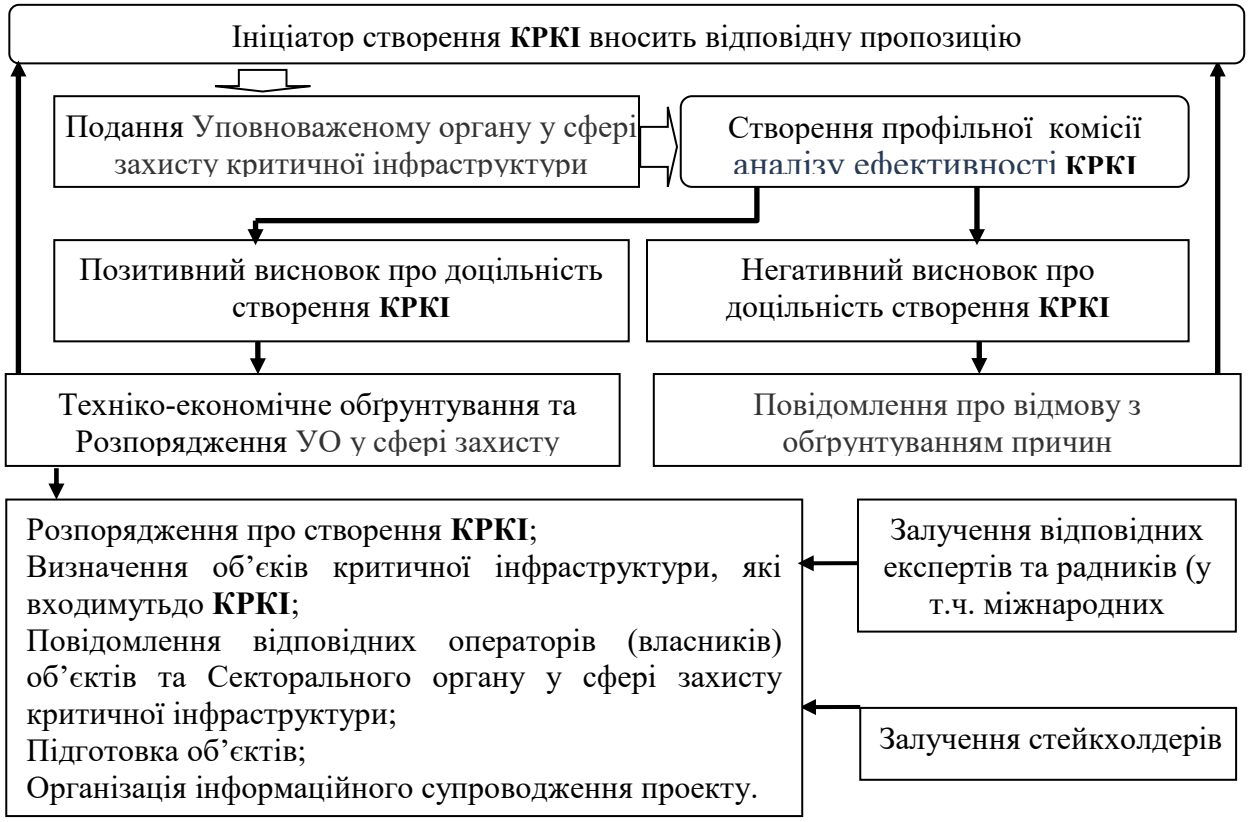


Рис.3.10. Алгоритм створення територіального кластеру резильєнтності критичної інфраструктури

Джерело: сформовано автором на основі [60], [200].

Ініціювати створення територіального кластеру резильєнтності критичної інфраструктури на основі пропозиції про здійснення державно-приватного партнерства можуть центральні, місцеві органи виконавчої влади, органи місцевого самоврядування чи органи АРК, Національна академія наук України, галузеві академії наук, державні, комунальні підприємства, установи, організації, господарські товариства (100 відсотків статутного капіталу яких належить державі), територіальні громади а також суб'єкти, які можуть бути стейкхолдерами відповідних об'єктів критичної інфраструктури. Зазначені суб'єкти подають до Уповноваженого органу у сфері захисту критичної інфраструктури відповідне подання та підготовлену

концептуальну записку необхідності створення КРКІ. Останній здійснює оцінку відповідності пропозиції вимогам законодавства та ініціює створення відповідної Комісії для оцінки ефективності, територіальних та функціональних можливостей КРКІ, до складу якої входять члени комітетів Верховної Ради України, до предмета відання яких належать об'єкти критичної інфраструктури та питання регіональної політики. Подання складається з концептуальної записки де обґрунтовано концептуальні аспекти формування відповідного кластеру. Комісія здійснює оцінку та визначає склад функціональних типів територій України на яких планується створення кластеру та аналізує техніко-економічні особливості на основі чого формує висновок за результатами аналізу ефективності. Висновок містить інформацію щодо проєкту, інформацію про очікувані соціально-економічні, екологічні та безпекові результати створення КРКІ, обґрунтування факторів, що обумовлюють підвищення ефективності реалізації проекту саме у формі кластерної моделі, обґрунтування інформації про ризики здійснення проєкту, інформацію про потребу в державній підтримці та її форму (матеріальна, фінансова, інформаційна та ін.), інформацію про організаційну форму здійснення діяльності та висновок стосовно доцільності (недоцільності) створення КРКІ. Якщо Комісія встановлює, що пропозиція створення кластеру є недоцільною, вона видає негативний висновок, який має бути обов'язково достатньо аргументованим та повідомляє про це Уповноважений орган у сфері захисту критичної інфраструктури. Уповноважений орган повідомляє про відмову в розгляді пропозиції суб'єкту, який подав пропозицію, із зазначенням підстави відмови. У разі хвального висновку Комісія повідомляє про це Уповноважений орган у сфері захисту критичної інфраструктури та розробляє техніко-економічне обґрунтування, останній видає відповідне розпорядження про створення КРКІ та повідомляє про це суб'єкт, який подав пропозицію [200], [222].

Для планування відновлення та стимулювання розвитку регіонів та

територій, а також з метою запровадження кластерів резильєнтності критичної інфраструктури Законом України № 2389-IX від 09.07.2022 р. «Про внесення змін до деяких законодавчих актів України щодо засад державної регіональної політики та політики відновлення регіонів і територій» [54] визначаються такі функціональні типи територій: території відновлення, регіональні полюси зростання, території з особливими умовами для розвитку, території сталого розвитку. Перелік функціональних типів територій, а також вимоги щодо показників для віднесення територій до різних функціональних типів визначаються Кабінетом Міністрів України.

Розпочати апробацію зазначеної ініціативи пропонуємо саме із територій відновлення. Дана категорія Законом ідентифікується як «мікрорегіони, територіальні громади, на території яких відбувалися бойові дії та/або які були тимчасово окуповані, та/або території яких зазнали руйнувань об'єктів критичної інфраструктури, соціальної інфраструктури, об'єктів житлового фонду внаслідок ведення бойових дій, а також які характеризуються різким погіршенням рівня соціально-економічного розвитку та значним переміщенням населення до інших регіонів та/або інших держав».

Регіональними полюсами подальшого розвитку моделі кластерного підходу до забезпечення резильєнтності критичної інфраструктури в Україні є мікрорегіони та територіальні громади, що віднесені до територій сталого розвитку. Вони є самодостатніми, з наявним соціально-економічним потенціалом територій та спроможні до збалансованого розвитку в економічній, соціальній та екологічній сферах.

У напрямі інституційно-правового врегулювання запропонованих ініціатив підтримуємо пропозицію Г. Ю. Зубка [83, с. 124]. щодо внесення відповідних змін до законів України «Про державно-приватне партнерство», «Про управління об'єктами державної власності», «Про концесію», які регулюють переважно партнерство і взаємодію в галузі економіки та реалізації інвестиційних й інфраструктурних проєктів а також Закону «Про

критичну інфраструктуру». Серед основних завдань кластерів варто визначити:

– підтримка публічно-приватного партнерства у розбудові системи захисту критичної інфраструктури, заснованої на спільній відповідальності, співпраці та довірі, а також інших принципах лібералізму державної політики, доступних для них інформаційних каналах, зовнішня підтримка, суттєва допомога або допомога у пошуку компетентних експертів, здатних вирішити конкретні проблеми, що виникають у функціонуванні критичної інфраструктури;

– співпраця з науковими установами в ідентифікації ризиків та загроз критичній інфраструктурі та допомога в пошуку компетентних експертів у побудові комплексу превентивних заходів та методів їх застосування, методів прогнозування результатів, які можуть бути використані при удосконаленні моделі кластерного підходу до забезпечення резильєнтності критичної інфраструктури в Україні;

– звітність про проблеми, виявлені під час впровадження моделі кластерного підходу, подання пропозицій щодо вирішення проблем та пропозицій щодо вдосконалення системи захисту органам державної влади;

– розробка пропозицій внесення змін до нормативно-правових актів з метою сприяння та підтримки виконання завдань у сфері забезпечення резильєнтності критичної інфраструктури;

– оцінка ризиків порушення роботи систем критичної інфраструктури, спричиненого руйнуванням або дисфункцію об’єктів (збір інформації, необхідної для виявлення загроз, прогнозування наслідків та визначення вразливостей критичних об’єктів);

– співпраця з органами, до компетенції яких входять регулювання питань критичної інфраструктури;

– співпраця з іншими координаторами функціонування критичної інфраструктури (ідентифікація взаємозалежностей між системами критичної

інфраструктури, робота з експертами з інших систем, моделюванням вразливостей та превентивних заходів, інформування про загрози);

– співпраця з операторами критичної інфраструктури у сфері її захисту, активізація співпраці із науковими установами та її підтримка (ініціювання та підтримка контактів, запрошення на конференції, симпозіуми, тренінги, на яких розглядаються питання, пов'язані із резильєнтністю критичної інфраструктури, оцінкою ризиків, методами управління у надзвичайних ситуаціях, підготовка консультативних зустрічей з операторами критичної інфраструктури, тощо);

– задоволення потреб операторів та стейкхолдерів щодо обміну актуальною інформацією;

– підтримка організації системних міжсекторальних навчань з підвищення ефективності захисту критичної інфраструктури (допомога в розробці програми навчань, допомога у приєднанні до програми, виконання ролі арбітра, спостерігача навчань, допомога в оцінці результатів навчань, допомога в наданні необхідної інформації);

– діяльність, спрямована на відновлення функціональності пошкоджених об'єктів критичної інфраструктури (підтримка контактів з операторами щодо їхніх потреб, надання інформації іншим координаторам системи, органам державної влади, допомога в пошуку компетентних експертів та інвесторів) ;

– проведення періодичного аналізу та оцінки ефективності захисту критичної інфраструктури у відповідній системі (на основі співпраці з операторами, робочих візитів, опитувань, інтерв'ю);

– стимулювання впровадження сучасних методів захисту критичної інфраструктури (збір інформації про сучасні методи захисту, обмін цією інформацією з операторами критичної інфраструктури);

– організація тренінгів, конференцій та науково-дослідницьких симпозіумів, удосконалення організаційно-технічних та формально-правових

заходів щодо протидії збоям у функціонуванні критичної інфраструктури;

– стимулювання активності суб'єктів, залучених до процесу захисту критичної інфраструктури (листування, опитування та інтерв'ю щодо виявлення прогалин у системі захисту та потреб операторів, візити, збір тем для обговорення та ін.);

– підтримка системних ініціатив, спрямованих на підвищення безпеки критичної інфраструктури (збір інформації про ініціативи операторів щодо підвищення її безпеки, матеріально-технічна підтримка, допомога в контактах зі стейкхолдерами, які можуть посилити ці ініціативи та ін.).

Як показують результати досліджень, найперспективнішими джерелами фінансування ініціатив розвитку кластерів резильєнтності критичної інфраструктури в умовах воєнного стану в Україні можуть стати наступні міжнародні проєкти, що доступні в межах програм, що реалізуються міжнародними фондами:

– програми підтримки розвитку інноваційного підприємництва на локальному та міжнародному рівнях (наприклад Accelerate-2030, Climate-KIC Accelerator, European Institute of Innovation and Technology та ін.);

– міжнародна система освіти, міжнародні форуми, конференції та семінари у напрямку розвитку необхідних компетентностей (наприклад USAIDE, PAUCI, Open Society Institute, Soros Foundation та ін.);

– проекти розвитку та підтримки транскордонного співробітництва (Світовий банк, фонди ЄС, ОЕСР та ін.).

Для ефективного відновлення інфраструктури в межах кластерів резильєнтності критичної інфраструктур після екстремальних подій операторам важливо знати фактори (зовнішні, технічні та організаційні), які впливають на процес відновлення та можливість спрогнозувати можливі наслідки. Такі знання допоможуть операторам та інститутам державної влади приймати раціональні рішення на основі реалістичної оцінки швидкості та часу потрібного на відновлення продуктивності інфраструктурного об'єкта. У даному випадку корисним вважаємо підхід до забезпечення резильєнтності

критичної інфраструктури на основі «трикутника стійкості». Дана теорія ілюструє втрату продуктивності об'єкта критичної інфраструктури у часі (рис 3.11.).

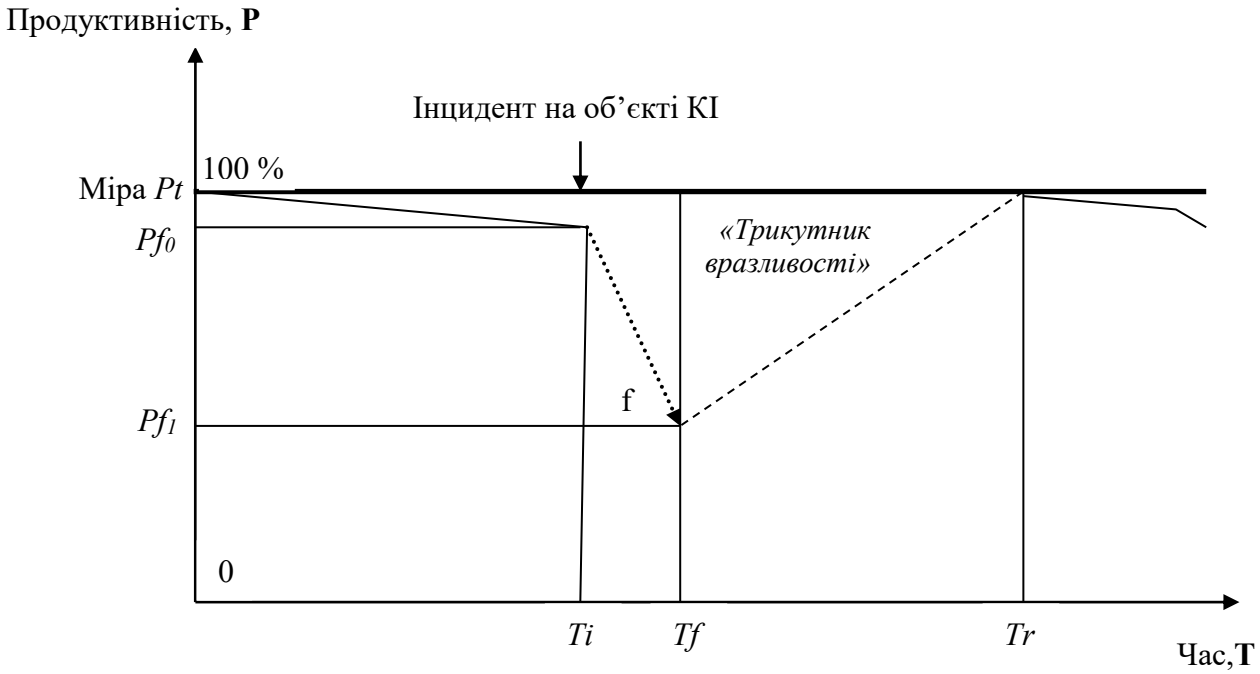


Рис. 3.11. Моделювання втрати продуктивності об'єктом критичної інфраструктури

Джерело: розроблено автором на основі [288, с. 742], [344, с. 8]

Цей підхід базується на гіпотезі про те, що якість послуг об'єкта критичної інфраструктури для потреб стейкхолдерів визначено міру Pt (100%), яка в нормальних умовах є стабільною у часі (наприклад електропостачання). Однак, продуктивність (P) може коливатися від 0% до 100%, (залежно від певних факторів впливу) де 100% означає відсутність погіршення якості обслуговування, а 0% означає, що послуга недоступна. Інцидент деструктивного впливу на об'єкт (наприклад ракетний удар), що стався у момент часу T_i, може завдати миттєвої шкоди критичній інфраструктурі, що призведе до негайного зниження продуктивності (від 100% до 0%). Очікується, що у момент часу T_f розпочнеться процес відновлення інфраструктури відбуватиметься з часом, як показано на цьому малюнку, до часу Tr, коли вона буде повністю відремонтована (вказується

якістю 100%). «Трикутник вразливості» об’єкта критичної інфраструктури ілюструє обсяг втрати продуктивності та час необхідний на його відновлення, що залежить від превентивних заходів проведених на об’єкті. Таким чином, чим менша площа даного трикутника, тим резильєнтнішою є інфраструктура. Ця гіпотеза підкреслює, що резильєнтність має свої часові виміри, включаючи здатність чинити опір, реорганізовуватися, змінюватися та навчатися у відповідь на загрозу. Отже, складові описаного «трикутника вразливості» можуть бути компенсовані тріадою відповідних детермінант резильєнтності – протидія (превентивний захист), адаптація та відновлення.

На основі запропонованої гіпотези, з метою можливості оцінки досягнутої резильєнтності критичної інфраструктури в межах кластерної моделі, варто розглянути можливість застосування певного вимірника. З цією метою можна ініціювати застосування Індексу резильєнтності критичної інфраструктури (stability index – SI), як суми індексу ефективності превентивного захисту, індексу адаптованості до загроз, індексу відновлюваності критичної інфраструктури:

$$SI_{KI} = \mathrm{RI}_{KI}\mathrm{AI}_{KI}\mathrm{PPI}_{KI}$$

Чим вищий показник індексу, тим вища резильєнтність і тим стійкішою є критична інфраструктура.

Індекс відновлюваності критичної інфраструктури (RI_{KI}) – це співвідношення рівня регенерації функціональності, яке вимірюється як рівень відновленої виробничої потужності (restored production capacity – RPC) до втраченої виробничої потужності (lost production capacity – LPC):

$$RI_{KI} = \frac{\mathrm{RPC}}{\mathrm{LPC}} * 100\% \qquad (3.1.)$$

Індекс адаптованості до загроз (IA_{KI}) – відношення часу на відновлення одиниці продуктивності у результаті впливу зафіксованого деструктивного інциденту (performance recovery time – PRT) до часу на відновлення одиниці продуктивності при повторному інциденті того ж характеру (performance recovery time – PRT re-incident):

$$\mathrm{A}I_{KI} = \frac{\mathrm{PRT}}{\mathrm{PRT\,re-incident}} * 100\% \qquad (3.2.)$$

Індекс ефективності превентивного захисту (PPI_{KI}) – відношення між реальним рівнем продуктивності критичної інфраструктури (real level of productivity – RLP) після інциденту із урахуванням застосованих превентивних мір до прогнозованого рівня продуктивності цієї інфраструктури (predicted level of productivity – PLP) після надзвичайної ситуації на основі розроблених превентивних заходів.

$$\mathrm{PPI}_{KI} = \frac{\mathrm{RLP}_{KI}}{\mathrm{PLP}_{KI}} * 100\%$$

Рівень продуктивності вимірюється кількістю нормально працюючих компонентів у системі інфраструктури та достатнім рівнем її потужності для виконання своїх функцій.

Отже, пристальної уваги законодавчої влади в Україні потребують питання забезпечення резильєнтності критичної інфраструктури, зокрема комплексне удосконалення правової основи захисту критичної інфраструктури, створення системи державного управління її безпекою, налагодження співробітництва між суб'єктами систем безпеки та сил реагування на надзвичайні ситуації, розвиток публічно-приватного партнерства у сфері критичної інфраструктури, розроблення та запровадження механізмів комунікації між державними інститутами, населенням і приватним бізнесом стосовно загроз та ризиків критичній інфраструктурі, розвиток міжнародного співробітництва в цій сфері та посилення вектору превентивного захисту. Реалізація цих завдань в умовах військового стану та військового вторгнення рф передбачає налагодження тісної співпраці і створення дієвих організаційних механізмів на загальнодержавному рівні, а також на регіональному, місцевому та локальному рівнях, що дозволить активізувати превентивне реагування на кризові ситуації та загрози. З цією метою необхідним є ініціалізація постійно функціонуючих форматів комунікації населення, органів державної і місцевої влади, підприємств і організацій. Це є необхідною умовою ескалації

ефективності державної політики у сфері захисту та стійкості критичної інфраструктури. Цього можна досягти за рахунок створення кластерів резильєнтності критичної інфраструктури на основі публічно-приватного партнерства, що посилить ефективність та оперативність реагування на деструктивні явища і дозволяють попередити негативні наслідки.

Висновки до розділу 3

1. Встановлено, що сучасна воєнно-політична ситуація у світі породжує додаткові бінарні ризики у сфері найважливіших безпекових пріоритетів держави. У цих умовах глобалізація світового безпекового простору інспірує необхідність ампліфікації державного та приватного сектору в напрямку посилення систем захисту критичної інфраструктури, що потребує результативного управління системними ризиками та посилення симбіозу міжнародних, національних та приватних інститутів, діючих з метою захисту критично важливих об'єктів. Обгрунтовано актуальність вивчення та аналізу передових підходів країн світу до конструювання та реалізації державної політики у сфері безпеки критичної інфраструктури.

2. Аналіз досвіду передових країн світу у напрямку збереження критичної інфраструктури, дозволив виявити певні спільні риси, які доцільно спроєктувати на удосконалення моделі вітчизняної державної політики у даному сегменті. У якості найбільш успішного було проаналізовано досвід США та країн ЄС у результаті чого, виявлено наявність розгалуженої мережі інститутів, відповідальних за безпеку та захист критичної інфраструктури. . Визначено, що важливу складову у світовому досвіді ефективної державної політики захисту критичної інфраструктури відіграють профільні інституції. Важливу роль у політиці захисту критичної інфраструктури у світі займає обмін інформацією з партнерами державного, так приватного секторів, що має важливе значення для безпеки та стійкості

3. Закордонний досвід також свідчить про важливу роль науково-дослідної та освітньої складової. На основі узагальнення кращих світових практик, систематизовано ряд кроків для формування концепції безпеки та

стійкості критичної інфраструктури, зокрема: встановити основні цілі та завдання концепції, на основі систематизації закордонного досвіду визначити елементи які можуть бути трансплантовані у інституційно-правову структуру державної політики України, закріпити перспективи адаптації визначених практик за конкретними секторами критичної інфраструктури, ідентифікувати перелік стейкхолдерів об'єктів критичної інфраструктури у відповідних секторах.

4. Досягнення стійкості об'єктами критичної інфраструктури детермінує здатність протидіяти, адаптуватися, регенерувати спроможність після потенційно руйнівної події та навчатися на основі аналізу допущених помилок. Така здатність дозволяє запобігати, протистояти, пом'якшувати, абсорбувати, пристосовуватися та відновлюватися після інциденту, який порушує або може порушити роботу критично важливого об'єкта. Кінцевим продуктом даного процесу вбачаються управлінські рішення на місцевому, регіональному і загальнодержавному рівнях, орієнтовані на реалізацію комплексу заходів із ідентифікації потенційних ризиків, інвестування в заходи зі зниження відомих ризиків, удосконалення організаційно-правових форматів управління ризиками, підвищення ефективності оперативного реагування на загрози та відновлення після надзвичайних ситуацій.

5. Основоположними напрямками інституційних перетворень у сфері державної політики захисту критичної інфраструктури вбачається розвиток її поліінституціональності, що передбачає залучення до її реалізації стейкхолдерів об'єктів критичної інфраструктури, без яких неможливо ефективне вирішення кризових ситуацій. Даний феномен пояснюється активною участю у формуванні й реалізації державної політики та безпекових заходів у сфері захисту критичної інфраструктури приватного сектору, власників і операторів об'єктів критичних об'єктів, державних урядових установ, місцевого самоврядування, неурядових організацій, секторальних агентств, та науково-дослідних установ і освітніх закладів. Цей процес дозволить посилити інноваційність 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.

6. У напрямку забезпечення захисту критичної інфраструктури з позиції сучасної міжнародної практики, доцільним вважається інтегрувати у сферу державної політики термін «резильєнтність критичної інфраструктури», що трактується як здатність об'єктів критичної інфраструктури протидіяти гібридним загрозам, за рахунок забезпечення посилення здатності країни, суспільства, органів державної влади та об'єктів критичної інфраструктури реалізувати 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. Базові складові резильєнтності включають «аналіз ризиків/загроз», «передбачення/підготовку», «проходження/витримку», «реагування/ відновлення» та «адаптацію/навчання». Зазначені атрибути резильєнтності імплікують інституційні трансформації систем захисту крізь призму ресурсних системних детермінант, серед яких визначено фізичний захист і оборону, кіберзахист і оборону, превентивні заходи захисту й оборони та освітньо-науковий підхід.

7. В межах інституційних перетворень у напрямку посилення резильєнтності критичної інфраструктури внесено пропозиції до посилення на державному рівні активності у забезпеченні здійснення регулярних міжсекторальних навчань із оперативно-тактичного реагування на кризові ситуації на об'єктах критичної інфраструктри з метою підвищення рівня міжвідомчої взаємодії. Підкреслено необхідність методологічної дифузії науково-освітнього забезпечення у сферу державної політики захисту критичної інфраструктри з метою досягнення її резильєнтності. Доведено, що серед фахових компетенцій, передбачених стандартами підготовки майбутніх фахівців у сфері державної політики немає жодної, яка б передбачала

підготовку до управління безпекою критичної інфраструктури. Пропонується внести зміни до чинного Класифікатора професій та Стандарту вищої освіти України спеціальності 281 Публічне управління та адміністрування в частині доповнення фахових компетентностей орієнтованих на управлінське забезпечення національної системи захисту об’єктів критичної інфраструктури.

8. Обґрунтовано пропозицію щодо інституційного закріплення механізму колективного підходу до захисту критичної інфраструктури. Запропоновано інноваційну ідею концепції кластерного підходу до забезпечення резильєнтності критичної інфраструктури в умовах воєнного стану в Україні на основі створення кластерів резильєнтності критичної інфраструктури (КРКІ). Головна ідея даного концепту передбачає створення навколо важливих інфраструктурних об’єктів унікальних інтеграційних об’єднань, спроможних забезпечити синергію безпекових заходів реалізованих в межах співпраці державних інститутів влади, систем захисту та реагування, самих інфраструктурних об’єктів та їх стейкхолдерів. Основними індикаторами зазначених структур визначено інноваційність, географічну близькість, автономність учасників та їх спільний інтерес.

ВИСНОВКИ

Дисертаційне дослідження орієнтоване на розв'язання важливої квестії щодо теоретичного узагальнення особливостей сучасної державної політики у сфері захисту критичної інфраструктури, обґрунтування доктринальних поглядів у фокусі на вдосконалення системи державного управління забезпеченням безпеки об'єктів критичної інфраструктури та генерування науково-практичних рекомендацій.

1. За результатами аналізу теоретичних підходів до сутності критичної інфраструктури як об'єкту державного управління запропоновано авторське бачення змістовного наповнення даної дефініції яким підкреслено множинність функціонально пов'язаних елементів національної інфраструктури у їх фізичній, організаційній інформаційно-комунікаційній структурі, що детермінує виконання державою своїх життєво важливих для суспільства функцій. Авторським формулюванням акцентовано увагу на значимості непорушності функціонування об'єктів критичної інфраструктури для здатності державної влади гарантувати національну безпеку й оборону та уникнути людських жертв, значних матеріальних та екологічних збитків, інших драматичних наслідків та підкреслено приналежність об'єктів критичної інфраструктури до сфери національної безпеки та акцентується пріоритетність відповідальності за її збереження саме за державою, що відповідає принципам системності, цілеспрямованості, множинності галузей та пріоритетної тріади людина-суспільство-держава у відповідності до антропоцентричного підходу та концепції сталого розвитку.

2. За результатами дослідження теоретико-методичних засад забезпечення захисту критичної інфраструктури ідентифіковано спектр загроз для критичної інфраструктури, серед яких військові загрози, диверсійні, терористичні, кіберзагрози, економічні загрози, сепаратизм, викрадення державної таємниці, природні та техногенні, колаборантні загрози. Поглиблений аналіз дозволив визначити, що предикат безпеки будується на основі трьох аспектів – концептуального, практичного та

ціннісного, що визначає ключові проблемні питання, серед яких потреба у формуванні комплексу організаційних, нормативно-правових, інженерно-технічних, експлуатаційних, наукових та державно-партнерських заходів забезпечення безпеки та стійкості критичної інфраструктури; урахування сучасних обставин військового стану в Україні при розробці державної стратегії захисту критичної інфраструктури; значний відсоток приватної власності у структурі об'єктів критичної інфраструктури; просторова розпорошеність об'єктів; тривала відсутність централізованої інформаційної платформи для накопичення інформації про об'єкти критичної інфраструктури; обширність суб'єктного складу та нескоординованість режимів функціонування, планів і процедур реагування на різні набори загроз і ризиків у сфері захисту критичної інфраструктури; тривала відсутність на загальнодержавному рівні затвердженого визначення її сутності, відповідної законодавчої бази та тектологічної системи захисту на об'єктах критичної інфраструктури, а також слабко відпрацьована практика інтерпретації механізму державно-приватного партнерства у сферу захисту критичної інфраструктури. Результатом аналізу понятійно-категорійного апарату є авторське формулювання дефініції «захист критичної інфраструктури», яке змінює кут уваги із процесу захисту критичної інфраструктури до процесів профілактики та превенції кризових ситуацій, диференціювавши відповідальність між державою, власниками, безпосередніми працівниками критичних об'єктів, а також їх стейкхолдерів.

3. Проаналізовано сучасні наукові парадигми формування державної політики у сфері захисту критичної інфраструктури, що дозволило визначити основні якості процесу формування державної політики у сфері захисту критичної інфраструктури, серед яких фундаментальність, багатоплановість, конкретність, здатність віддзеркалювати сутнісні характеристики відповідних об'єктів і процесів, системність, певний ступінь усталеності, суб'єктність, прийнятність, відтворюваність, дієвість, взаємозалежність із об'єктивною дійсністю та ступенем розвитку суспільства, орієнтація на

світоглядні підходи, спроможність удосконалення внаслідок суттєвих змін в науці. Науково обґрунтовано, що в основу інституційного цілепокладання заходів державної політики у сфері захисту критичної інфраструктури варто закласти парадигму національного безпекознавства, яка включає в себе аналіз політики, стратегії, загроз і відповідей національної безпеки країни. Ця парадигма досліджує такі питання, як внутрішня та зовнішня загрози, оборонна політика, розвідка, кібербезпека та інші аспекти, що впливають на безпеку країни, що нерозривно пов'язано із сектором критичної інфраструктури, що є детермінантою національної безпеки. До основних аспектів реалізації зазначеної парадигми пропонується включити ліквідацію протиріч у валідності тлумачень сфери критичної інфраструктури, симбіоз наукових знань у формотворчому вимірі міждисциплінарної наукової взаємодії, розгляд варіантів процесу формування державної політики захисту критичної інфраструктури поза формалізованими рамками, зокрема у інноваційних формах міжсекторальної взаємодії, комплексну модернізацію правового поля у напрямку ліквідації рудиментарних елементів та інспірації інноваційного забезпечення в процесі інтеграції та диференціації наук, а також як колективні форми роботи вчених різних галузей знання з дослідження процесу формування та реалізації державної політики захисту критичної інфраструктури, що дозволить генерувати множинність варіантів вирішення комплексу проблем, пов'язаних із безпекою критичної інфраструктури. У практичній адаптації зазначених імператив, ключовим визначено іррадацію суб'єктного складу захисту критичної інфраструктури за межі усталених державних інститутів на основі розвитку державно-приватного партнерств, моніторинг оперативної інформації стосовно загроз критичній інфраструктурі та розвиток міжнародного співробітництва.

4. Проведений логіко-семантичний аналіз стрижневих компонентів атрибутиву інституційно-правових аспектів державної політики дозволив виявити синергетичну дуальність її ключових тригерів – механізмів державного управління та механізмів правового регулювання.

Екстрапольовано трактування інституційно-правового регулювання реалізації державної політики у сфері захисту критичної інфраструктури як систему організаційно-управлінських і правових заходів, що реалізовують інститути державної влади, орієнтовані на запобігання диференційованим ризикам, загрозам і небезпекам об'єктам критичної інфраструктури основані на тріаді людина-суспільство-держава. Проведено скринінг нормативно-правової бази у сфері захисту критичної політики, що формує магістральну основу інституційно-правового механізму державної політики, що дозволило узагальнити спектр основоположних інститутів, які структурують архітектуру безпекової парадигми об'єктів критичної інфраструктури та ідентифіковано їх повноваження у даній сфері. За рахунок послідовного аналізу встановлено, що за період 2022-2023 року відбулась суттєва модернізація інституційно-правового забезпечення у сфері захисту критичної інфраструктури, яка визначає єдність адміністративних заходів державної влади, серед яких внесення відомостей про об'єкт критичної інфраструктури до Реєстру об'єктів критичної інфраструктури розроблення та погодження паспорта безпеки на об'єкт критичної інфраструктури, актів оцінки стану їх захищеності, результати моніторингу безпеки об'єктів, ідентифікація проектних загроз та ризиків. У практичній реалізації архітектури національної безпеки ідентифіковано комплекс автономних державних систем захисту критичної інфраструктури. Розкрито основні завдання державної політики захисту критичної інфраструктури, серед яких розвиток спроможностей суб'єктів забезпечення державної безпеки щодо превентивного комплексу заходів на об'єктах критичної інфраструктури, контррозвідувального режиму, інтенсифікація боротьби з тероризмом та організованою злочинністю, нарощування технологічних можливостей державної безпеки, прийняття на озброєння новітніх систем апаратних комплексів та спеціальних засобів, підвищення професійного рівня фахівців із забезпечення безпеки,

удосконалення нормативно-правового забезпечення, організаційних засад, упровадження дієвих механізмів взаємодії суб'єктів забезпечення державної безпеки із громадянським суспільством, подальший розвиток міжнародного співробітництва в безпековій сфері з питань захисту об'єктів критичної інфраструктури та запровадження національної системи стійкості.

5. Поведено оцінку інституційної спроможності національної системи захисту критичної інфраструктури, що дозволило встановити її рівень у розрізі спроможностей структурних, організаційних, технічних систем та окремих індивідів. До спектру спроможностей включено розвиток навичок і компетенцій на всіх рівнях провадження державної політики у сфері захисту критичної інфраструктури крізь діоптрій процесних інституцій – правил, процедур, засобів, інструментів, методів, організацій і ресурсів. Інституційна спроможність національної системи захисту критичної інфраструктури ідентифікована як комплементарність внутрішньої системи профільних інститутів та відповідних інституцій, що детермінує їх здатність синхронно забезпечувати захист об'єктів критичної інфраструктури з метою безперебійності їх функціонування. Виокремлено тріаду базових індикаторів інституційної спроможності: внутрішня синхронізація складових інституційної системи, зовнішня комплементарність складових інституційної системи, конгруентність внутрішніх та зовнішніх складових інституційної системи. Важливим кроком у досягненні інституційної спроможності національної системи захисту критичної інфраструктури визначено реалізацію стратегічного цільового пента-комплексу спроможності: правову регламентацію діяльності суб'єктів національної системи захисту критичної інфраструктури, створення системи координації та взаємодії суб'єктів національної системи захисту критичної інфраструктури, запровадження управління ризиками критичної інфраструктури, посилення стійкості національної системи захисту критичної інфраструктури, налагодження

міжнародної співпраці, а також еманацію архітектури практичної реалізації зазначених заходів. Проведений аналіз показників інституційної спроможності національної системи захисту критичної інфраструктури в Україні дозволив виявити ряд проблемних питань, зокрема: обмеженість наукових досліджень за участю органів публічного управління відповідальних за політику захисту критичної інфраструктури, відсутність у складі освітніх програм управлінських спеціальностей в закладах вищої освіти та спеціалізованих установах підвищення кваліфікації фахових компетентностей, орієнтованих на управління у сфері захисту об'єктів критичної інфраструктури, повільність інформаційного наповнення Реєстру об'єктів китичної інфраструктури та невиконання секторальними органами у сфері захисту критичної інфраструктури завдань з їх ідентифікації та категоризації об'єктів, відсутність компетентного наглядового органу за результативністю державної політики у сфері захисту критичної інфраструктури, не розроблено План врегулювання кризових ситуацій на випадок масштабних кіберінцидентів та аварій на об'єктах критичної інфраструктури, не врегульовано законодавством порядок залучення волонтерів у сферу кібербезпеки та захисту критичної інфраструктури, Збройні Сили України не мають у своєму складі підрозділів кібервійськ та не проводять навчання з кібероперацій або кіберзахисту, не сформовано перелік об'єктів критичної інформаційної інфраструктури, не розроблено дієву модель міжсекторальної співпраці у сфері захисту критичної інфраструктури та залучення стейкхолдерів.

6. Проаналізовано дієвість сучасної парадигми державної політики у сфері захисту критичної інфраструктури в умовах воєнного стану, що дало підстави констатувати, що архітектура державної політики у сфері захисту критичної інфраструктури розвивається в умовах масштабних змін геополітичних інтересів у сфері перерозподілу територій та світових ресурсів, детермінуючи боротьбу за центри впливу на найбільш важливі об'єкти критичної інфраструктури. Встановлено, що підходи до вироблення

адміністративно-правових основ сучасної політики у сфері захисту критичної інфраструктури реалізується в умовах воєнного стану та безперервної російської військової агресії. Подано дані систематичного порушення ворогом міжнародних нормативно-правових актів, у тому числі й у сфері захисту критичної інфраструктури, її дестабілізація у вигляді бойових ударів по атомних електростанціях, електропідстанціях, об'єктах гідроенергетики, теплової генерації, паливо проводах та ін.. Констатовано, що такі дії призводять до розширення загроз за межі локальної безпекової політики. Проаналізовано ретроспективи формування сучасної парадигми державної політики у сфері захисту критичної інфраструктури та визначено ряд стратегічних прорахунків, які були допущені у безпековій політиці незалежної України, серед яких прийняття без'ядерного статусу, позиції нейтралітету та позаблокового статусу, прихована демілітаризація та штучна деградація обороноздатності суб'єктів системи забезпечення національної безпеки та захисту критичної інфраструктури, трансформація корупції у системоутворюючий чинник державної влади, добровільне підписання умов перебування воєнної бази Чорноморського флоту Російської Федерації на території України.

Аналіз сучасних аспектів парадигми державної політики у сфері захисту критичної інфраструктури в умовах правого режиму воєнного стану в Україні, дозволив виявити, що архітектура безпеки критичної інфраструктури побудована на основі чіткої ідентифікації секторів та формуванні реєстру об'єктів критичної інфраструктури, ідентифікації актуальних загроз, формування суб'єктного складу, удосконаленні інституційного забезпечення державної політики у цій сфері, створенні системи захисту об'єктів критичної інфраструктури, вжитті комплексних заходів із подолання наслідків пошкодження та руйнації критичних об'єктів. Обгрунтовано, що сучасна полідика у сфері захисту критичної інфраструктури має включати сектор превентивного та антикризового управління загрозами та ризиками, який відповідатиме пріоритезації

предикату стійкості відносно захисту, що пропагує сучасна парадигма безпекознавства у країна ЄС. Узагальнено методичний підхід до розробки концептуальних засад захисту критичної інфраструктури на основі забезпечення стійкості у штатному режимі, режимі готовності та запобігання, режимі реагування та режимі відновлення. Структуровано формат інтегрованої безпекової моделі критичної інфраструктури, що передбачає формувати безпеково-ситуаційні моделі у якості фідбеку до моделі проєктних загроз, перелік яких доповнено «колаборaційними загрозами», які трактовано як небезпеки, що походять від громадян держави, які співпрацюють із ворогом з метою забезпечення реалізації його інтересів та заподіяння шкоди.

7. Аналіз особливостей іноземної практики реалізації ефективної державної політики у сфері захисту критичної інфраструктури дав підстави зробити висновок, що Україна запозичила досвід американської моделі, опираючись також на досвід ЄС. Також виділено ряд особливостей у іноземній практиці: розвиток освіти та науки у напрямку підготовки спеціалістів у сфері захисту критичної інфраструктури; інформаційний реверс між стейкхолдерами безпеки та стійкості об’єктів критичної інфраструктури, у напрямку акумуляції дієвого досвіду протидії загрозам та ризикам, створення та підтримки зручних систем комунікації; ідентифікація стейкхолдерів захисту об’єктів критичної інфраструктури у сфері приватного бізнесу та розвиток відносин на основі державно-приватного партнерства та кластеризації; політика у сфері захисту критичної інфраструктури більшості країн орієнтована на розвиток потенціалу інвестиційної активності; розробка активних державних стратегії управління ризиками для критичної інфраструктури, що передбачає домінування превентивного захисту. Встановлено, що сучасна українська парадигма державної політики у сфері захисту критичної інфраструктури розвивається крізь призму положень нової Директиви ЄС 2557 сфокусованої на забезпеченні стійкості, а не захисту об’єктів критичної інфраструктури, що пояснюється неможливістю

досягнути бездоганної захищеності інфраструктури в умовах активної фази війни, а необхідністю швидкої регенерації втрачених потужностей у разі надзвичайної деструктивної ситуації. Стійкість трактується як тристадійний процес антикризового управління, орієнтований на превентивність дій із забезпечення тріади варіантив стійкості: соціальної, організаційної та технологічної. Зазначені складові формують «трикутник стійкості», що є базовим індикатором для оцінки ефективності державної політики захисту критичної інфраструктури. На основі результатів оціночного огляду закордонного досвіду у сфері державної політики, узагальнено концептуальні положення вектору посилення стійкості критичної інфраструктури на загальнодержавному і регіональному рівнях за рахунок удосконалення політичної та інституційно-правової бази, розвиток кадрового потенціалу, перегляду секторів критичної інфраструктури, інтегрованої оцінки ризиків та загроз, моделювання, оперативного планування та розробки сценаріїв дій, посилення ресурсного забезпечення, забезпечення міжсекторальної координації та співпраці, а також створення партнерств зі стейкхолдерами.

8. Запропоновано напрями інституційних перетворень у векторі підвищення ефективності державної політики захисту критичної інфраструктури, основоположними із яких вбачається розвиток її поліінституціональності, що передбачає залучення стейкхолдерів об’єктів критичної інфраструктури, без яких неможливо ефективне вирішення кризових ситуацій. Даний феномен передбачає активну участь у формуванні й реалізації державної політики та безпекових заходів у сфері захисту критичної інфраструктури приватного сектору, власників і операторів об’єктів критичних об’єктів, державних урядових установ, місцевого самоврядування, неурядових організацій, секторальних агентств, та науково-дослідних установ і освітніх закладів.

У напрямку забезпечення захисту критичної інфраструктури з позиції сучасної міжнародної практики, пропонується у якості розширеної альтернативи предикату «стійкість критичної інфраструктури» інтегрувати у

сферу державної політики термін «резильєнтність критичної інфраструктури», що трактується як здатність об'єктів критичної інфраструктури протидіяти гібридним загрозам, за рахунок забезпечення посилення здатності країни, суспільства, органів державної влади та об'єктів критичної інфраструктури реалізувати 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. Базові атрибути резильєнтності включають «аналіз ризиків/загроз», «передбачення/підготовку», «проходження/витримку», «реагування/ відновлення» та «адаптацію/навчання» та імплікують інституційні трансформації систем захисту крізь призму ресурсних системних детермінант, серед яких визначено фізичний захист і оборону, кіберзахист і оборону, превентивні заходи захисту й оборони та освітньо-науковий підхід. Із цією метою запропоновано внести зміни до чинного Класифікатора професій та Стандарту вищої освіти України спеціальності 281 Публічне управління та адміністрування в частині доповнення фахових компетентностей орієнтованих на управлінське забезпечення національної системи захисту об'єктів критичної інфраструктури, що дозволить посилити інституційну спроможність у цій сфері.

9. Подано авторські концептуальні пропозиції, що передбачають наочну репрезентацію удосконалення державних механізмів реалізації політики захисту критичної інфраструктури України в умовах воєнного стану, шляхом інституційного закріплення механізму колективного підходу. Запропоновано інноваційну ідею концепції кластерного підходу до забезпечення резильєнтності критичної інфраструктури в умовах воєнного стану в Україні на основі створення «кластерів резильєнтності критичної інфраструктури», що має на меті створення навколо важливих інфраструктурних об'єктів унікальних інтеграційних об'єднань, спроможних

забезпечити синергію безпекових заходів реалізованих в межах співпраці державних інститутів влади, систем захисту та реагування, самих інфраструктурних об'єктів та їх стейкхолдерів. Основними індикаторами зазначених структур визначено інноваційність, географічну близькість, автономність учасників та їх спільний інтерес. Інфраструктурні об'єкти в даному проєкті позиціонуються як тригери формування конкурентних переваг учасників кластера, що імплікує їм статус «стейкхолдерів». Для створення умов комплексної реалізації моделі кластерного підходу запропоновано інтегрувати у сферу державної політики термін «публічно-приватне партнерство», як систему законодавчо врегульованих і юридично оформлених відносин між органами державної влади, органами місцевого самоврядування, приватним бізнесом (юридичними та фізичними особами), громадськими організаціями для вирішення суспільно значущих проблем на довготривалий період часу, заснованих на узгодженні інтересів і взаємній зацікавленості в досягненні намічених цілей, на довірі і таких, що передбачають добровільне об'єднання ресурсів, спільне ухвалення рішень, раціональний розподіл ризиків і спільну відповідальність за результати на основі договору про спільну діяльність. Розпочати апробацію зазначених ініціатив вбачається доцільним на територіях повоєнного відновлення. Вимірність резильєнтності об'єктів критичної інфраструктури проілюстровано у вигляді «трикутника вразливості» об'єкта критичної інфраструктури, що ілюструє обсяг втрати продуктивності та час необхідний на його відновлення, що залежить від превентивних заходів проведених на об'єкті. Таким чином, чим менша площа даного трикутника, тим резильєнтнішою є інфраструктура. Складові описаного «трикутника вразливості» можуть бути компенсовані тріадою відповідних детермінант резильєнтності – протидія (превентивний захист), адаптація та відновлення. На основі запропонованої гіпотези, з метою можливості оцінки досягнутої резильєнтності критичної інфраструктури в межах кластерної моделі.

Список використаної літератури

1. Азаров С. І., Сидоренко В.Л., Єременко С.А., Пруський А.В., Демків А.М Захист критичної інфраструктури в умовах надзвичайних ситуацій: монографія. за заг. ред. П.Б. Волянського. Київ, 2021. 375 с.

2. Антикризовий механізм сталого розвитку підприємства / за ред. проф. Перерви П. Г., проф. Товажнянського Л. Л.: монографія. Харків, 2012. 705 с.

3. Бараннік В. О. Щодо сприяння розвитку регіональних кластерів в Україні. Національний інститут стратегічних досліджень. 2021. URL: https://niss.gov.ua/sites/default/files/2021-08/klustery.pdf

4. Бевз С. І. Поняття та елементи механізму адміністративно-правового регулювання державного управління господарською діяльністю. Прикарпатський юридичний вісник. Вип. 4(25). Т. 2, 2018. С. 43-47.

5. Бєлай С. В., Євтушенко І. В., Мацюк В. В. Теоретико-методологічні засади підготовки кадрів у сфері захисту критичної інфраструктури України. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2021. Вип. 2. С. 342-350.

6. Бєлоусов А. В. Наукові підходи до визначення ризику надзвичайних ситуацій як об'єкту управління. Наукові розвідки з державного та муніципального управління. 2015. №1. С. 224-235.

7. Бжезінський З. К. Україна та Європа. Національна безпека і оборона. 2000. № 7. С. 11-15.

8. Бірюков Д. С. Захист критичної інфраструктури в Україні: від наукового осмислення до розробки засад політики. Науково-інформаційний вісник Академії національної безпеки. 2015. № 3-4. С. 155-170.

9. Бірюков Д.С., Кондратов С.І. Стратегія захисту критичної інфраструктури в системі національної безпеки держави. Стратегічні пріоритети. 2012. № 3(24). С. 107–113.

10. Бірюков Д.С., Кондратов С.І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. К.: НІСД, 2012. 96 с.

11. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній

інфраструктурі. Стратегічні пріоритети. Серія: Економіка. 2015. № 4. С. 83-93.

12. Бобро Д. Г. Удосконалення методології ранжування об’єктів критичної інфраструктури та їх віднесення до критичної інфраструктури: аналіт. зап. URL: http://www.niss.gov.ua/content/articles/files/krutuchna_infra-a7636.pdf.

13. Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М. Організаційні та правові аспекти забезпечення безпеки і стій кості критичної інфраструктури України: аналіт. доп. за заг. ред. О. М. Суходолі. К.: НІСД, 2019. 224 с.

14. Бобро Д. Г. Проектна загроза та паспорти безпеки як ключові елементи системи захисту критичної інфраструктури. URL: https://niss.gov.ua/sites/default/files/2018-07/Presentation_Bobro.pdf.

15. Богуцький П. П. Концептуальні засади права національної безпеки України: монографія. Київ – Одеса: Фенікс, 2020. 376 с.

16. Богуцький П. П. Військово-правова парадигма взаємодії громадянського суспільства та сектору безпеки і оборони. Взаємодія громадянського суспільства з сектором безпеки і оборони: сучасні виклики : тези доп. учасників наук.-практ. конф. (Харків, 21 груд. 2021 р.), С. 9-12.

17. Валіхновський Р. Підходи щодо побудови гуманітарної парадигми забезпечення національної безпеки. Вісник Національної академії державного управління при Президентові України. 2010. № 1. С. 243-253.

18. Велика українська енциклопедія. Державна наукова установа «Енциклопедичне видавництво». URL: https://vue.gov.ua/.

19. Великий енциклопедичний юридичний словник. За ред. акад. НАН України Ю.С. Шемшученка. 2-е вид., переробл. і доповн. К.: Вид-во «Юридична думка», 2012. 1020 с.

20. Великий тлумачний словник сучасної української мови . Укл. і гол. ред. В.Т. Бусел. К.: Ірпінь: ВТФ «Перун», 2005. 1728 с.

21. Верголяс О. О. Реформування системи захисту та підвищення стійкості критичної інфраструктури України в розрізі актуальних загроз.

URL: https://coolyanews.info.html.

22. Вітлінський В. В., Великоіваненко Г. І. Ризикологія в економіці та підприємництві: монографія. К.: КНЕУ, 2004. 480 с.

23. Войтовський К. Щодо розроблення планів забезпечення організаційної стійкості. Національний інститут стратегічних досліджень. URL: https://niss.gov.ua/sites/default/files/2023-02/az_planuvannya-org-stiykosti_24022023.pdf.

24. Герасименко П. В. Небезпечний нейтралітет. URL: https://zaxid.net/nebezpechniy_neytralitet_n1541767.

25. Гладиш М. Еволюція безпекової парадигми скандинавських держав протягом XX століття. Вісник Львівського університету. Серія: Міжнародні відносини. 2019. Вип. 46. С. 27-36.

26. Гладка О. В. Передумови реалізації адміністративноправової доктрини людино центризму. Адміністративне та інформаційне право. 2017. № 1(3). С.64-73.

27. Гнатюк С. О., Рябий М. О., Лядовська В. М. Визначення критичної інформаційної інфраструктури та її захисту: аналіз підходів. Зв'язок. 2014. № 4. С. 3-7.

28. Гнатюк С. О., Сєйлова Н. А., Сидоренко В. М. Універсальна модель даних для формування переліку об'єктів критичної інформаційної інфраструктури держави. Ukrainian Scientific Journal of Information Security, 2017. vol. 23. issue 2. P. 80–91.

29. Гольцов А .Г. Геостратегія України щодо Російської Федерації. Вісник НТУУ «КПІ». Політологія. Соціологія. Право: збірник наукових праць. 2023. № 1 (57). С. 71-77.

30. Гончар М. Ф. Системи стрес-менеджменту на підприємствах: формування, використання та моделювання: монографія. Львів: Видавництво Львівської політехніки, 2018. 272 с.

31. Гордина В. В. Некоторые аспекты формирования системы риск-контроллинга на предприятии. Финансы и кредит. 2012. № 28. С. 30-36.

32. Декларація про державний суверенітет України. Документ № 55-XII

від 16.07.1990 р. URL: https://zakon.rada.gov.ua/laws/show/55-12#Text.

33. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. за ред. О. М. Суходолі. Київ: НІСД, 2020. 28 с .

34. Дєєва Н. Е., Хмурова В. В. Публічно-приватне партнерство: інтереси зацікавлених сторін. Економіка України. 2018. № 9(682). С. 99-111.

35. Директива Європейського Парламенту і Ради (ЄС) «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» № 2016/1148 від 06.07.2016 р. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text.

36. Директива Ради ЄС «Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту» № 2008/114/ЄС від 08.12.2008 р. URL: https://zakon.rada.gov.ua/laws/show/984_002-08#Text.

37. Дмитренко О. А. Інституційна спроможність неурядових організацій в Україні: фінансовий аспект. Науковий часопис НПУ ім. М. П. Драгоманова. 2020. Вип. 28. С. 48-55.

38. Дмитренко О. А. Інституційна спроможність неурядового сектору в Україні: дис. … докт. філософії: 052. Ін-т політ. І етнонаціональних досліджень ім. І. Ф. Кураса НАН України. Київ, 2022. 208 с.

39. Додатковий протокол до Женевських конвенцій від 12.08.1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 08.06.1977 р. URL: https://zakon.rada.gov.ua/laws/show/995_199#Text.

40. Домарацький М. Б. Забезпечення безпеки та підвищення ефективності захисту критично важливих об’єктів на державному рівні. Публічне управління і адміністрування в Україні. 2019. Вип. 14. С. 82-85.

41. Домбровська С. М. Механізми забезпечення державної соціальної безпеки в Україні. Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія». Серія: Державне управління. 2015. Т. 254, Вип. 242. С. 28-32.

42. Донець Л.І. Економічні ризики та методи їх вимірювання: Навч.

посіб. К.: Центр навч. літ., 2006. 312 с.

43. Дранишников Л. В., Сугаль Є. О. Оцінка зовнішнього ризику за допомогою нечіткої логіки. Математичне моделювання. 2017. № 2. С. 63-66.

44. Енциклопедія державного управління: у 8 томах. Нац. акад. держ. упр. при Президентові України. Київ: НАДУ, 2011. Т. 2. С. 13-17.

45. Євсєєв В. О. Можливі шляхи удосконалення захисту критичної інфраструктури України з урахуванням світового досвіду. Збірник наукових праць ХНУПС. 2016. № 4. С. 168-172.

46. Єрменчук О. П. Нормативно-правове регулювання діяльності у сфері захисту національної критичної інфраструктури: аналіз та узагальнення нормотворчої практики США. Науковий вісник ДДУВС. 2017. № 3. С. 135-140.

47. Єрменчук О. П. Складові національної інфраструктури. Науковий вісник ДДУВС. 2017. № 4. С. 109-115.

48. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монограф. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

49. Заболотний А.В. Юник І.Г. Організаційно-правові аспекти проходження публічної служби та виконання посадових обов’язків на об’єктах критичної інфраструктури в умовах правового режиму воєнного стану в Україні. Інвестиції, практика та досвід. №8. 2024. URL: https://www.nayka.com.ua/index.php/investplan/article/view/3602/3637.

50. Закон України No2980-IX від 20.03.2023 р. «Про одноразову грошову допомогу за шкоду життю та здоров'ю, завдану працівникам об'єктів критичної інфраструктури, державним службовцям, посадовим особам місцевого самоврядування внаслідок військової агресії Російської Федерації проти України». URL: https://zakon.rada.gov.ua/laws/show/2980-20/ed20230-320#Text.

51. Закон України «Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України» № 2684-IX від 18.10.2022 р. URL:

https://zakon.rada.gov.ua/laws/show/2684-20#Text.

52. Закон України «Про боротьбу з тероризмом» №638-IV від 20.03.2003 р. URL: https://zakon.rada.gov.ua/laws/show/638-15/ed20030320#Text.

53. Закон України «Про військово-цивільні адміністрації» № 141-VIII від 03.02.2015 р. URL: https://zakon.rada.gov.ua/laws/show/141-19#Text.

54. Закон України «Про внесення змін до деяких законодавчих актів України щодо засад державної регіональної політики та політики відновлення регіонів і територій» №2389-IX від 09.07.2022 р. URL: https://zakon.rada.gov.ua/laws/show/2389-20#Text.

55. Закон України «Про державно-приватне партнерство». № 2404-VI від 01.07.2010 р. URL: https://zakon.rada.gov.ua/laws/show/2404-17/ed20230903.

56. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» № 3475-IV від 31.03.2023 р. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text.

57. Закон України «Про Державну службу» № 889-VIII від 10.12.2015 р. URL: https://zakon.rada.gov.ua/laws/show/889-19#Text.

58. Закон України «Про засади внутрішньої і зовнішньої політики» № 2411-VI від 01.07.2010 р. URL: https://zakon.rada.gov.ua/laws/show/2411-17#Text.

59. Закон України «Про Кабінет Міністрів України» № 794-VII від 03.08.2023 р. URL: https://zakon.rada.gov.ua/laws/show/794-18#Text.

60. Закон України «Про критичну інфраструктуру» № 1882-IX від 05.12.2022 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.

61. Закон України «Про місцеве самоврядування в Україні» № 280/97-ВР від 21.05.1997 р. URL: http://zakon4.rada.gov.ua/laws/show/280/97-вр/page#Text.

62. Закон України «Про національну безпеку України» № 2469-VIII від 31.03.2023 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

63. Закон України «Про Національну систему конфіденційного зв'язку» від 10.01.2002 № 2919-III. URL: https://zakon.rada.gov.ua/laws/show/2919-14/ed20220101#Text.

64. Закон України «Про об’єкти підвищеної небезпеки» від 18.01.2001 №2245-III. URL: https://zakon.rada.gov.ua/laws/show/2245-14#Text.

65. Закон України «Про органи самоорганізації населення» http://zakon4.rada.gov.ua/laws/show/2625-14 .

66. Закон України «Про основи національного спротиву» № 1702-IX від 03.08.2023 р. URL: https://zakon.rada.gov.ua/laws/show/1702-20#Text.

67. Закон України «Про основи національної безпеки України» від 19.06.2003 № 964-IV. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text (втратив чинність на підставі Закону № 2469-VIII від 21.06.2018).

68. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19/ed20220817#Text.

69. Закон України «Про охорону культурної спадщини» від 08.06.2000 № 1805-III. URL: https://zakon.rada.gov.ua/laws/show/1805-14#Text.

70. Закон України «Про платіжні системи та переказ коштів в Україні» від 05.04.2001 № 2346-III. URL: https://zakon.rada.gov.ua/laws/show/2346-14#Text.

71. Закон України «Про правовий режим воєнного стану» № 389-VIII від 19.10.2023 р. https://zakon.rada.gov.ua/laws/show/389-19#Text.

72. Закон України «Про Раду національної безпеки і оборони України» № 183/98-ВР від 29.07.2023 р. URL: https://zakon.rada.gov.ua/laws/show/183/98 вр#Text.

73. Закон України «Про систему екстреної допомоги населенню за єдиним телефонним номером 112» від 13.03.2012 № 4499-VI. URL: https://zakon.rada.gov.ua/laws/show/4499-17#Text.

74. Закон України «Про стимулювання розвитку регіонів» № 2850-IV від від 08.09.2005 р. URL: https://zakon.rada.gov.ua/laws/show/2850-15#Text.

75. Закон України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» № 2064-III від 16.10.2022 р. URL: https://zakon.rada.gov.ua/laws/show/2064-14#Text.

76. Залознова Ю. С., Бутенко Н. В., Петрова І. П. Публічно-приватне партнерство в Україні: стан, проблеми та перспективи розвитку. Економічний вісник Донбасу. 2016. № 2. С. 21-28.

77. Звіт про виконання у 2019 році Стратегії реформування державного управління України. URL: https://www.kmu.gov.ua/storage/app/sites/1/zviti-pro-vikonannya/par-report-ukr-web.pdf.

78. Звіт про відстеження результативності постанови КМУ «Деякі питання об'єктів критичної інфраструктури» № 1109 від 09.10.2020 р. за підсумками 2022 р. URL: https://cip.gov.ua/ua/news/zvit-pro-povtorne-vidstezhennya-rezultativnosti-postanovi-kabinetu-ministriv-ukrayini-vid-09-zhovtnya-2020-r-1109-deyaki-pitannya-ob-yektiv-kritichnoyi-infrastrukturi.

79. Зелена книга з питань захисту критичної інфраструктури в Україні: зб. матеріалів міжнар. експерт. нарад. Упоряд. Д.С. Бірюков, С.І Кондратов ; за заг. ред. О.М.Суходолі. К.: НІСД, 2016. 176 с.

80. Зубко Г. Ю. Система суб'єктів реалізації державної інфраструктурної політики України. Правові новели. 2020. № 11. С. 166-178.

81. Зубко Г. Ю. Шостий технологічний уклад: інфраструктурно-правовий аспект. Підприємництво, господарство і право. 2019. № 11. С. 218-229.

82. Зубко Г. Ю. Адміністративно-правові засади формування переліку об'єктів критичної інфраструктури. Держава та регіони. Серія «Право». 2020. № 3(69). Т. 2. С. 36-42.

83. Зубко Г. Ю. Державна інфраструктурна політика України: адміністративно-правові засади регулювання: монографія. Херсон: Видавничий дім «Гельветика», 2020. 412 с.

84. Зубко Г. Ю. Публічно-приватне партнерство у сфері безпеки стратегічної інфраструктури України. Юридичний науковий електронний журнал. 2020. № 2. Т. 2. С. 13-17.

85. Зубко Г. Ю. Система суб'єктів реалізації державної інфраструктурної політики України. Правові новели. 2020. № 11. С. 166-178.

86. Зубко Г. Ю. Сучасні підходи до визначення поняття державної

інфраструктурної політики. Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція». 2020. № 48. С. 78-84.

87. Інституціоналізація публічного управління в Україні: наук.-аналіт. доп. за заг. ред. М. М. Білинської, О. М. Петроє. Київ: НАДУ, 2019. 210 с.

88. Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT). Київ: Мінекономрозвитку України, 2015. 74 с.

89. Клебанова Т. С., Коваленко К. С. Моделі оцінки кризовості коксохімічних підприємств на основі превентивного підходу. Нейро-нечіткі технології моделювання в економіці. 2015. № 4. С. 80-112.

90. Кодекс цивільного захисту України. від 03.04.2022 № 5403-VI. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text.

91. Кодекс цивільного захисту України: Закон України № 5403-VI від 05.10.2023 р. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text.

92. Козловський С. В. Управління сучасними економічними системами, їх розвитком та стійкістю: монографія. В.: Меркьюрі-Поділля, 2010. 432 с.

93. Колпаков В. К., Кузьменко О. В. Нелегальна міграція: генезис і механізм протидії: монографія. Д: «Наука і освіта», 2002. 371 с.

94. Кондратенко О. Ю. Геоекономічний вимір гібридної війни Російської Федерації проти України. Вісник Київського національного університету імені Тараса Шевченка. Міжнародні відносини. № 2(50). 2019. С.12-19.

95. Кондратов С. І., Суходоля О. М. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. за ред. Суходолі. Київ: НІСД, 2020. 28 с.

96. Конституція України: Закон України № 254к/96-ВР від 01.01.2020 р. URL: https://zakon.rada.gov.ua/laws/show/ 254к/96-вр#Text.

97. Королюк Н. О., Першин О. В., Грідньова Т. О., Шевченко С. О. Обґрунтування сучасного підходу щодо автоматизації процесів прийняття рішень по управлінню авіацією. Збірник наукових праць Харківського національного університету Повітряних Сил. 2019. №1(59). С. 32-39.

98. Кочетков О. В., Гаур Т. О., Машін В. М. Система оцінки ризиків

інформаційної безпеки підприємства на основі нечіткої логіки. Наукові праці ОНАЗ ім. О. С. Попова. 2019. № 1. С. 97-104.

99. Кримінальний кодекс України: Закон України № 341-III від 05.10.2023 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

100. Криштанович М. Ф., Пушак Я. Я., Флейчук М. І., Франчук В. І. Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення: монографія. Львів: Сполом, 2020. 418 с.

101. Крук С. І. Аналіз стану організаційно-правових механізмів державного управління у сфері забезпечення національної безпеки України. Інвестиції: практика та досвід. 2018. № 20. С. 76-78.

102. Крук С. І. Інституційний і правовий механізми державного управління у сфері забезпечення національної безпеки України. Публічне управління та митне адміністрування. 2018. № 2 (19). С.70-73.

103. Кузмін О. Є., Мельник О. Г., Адамів М. Є. Антисипативне управління підприємствами: процесно-структурований підхід. Економіка: реалії часу. 2012. № 2 (3). С. 71-77.

104. Культура безпеки. Серія видань по безпеці. № 75-INSAG-4. Доповідь Міжнародної консультативної групи з ядерної безпеки. Вена: МАГАТЕ, 1991. URL: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub882r_web.pdf.

105. Кульчій І. М. Публічно-приватне партнерство як спосіб забезпечення сталого розвитку сільських територій. Проблеми законності: зб. наук. пр. 2017. Вип. 138. С. 99-108.

106. Лазор О.Я., Заболотний А.В., Зубар І.В. Роль критичної інфраструктури у забезпеченні державної політики продовольчої безпеки в Україні. Актуальні питання у сучасній науці. №4 (20). 393-409.

107. Лазор О.Я., Юник І.Г. Перспективи розвитку державно-приватного партнерства у сфері захисту критичної інфраструктури в Україні. Наукові перспективи. №4. 2024. С.246-258.

108. Лазор О.Я., Юник І.Г., Заболотний А.В. Державна стратегія повоєнного відновлення та розвитку критичної інфраструктури в Україні.

Державне управління: удосконалення та розвиток. №4. 2024. URL: https://doi.org/10.32702/2307-2156.2024.4.2.

109. Лазор О. Я., Лазор О. Д. Публічне управління та адміністрування: ретроспектива деяких теоретичних аспектів. Університетські наукові записки. 2015. № 4. С. 111-121.

110. Ліпкан В. А. Теорія національної безпеки. 2009. Київ: КНТ. 576 с.

111. Ліпкан В. А. Безпекознавство: Навчальний посібник. К.: Вид-во Європейського університету, 2003. 208 с.

112. Ліпкан В. А., Зубко Г. Ю. Інфраструктурні стратегії: формування нового концепту. Юридичний бюлетень. 2020. № 17. С. 13-20.

113. Ліпкан В. А. Геостратегія сучасної української держави: засади формування Вісник Львівського університету. Серія філос.-політолог. студії. 2022. Вип. 42, с. 268-277.

114. Лойко В. В., Храпкіна В. В., Маляр С. А., Руденко М. В. Economic and legal principles of ensuring the protection of critical infrastructure. Фінансово-кредитна діяльність: проблеми теорії та практики. 2020. № 4 (35). С. 427-438.

115. Матвійчук А. В. Моделювання економічних процесів із застосуванням методів нечіткої логіки: монографія. К.: КНЕУ, 2007. 264 с.

116. Мельник Р. С. Концепція людиноцентризму у сучасній доктрині адміністративного права. Юридичний журнал «Право України». 2015. №10. 157-165.

117. Меморандум про гарантії безпеки у зв'язку з приєднанням України до Договору про нерозповсюдження ядерної зброї. Закон України №998 від 05.12.1994 р. URL: https://zakon.rada.gov.ua/laws/show/998_158#Text

118. Мусієнко В. О., Зінченко М. Е. Технологія ризик-менеджменту як елемент системи забезпечення економічної безпеки суб'єкта господарювання. Економічний вісник Дніпровської політехніки. 2020. № 3. С. 98-108.

119. Мушникова С. А. Побудова поліпарадигмальної моделі ієрархії стратегій управління безпекою розвитку підприємства. Проблеми системного

підходу в економіці. 2020. Вип. 1 (75). Ч. 1. С. 130–136.

120. Мушникова С. А. Трансдисциплінарна парадигма й інноваційні трансформації економічного середовища як фундаментальна основа управління безпекою розвитку металургійних підприємств. Бізнес Інформ. 2020. № 4. С. 446-452.

121. Надолішній П. І., Піроженко Н. В. Публічно-приватне партнерство в Україні: теоретикометодологічні засади і умови інституціалізації. Теоретичні та прикладні питання державотворення: зб. наук. пр. 2012. Вип. 10. С. 1 7-52.

122. Назаров М. С. Соціальна стійкість на рівні територіальних громад в умовах сучасних викликів. Науковий журнал «Політикус». №2. 2022. С.54-59

123. Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України «Про затвердження Змін до Положення про територіальний орган Адміністрації Державної служби спеціального зв'язку та захисту інформації України» № 467 від 31.05.2023 р. URL: https://zakon.rada.gov.ua/laws/show/z1124-23#Text

124. Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України «Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури» № 23 від 15.01.2021 р. URL: https://zakon.rada.gov.ua/rada/show/v0023519-21#Text

125. Наказ Адміністрації Держспецзв'язку «Про затвердження Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» № 94 від 10.01.2023 р. URL: https://zakon.rada.gov.ua/laws/show/z0603-08#Text

126. Наказ Адміністрації Держспецзв'язку «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-

комунікаційних системах» № 660 від 10.01.2023 р. URL: https://zakon.rada.gov.ua/laws/show/z0090-15#Text.

127. Наказ Адміністрації Держспецзв'язку «Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті» № 20 від 15.01.2016 р. URL: https://zakon.rada.gov.ua/laws/show/z0196-16#Text.

128. Наказ Міністерства енергетики України «Про Вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури» № 417 від 15.12.2022 р. URL: https://zakon.rada.gov.ua/laws/show/z0249-23#Text.

129. Наказ МОН України «Про затвердження Стандарту вищої освіти України другого (магістерського) рівня вищої освіти ступеня «магістр» за спеціальністю 281 Публічне управління та адміністрування» № 1001 від 04.08.2020 р. URL: https://mon.gov.ua/ua/npa/pro-zatverdzhennya-standartu-vishoyi-osviti-za-specialnistyu-281-publichne-upravlinnya-ta-administruvannya-dlya-drugogo-magisterskogo-rivnya-vishoyi-osviti.

130. Наказ МОН України «Про затвердження Стандарту вищої освіти України першого (бакалаврського) рівня вищої освіти ступеня «бакалавр» за спеціальністю 281 Публічне управління та адміністрування» № 1172 від 29.10.2018 р. URL: https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/12/21/281-Publ.upr.ta.administruvannya-bakalavr.21.01.22.pdf.

131. Національна парадигма сталого розвитку України. за заг. ред. академіка НАН України, д.т.н., проф., засл. діяча науки і техніки України Б. Є. Патона. К.: Державна установа "Інститут економіки природокористування та сталого розвитку Національної академії наук України", 2012. 72 с.

132. Національний класифікатор України. Класифікатор професій ДК 003:2010. URL: https://zakon.rada.gov.ua/rada/show/va327609-10#Text.

133. Наше спільне майбутнє: Доповідь Міжнародної комісії з навколишнього середовища та розвитку. URL: http://www.un.org/ru/ga/pdf/brundtland.pdf.

134. Нестерова М. А. Трансдисциплінарність когнітивістики. Нова парадигма. 2014. № 123. С. 42-49.

135. Нестор О. Ю. Публічно-приватне партнерство: сутність, особливості та проблеми розвитку на тлі пандемії COVID-19. Соціально-економічні проблеми сучасного періоду України: зб. наук. пр. 2021. Вип. 2(148). С. 58-68.

136. Ніколаюк С. І., Радченко Р. А. Використання можливостей нечіткої логіки для алгоритмізації дій оперативних працівників під час виявлення та фіксації злочинів. Юридичний часопис Національної академії внутрішніх справ. 2015. № 1. С. 280-293.

137. Носов О. Ю., Черничко Т. В. Нормативно-правове регулювання кластеризації в Україні. Науковий вісник Мукачівського державного університету. Серія «Економіка». Вип. 1(11). С.21-27.

138. Овчарук В. В. Сутність адміністрування на підприємствах. Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство. 2018. Вип. 19(2). С. 115-118.

139. Олизаренко С. А., Перепелица А. В., Капранов В. А. Интервальные нечеткие множества типа 2. Терминология, представление, операции. Системи обробки інформації. Х.: ХУПС, 2011. Вип. 2(92). С. 39-45.

140. Омаров Ш. А. Теоретичні засади формування стратегії сталого розвитку регіонів України. Вісник Чернігівського державного технологічного університету. 2014. № 3 (75). С. 149-157.

141. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. Д. Г. Бобро, С. П. Іванюта, С. І. Кондратов, О. М. Суходоля ; за заг. ред. О. М. Суходолі. Київ: НІСД, 2019. 224 с.

142. Офіціальний веб-сайт The Department of Homeland Security. URL: https://www.dhs.gov/.

143. Офіційний веб сайт Єврпейської комісії. URL: https://commission.europa.eu/index_en.

144. Офіційний веб-сайт Centre for the Protection of National Infrastructure. URL: http://www.cpni.gov.uk/.

145. Офіційний веб-сайт European Cluster for Securing Critical Infrastructures. URL: https://www.finsec-project.eu/ecsci.

146. Офіційний веб-сайт European Commission's Joint Research Centre. URL: https://joint-research-centre.ec.europa.eu/index_en.

147. Офіційний веб-сайт Information Sharing and Analysis Centers. URL: https://www.enisa.europa.eu/.

148. Офіційний веб-сайт KSE Institute. URL: https://kse.ua/ua/.

149. Офіційний веб-сайт National Cybersecurity and Communications Integration Center. URL: https://www.cisa.gov/.

150. Офіційний веб-сайт National Infrastructure Simulation and Analysis Center. URL: https://www.cisa.gov/.

151. Офіційний веб-сайт Nederlands Instituut Publieke Veiligheid. URL: https://nipv.nl/.

152. Офіційний веб-сайт Real Estate Information Sharing and Analysis Center. URL: https://www.reisac.org/.

153. Офіційний веб-сайт Rządowe Centrum Bezpieczeństwa. URL: https://www.gov.pl/web/rcb/o-rcb2.

154. Офіційний веб-сайт Serwis Rzeczypospolitej Polskiej. URL: https://www.gov.pl/.

155. Офіційний веб-сайт The Cybersecurity and Infrastructure Security Agency. URL: https://www.cisa.gov/.

156. Офіційний веб-сайт US-CERT. URL: https://www.us-cert.gov/

157. Офіційний веб-сайт Академія електронного урядування Естонії (eGA). URL: https://ega.ee/.

158. Офіційний веб-сайт Департаменту національної безпеки США. URL: https://www.dhs.gov/.

159. Офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua.

160. Офіційний веб-сайт Європейського кластеру безпеки критичних

інфраструктур. URL: https://www.finsec-project.eu/ecsci.

161. Офіційний веб-сайт Збройних Сил України. URL: https://www.zsu.gov.ua/.

162. Офіційний веб-сайт Комп'ютерної аварійної служби України CERT-UA. URL: https://cert.gov.ua/.

163. Офіційний веб-сайт Конгресу США. Report to Congress of the U.S.-China Economic and Security Review Commission. November 12, ss 127-189. URL: https://www.uscc.gov.

164. Офіційний веб-сайт Міністерства внутрішньої безпеки США: DHS Lexicon Terms and Definitions. URL: https://www.dhs.gov/.

165. Офіційний веб-сайт Міністерства енергетики України URL: https://www.mev.gov.ua/.

166. Офіційний веб-сайт Міністерство захисту довкілля та природних ресурсів URL: https://mepr.gov.ua/.

167. Офіційний веб-сайт Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг https://www.nerc.gov.ua/.

168. Офіційний веб-сайт Національного агентства України з питань державної служби. URL: https://nads.gov.ua/.

169. Офіційний веб-сайт Національного інституту стратегічних досліджень (НІСД). URL: https://niss.gov.ua/.

170. Офіційний веб-сайт Національного Кластеру Кібербезпеки. URL: https://cybersecuritycluster.org.ua/.

171. Офіційний веб-сайт НБУ. URL: https://bank.gov.ua/.

172. Офіційний веб-сайт ООН. URL: https://www.un.org/ru/.

173. Офіційний веб-сайт Програми розвитку ООН в Україні (United Nations Development Programme). URL: https://www.undp.org.

174. Офіційний веб-сайт Світового банку. URL: https://www.worldbank.org/.

175. Офіційний веб-сайт Служби безпеки України URL: https://ssu.gov.ua/antyterorystychnyi-tsentr-pry-ssu.

176. Офіційний веб-сайт Уряду Великобританії. URL: https://www.gov.uk/.

177. Офіційний веб-сайт Федерального відомства інформаційної безпеки Німеччини. URL: https://www.bsi.bund.de/.

178. Офіційний веб-сайт. Office of Science and Technology Policy. URL: https://www.whitehouse.gov/ostp/.

179. Павлов Д. М., Микитюк М. А. Правові та організаційні засади забезпечення захисту критичної інфраструктури у контексті формування нової безпекової парадигми України. Честь і закон. 2020. № 4. С. 69-77.

180. Павлов Д. М. Організаційно-правові засади реформування системи цивільного захисту України у контексті зміни безпекової парадигми. Evropský politický a právní diskurz. 2015. Sv. 2 Vyd. 5. C. 145-149.

181. Панченко К. Механізм державно-приватного партнерства потрібно адаптувати до залучення інвестицій на відбудову зруйнованої інфраструктури. Українська правда. 2022. URL: https://www.epravda.com.ua/columns/2022/07/19/689341/.

182. Пасічник В. М. Філософська категорія безпеки як основа нової парадигми державного управління національною безпекою. Демократичне врядування. 2011. Вип. 7. URL: http://nbuv.gov.ua/UJRN/DeVr_2011_7_7.

183. Петрашко І. Р. Аналіз регуляторного впливу проекту Закону України «Про критичну інфраструктуру та її захист». URL: https://www.drs.gov.ua/wp-content/uploads/2020/07/5854-ob.pdf.

184. Петренко К. Особливості інституційної спроможності громадських об’єднань в Україні. Наукові записки Інституту політичних і етнонаціональних досліджень ім.. І.Ф. Кураса НАН України. 2015. Випуск 4 (78). С. 376-388, 377 с.

185. Пирожков С. І., Божок Є. В., Хамітов Н. В. Національна стійкість (резильєнтність) країни: стратегія і тактика випередження гібридних загроз. Вісник Національної академії наук України. 2021. № 8. С. 74–82.

186. Пирожков С. І., Хамітов Н. В. Цивілізаційний проект України: від амбіцій до реальних можливостей. Вісник Національної академії наук

України. 2016. № 6. С. 45–52.

187. Пілько А. Д. Гарда Т. П. Соціально-економічний розвиток регіону: пошук нових орієнтирів та механізмів реалізації в контексті еволюції безпекознавчих парадигм. Бізнес Інформ. 2016. № 10. С. 112-116.

188. Пілько А. Д. Управління територіальною системою: еволюція безпекознавчої парадигми. Моделювання регіональної економіки. 2012. № 2. С. 332-340.

189. Політологічний енциклопедичний словник. упоряд. В. П. Горбатенко. - 2-е вид., доп. і перероб. Київ : Генеза, 2004. 736 с.

190. Посохов І. М. Аналіз змісту поняття ризик і наукові підходи щодо визначення сутності ризику. Вісник Нац. техн. ун-ту "ХПІ" : зб. наук. пр. Темат. вип.: Технічний прогрес та ефективність виробництва. Харків: НТУ "ХПІ", 2012. № 5. С. 101-108.

191. Постанова КМУ «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» № 1295 від 23.12.2020 р. URL: https://zakon.rada.gov.ua/laws/show/1295-2020- п#Text.

192. Постанова КМУ «Деякі питання об’єктів критичної інформаційної інфраструктури» № 943 від 09.10.2020 р. URL: https://zakon.rada.gov.ua/laws/show/943-2020-п#Text.

193. Постанова КМУ «Деякі питання об’єктів критичної інфраструктури» № 1109 від 09.10.2020 р.. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п#Text.

194. Постанова КМУ «Деякі питання організації здійснення державно-приватного партнерства» № 384 від 11.04.2011 р. URL: https://zakon.rada.gov.ua/laws/show/384-2011-п#n274.

195. Постанова КМУ «Деякі питання паспортизації об’єктів критичної інфраструктури» № 818 від 04.08.2023 р. URL: https://zakon.rada.gov.ua/laws/show/818-2023-п#Text.

196. Постанова КМУ «Деякі питання подання інформації у сфері захисту критичної інфраструктури» № 1175 від 14.10.2022 р. URL:

https://zakon.rada.gov.ua/laws/show/1175-2022-п#Text.

197. Постанова КМУ «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури» № 257 від 24.03.2023 р. URL: https://zakon.rada.gov.ua/laws/show/257-2023- п#Text.

198. Постанова КМУ «Про внесення змін до переліку секторів критичної інфраструктури» № 455 від 09.05.2023 р. URL: https://zakon.rada.gov.ua/laws/show/455-2023- п#Text.

199. Постанова КМУ «Про внесення змін до Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України» № 167 від 24.02.2023 р. URL: https://zakon.rada.gov.ua/laws/show/167-2023-п#Text.

200. Постанова КМУ «Про внесення змін до Порядку проведення аналізу ефективності здійснення державно-приватного партнерства» № 294 від 22.04.2020 р. URL: https://zakon.rada.gov.ua/laws/show/294-2020-п#Text.

201. Постанова КМУ «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» № 518 від 19.06.2019 р. URL:https://zakon.rada.gov.ua/laws/show/518-2019 п#Text.

202. Постанова КМУ «Про затвердження категорій об'єктів державної форми власності та сфер державного регулювання, які підлягають охороні органами поліції охорони на договірних засадах» від 21.10.2018 № 975. URL: https://zakon.rada.gov.ua/laws/show/975-2018-п#Text.

203. Постанова КМУ «Про затвердження Переліку об'єктів, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період»: від 24.04.1999 № 675-019. Кабінет Міністрів України. (для службового користування).

204. Постанова КМУ «Про затвердження переліку особливо важливих об'єктів електроенергетики, у тому числі територій забороненої зони та контрольованої зони гідротехнічних споруд, які підлягають охороні відомчою воєнізованою охороною» від 04.07.2018 № 575. URL: https://zakon.rada.gov.ua/laws/show/575-2018-п#n15.

205. Постанова КМУ «Про затвердження переліку підприємств, що

мають стратегічне значення для економіки та безпеки держави» від 04.03.2015 № 83. URL: https://zakon.rada.gov.ua/laws/show/83-2015-n#Text.

206. Постанова КМУ «Про затвердження Положення про єдину державну систему цивільного захисту» № 11 від 09.01.2014 р. URL: https://zakon.rada.gov.ua/laws/show/11-2014-п#Text.

207. Постанова КМУ «Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього» № 415 від 28.04.2023 р. URL: https://zakon.rada.gov.ua/laws/show/415-2023-п#Text.

208. Постанова КМУ «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах» № 1772 від 07.09.2022 р. URL: https://zakon.rada.gov.ua/laws/show/1772-2002-п#Text.

209. Постанова КМУ «Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури» № 821 від 22.07.2022 р. URL: https://zakon.rada.gov.ua/laws/show/821-2022- п#Text.

210. Постанова КМУ «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» № 563 від 23.08.2016 р. URL: https://zakon.rada.gov.ua/laws/show/563-2016- п#Text.

211. Постанова КМУ «Про затвердження Порядку функціонування державної системи фізичного захисту» № 1337 від 30.08.2022 р. URL: https://zakon.rada.gov.ua/laws/show/1337-2011- п#Text.

212. Постанова КМУ «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» № 373 від 29.03.2006 р. URL: https://zakon.rada.gov.ua/laws/show/1772-2002-п#Text.

213. Постанова КМУ «Про затвердження Правил техногенної безпеки у сфері цивільного захисту на підприємствах, в організаціях, установах та на небезпечних територіях» від 15.08.2007 № 1051. Кабінет Міністрів України. (для службового користування).

214. Постанова КМУ «Про затвердження Програми діяльності Кабінету Міністрів України» № 471 від 12.06.2020 р. URL: https://zakon.rada.gov.ua/laws/show/471-2020-п#Text.

215. Постанова КМУ «Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури» № 1174 від 14.10.2022 р. URL: https://zakon.rada.gov.ua/laws/show/1174-2022- п#Text.

216. Постанова КМУ «Про реалізацію статті 85 Закону України «Про відновлення платоспроможності боржника або визнання його банкрутом»» від 15.05.2013 № 339. URL: https://zakon.rada.gov.ua/laws/show/339-2013-%D0%BF#Text (втратила чинність).

217. Постанова КМУ «Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України» № 787 від 12.07.2022 р. URL: https://zakon.rada.gov.ua/laws/show/787-2022- п#Text.

218. Постанова Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг «Щодо захисту інформації, яка в умовах воєнного стану може бути віднесена до інформації з обмеженим доступом, у тому числі щодо об'єктів критичної інфраструктури» №349 від 26.03.2022 р. URL: https://zakon.rada.gov.ua/rada/show/v0349874-22#Text.

219. Постанова Правління НБУ «Про затвердження Положення про визначення об'єктів критичної інфраструктури в банківській системі України» № 151 від 30.11.2020 р. URL: https://zakon.rada.gov.ua/laws/show/v0151500-20#Text.

220. Постельжук О. П., Валюх Л. І., Невинна Г. Я., Михальчук Р. Ю. Транснаціональна злочинність і національна безпека: необхідність зміни безпекової парадигми України. Інвестиції: практика та досвід. 2021. № 22. С. 107-113.

221. Потеряйко С. П. Бєлікова К. Г., Твердохліб О. С. Теоретико-методологічне обгрунтування моделі визначення критерію безпеки населення

на основі прогнозу функціонування єдиної державної системи цивільного захисту. Інвестиції: практика та досвід. 2021. № 18. С. 40-48.

222. Резнікова О. О., Войтовський К. Є. Лепіхов А. В. Організація системи забезпечення національної стійкості на регіональному і місце вому рівнях : аналіт. доп.; за заг. ред. О. О. Резнікової. Київ: НІСД, 2021. 140 с.

223. Резнікова О. О. Щодо Концепції забезпечення національної стійкості. Аналіт. записка. Серія „Національна безпека". 2020. № 8. С. 1–8.

224. Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища: монографія. Київ: НІСД, 2022. 456 с.

225. Ризикологія в економіці та підприємництві: монографія. В. В.Вітлінський, Г. І. Великоіваненко. К.: КНЕУ, 2004. 480 с.

226. Рішення РНБО України «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» від 01.03.2014 р. URL: https://zakon.rada.gov.ua/laws/show/n0001525-14#Text.

227. Розпорядження КМУ «Деякі питання реформування державного управління України». № 831-р від 21.07.2021 р URL: https://zakon.rada.gov.ua/laws/show/831-2021-р#Text.

228. Розпорядження КМУ «Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури» № 825-р від 19.09.2023 р. URL: https://zakon.rada.gov.ua/laws/show/825-2023-р#Text.

229. Розпорядження КМУ «Про затвердження переліку особливо важливих об'єктів нафтогазової галузі» від 27.05.2009 № 578-р. URL: https://zakon.rada.gov.ua/laws/show/578-2009-р#Text.

230. Розпорядження КМУ «Про схвалення Концепції створення державної системи захисту критичної інфраструктури» № 1009-р від 06.12.2017 р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-п#Text.

231. Розпорядженням КМУ «Про затвердження плану пріоритетних дій Уряду на 2023 рік» № 221-р від 14.03.2023 р. URL: https://zakon.rada.gov.ua/laws/show/221-2023- р#Text.

232. Рось О. Г. Поняття та сутність нормативно-правового забезпечення інституційної спроможності представницьких органів місцевого самоврядування. Інвестиції: практика та досвід. 2019. № 18. С. 97-100.

233. Рудич Ф. М. Становлення суспільно-політичного устрою в сучасній Україні: політологічний аналіз. Шляхи виходу із кризи. Наукові записки Інституту політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України. 2016. Вип. 5-6. С. 63-88.

234. Садовський М. В. Правові механізми демілітаризації міністерства оборони України, як засіб оборонної реформи та елемент реформування сектору безпеки Юридичний вісник. № 3 (60). 2021. С. 117-121.

235. Система розробки і здійснення публічних політик в Україні. Під заг. ред. О. П. Дем'янчука. К.: Факт, 2004. 224 с.

236. Ситник Г. Інституційно-цивілізаційна парадигма дослідження проблем та державно-управлінських аспектів забезпечення національної безпеки. Вісник Національної академії державного управління при Президентові України. 2011. Вип. 2. С. 25-34.

237. Скопенко Н. С., Євсєєва-Северина І. В. Ризик-менеджмент як необхідна складова системи економічної безпеки виробничих підприємств. Наукові праці Національного університету харчових технологій. 2020. Т. 26, № 2. С. 120-129.

238. Словник іншомовних слів. за ред. О. С. Мельничука. К: Голов. ред. УРЕ АН УРСР, 1975. 768 с.

239. Соболєв В. М., Соболєва М. В. Інституційна спроможність системи вищої освіти та чинники її забезпечення. Проблеми економіки № 2 (48), 2021. С.63-69.

240. Стратегія національної безпеки України «Україна у світі, що змінюється» URL: https://zakon.rada.gov.ua/laws/show/105/2007 (втратила чинність на підставі Указу Президента № 287/2015 від 26.05.2015)

241. Страхніцький Я. О. Інституційні перетворення у напрямку підвищення ефективності державної політики захисту критичної інфраструктури. Публічне управління та регіональний розвиток. 2024. №1

(23). С. 28-52. DOI https://doi.org/10.34132/pard2024.23.02

242. Страхніцький Я. О. Особливості державної політики захисту критичної інфраструктури в Україні та напрями її удосконалення в умовах війни. Knowledge, Education, Law, Management. 2022. № 7. (51). С. 104-111. DOI https://doi.org/10.51647/kelm.2022.7.15

243. Страхніцький Я. О. Особливості сучасної системи захисту критичної інфраструктури в Україні. Наука, освіта, технології та суспільство: актуальні проблеми теорії та практики: матеріали Міжнар. наук-практ. конф., м. Полтава, 25 трав. 2022 р. Полтава, 2022. Ч. 1. С. 58-60.

244. Страхніцький Я. О. Структурно-функціональна характеристика системи захисту критичної інфраструктури в Україні. Публічне управління та митне адміністрування. 2022. № 4. (35). С.112-117. DOI https://doi.org/10.32782/2310-9653-2022-4.17.

245. Страхніцький Я. О. Формування наукової парадигми державної політики у сфері захисту критичної інфраструктури. Управління інноваційним процесом в Україні: напрями розвитку: матеріали IX Міжнар. наук-практ. конф., м. Львів, 19-21 трав. 2022 р. Львівська політехніка. Львів, 2022. С. 176-178.

246. Страхніцький Я. О. Структурно-функціональна характеристика системи захисту критичної інфраструктури в Україні. Публічне управління та митне адміністрування. 2022. № 4. (35). С.112-117. DOI https://doi.org/10.32782/2310-9653-2022-4.17

247. Страхніцький Я. О. Державна політика у сфері захисту критичної інфраструктури в умовах військового стану в Україні. Сучасна парадигма публічного управління: збірник тез IV Міжнар. наук.-практ. конф. м. Львів 10-12 листоп. 2022р. / За наук. ред. к.е.н., доцента Стасишина А.В.. ЛНУ імені Івана Франка, Львів, 2022. С. 376-381.

248. Страхніцький Я. О. Кластерний підхід до забезпечення захисту критичної інфраструктури в умовах воєнного стану в Україні. Інвестиції: практика та досвід. 2023. № 23. С.163-169. URL: https://www.nayka.com.ua/index.php/investplan/article/view/2610

DOI: https://doi.org/10.32702/2306-6814.2023.23.163.

249. Страхніцький Я. О. Концептуальні засади забезпечення резильєнтності об’єктів критичної інфраструктури в умовах гібридних загроз. Глобальні тенденції та національні особливості публічного управління та адміністрування: матер. круглого столу, м. Вінниця 22 груд. 2023 р. Вінниця: Вінницький державний педагогічний університет імені Михайла Коцюбинського, ТОВ «Друк», 2023. С. 42-44.

250. Суспільно-політичні процеси. Науково-популярне видання громадської організації «Академія політичних наук». К., 2017. № 2–3. 308 с.

251. Суходоля О. М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. Стратегічні пріоритети. 2016. № 3. С. 62-76.

252. Суходоля О. М. Захист критичної інфраструктури: сучасні виклики та пріоритетні завдання сектору безпеки. Науковий часопис Академії національної безпеки. 2017. № 1-2. С. 50-80.

253. Суходоля О. М. Стійкість енергетичної системи чи стійкість енергозабезпечення споживачів: постановка проблеми. Стратегічні пріоритети. 2018. № 2. С. 101–117.

254. Суходоля О. Нова Директива ЄС щодо стійкості критичної інфраструктури (CER Directive). https://niss.gov.ua/sites/default/files/2023-04/az_eu-cer_12042023.pdf.

255. Суходоля О. М. Стійкість здійснення життєво важливих функцій: узагальнення досвіду реагування України на руйнування енергетичної інфраструктури. URL: https://niss.gov.ua/sites/default/files/2023-07/az-dosvid-stiykosti-oes-2_20072023.pdf.

256. Теленик С. С. Досвід правового регулювання системи захисту критичної інфраструктури в США. Науковий вісник НАВС. 2018. № 2 (107). С. 358–370.

257. Теленик С. С. Державна система захисту критичної інфраструктури України: концептуальні засади адміністративно-правового регулювання: монографія. Одеса : Видавничий дім «Гельветика», 2020. 602 с.

258. Теленик С. С. Критична інфраструктура як об`єкт адміністративно-правового регулювання. Юридичний часопис Національної академії внутрішніх справ. 2018. № 1 (15). С. 179–189.

259. Теленик С. С. Державна система захисту критичної інфраструктури України: концептуальні засади адміністративно-правового регулювання: монографія. Одеса : Видавничий дім «Гельветика», 2020. 602 с.

260. Терещенко О. О. Антикризове управління фінансами підприємств : автореф. дис. д-ра екон. наук. Київ, 2005. 34 с.

261. Тертичка В. В. Державна політика: аналіз та здійснення в Україні. К.: Вид-во Соломії Павличко «Основи». 2002. 750 с.

262. Тристороння заява Президентів України, США та Росії. Закон України № 998 від 14.01.1994 р. URL:https://zakon.rada.gov.ua/laws/show/998_300#Text.

263. Тундаєв С. М. Поняття та сутність інституційної спроможності правоохоронних органів України щодо протидії діяльності злочинних спільнот та осіб, що перебувають у статусі підвищеного злочинного впливу. Юридичний науковий електронний журнал. 2022. № 11. С. 684-689.

264. Угода між Україною і Російською Федерацією про статус та умови перебування Чорноморського флоту Російської Федерації на території України №643-076 від 20.10.2010 р. URL: https://zakon.rada.gov.ua/laws/show/643_076#Text.

265. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14.09.2020 р. «Про Стратегію національної безпеки України» № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020.

266. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 06.05.2015 р. «Про Стратегію національної безпеки України» № 287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text.

267. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки»» № 56/2022 від 16.02.2022 р. URL:

https://zakon.rada.gov.ua/laws/show/56/2022#Text.

268. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави» № 446 від 26.08.2021 р. URL: https://zakon.rada.gov.ua/laws/show/446/2021#Text.

269. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»» № 96/2016. від 15.03.2016 р. URL: https://www.rnbo.gov.ua/ua/Ukazy/417.html?PRINT.

270. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про Стратегічний оборонний бюлетень України» №473/2021 від 17.09.2021 р. URL: https://zakon.rada.gov.ua/laws/show/473/2021#n2.

271. Указ Президента України Про рішення Ради національної безпеки і оборони України від 17 жовтня 2023 року «Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій» № 695/2023 від 17.10.2023 р. URL: https://www.president.gov.ua/documents/6952023-48641

272. Указ Президента України. «Про Антитерористичний центр» № 1343/98 від 13.04.2004 р. URL: https://zakon.rada.gov.ua/laws/show/1343/98#Text.

273. Фадєєва І. Г. Гринюк О. І. Нечітка логіка як інструмент ризик-контролінгу в контексті проактивного управління нафтогазовидобувними підприємствами. Бізнес Інформ. 2019. № 4. С. 212-220.

274. Хаустова В. Є. Омаров Ш. А. Концепція сталого розвитку як парадигма розвитку суспільства. Проблеми економіки. 2018. № 1. С. 265-273.

275. Хитра О. Л. Реагування на кризові ситуації, що загрожую національній безпеці України: адміністративно-правові засади реалізації теорії та досвіду: монографія. Львів: Растр-7, 2019. 398 с.

276. Цивільний кодекс України. Закон України № 435-IV від 16.01.2003 р. URL: https://zakon.rada.gov.ua/laws/show/435-

15/ed20030116#Text

277. Цюрупа М. В. Зміна парадигм воєнно-політичного мислення у доктринах та стратегіях воєнної безпеки України XX XXI ст.. Українознавчий альманах. 2021. Вип. 28. С. 120-126.

278. Чалий В. О. Нейтралітет для України – це пастка, адже ми на кордоні з рф. URL: https://hromadske.radio/podcasts/ukraina-vholos/neytralitet-na-kordoni-z-rf-nichoho-ne-zabezpechuie-tse-pastka-chalyy.

279. Чумаченко С. М., Троцько В. В. Оцінювання загроз об'єктам критичної інфраструктури. Науковий вісник: цивільний захист та пожежна безпека. 2017. № 1. С. 41-47.

280. Шатун В. Т. Позаблоковий статус держави та українські реалії. Південня правда. 2015. URL: http://www.up.mk.ua/mainpage/show_item/4024

281. Шемшученко Ю. С., Бобровник С. В. Правове регулювання. Юридична енциклопедія: в 6 т. Київ, 2003. Т. 5. П С. С. 40-41.

282. Яременко О. І., Страхніцький Я. О. Визначення та управління загрозами у структурі державної політики захисту критичної інфраструктури. *Університетські наукові записки*. 2022. № 3 (87). С. 73-82. DOI https://doi.org/10.37491/UNZ.87.6.

283. Яременко О. І., Страхніцький Я. О. Теоретико-методичні основи забезпечення системи захисту критичної інфраструктури держави. Державне управління: удосконалення та розвиток. 2022. № 1. URL: http://www.dy.nayka.com.ua/?op=1&z=2610. DOI: https://doi.org/10.32702/2307-2156-2022.1.38

284. Яременко О. І., Страхніцький Я. О. Теоретичні підходи до визначення дефініції критичної інфраструктури як об'єкту державного управління. Публічне управління та митне адміністрування. 2022. №1 (32). С. 76-82. DOI: https://doi.org/10.32836/2310-9653-2022-1.13.

285. Яременко О. І., Страхніцький Я. О. Сучасні проблеми державної політики України у сфері захисту критичної інфраструктури. Публічне управління в Україні: виклики сьогодення та глобальні імперативи»: матеріали Міжнар. наук-практ. конф., м. Хмельницький, 11 лют. 2022 р. /

Хмельницький: Хмельницький університет управління та права імені Леоніда Юзькова. Хмельницький, 2022. С. 126-129.

286. Bakushevych I., Martyniak I. (2013) Cluster infrastructure networking model for the knowledge economy development in Ukraine. Nierówności społeczne a wzrost gospodarczy., vol 35, pp. 41-51

287. Bhatt G. D. (2000) A resource-based perspective of developing organizational capabilities for business transformation. Knowledge and process management. Vol. 7. № 2. P. 119-129.

288. Bruneau, M, Chang, SE, Eguchi, RT, et al. (2003). A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. Earthquake Spectra. 19(4), 733-752

289. Cantelmi R., Gravio G., Patriarca R. (2021) Reviewing qualitative research approaches in the context of critical infrastructure resilience. Environment Systems and Decisions 41(3) pp. 1-36.

290. Carrillo-Hermosilla J., Unruh G. C. (2006). Technology Stability and Change: An Integrated Evolutionary Approach. Journal of Economic Issues. vol 3. pp. 707-742.

291. Cenuşa, D. (2023) Ukraine's critical infrastructure vs. Russia's energy positioning - the «war of nerves». Analysis by Dionis Cenuşa. URL:https://www.ipn.md/en/ukraines-critical-infrastructure-vs-russias-energy-positioning-the-7978_1093693.html#ixzz8GikIr7Au.

292. Commission of the European Communities (2005), Green Paper on a European programme for critical infrastructure protection. URL: https://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_6_raporlar/1_2_green_papers/com2005_green_paper_on_critical_infrastructure.pdf.

293. Communication from the commission on a European Programme for Critical Infrastructure Protection. Commission of the European Communities Brussels, 12.12.2006. COM (2006) 786 final. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786: FIN:EN:PD.

294. Coombs T. W. (2021) Ongoing Crisis Communication: Planning, Managing, and Responding, SAGE Publications, 304 p.

295. Council Directive 2008/114/EC of 08.12.2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. URL: http://eur-lex.europa. eu/.

296. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance). URL: http://data.europa.eu/eli/dir/2008/114/oj.

297. Critical infrastructure protection. An official website of the European Union. URL: https://joint-research-centre.ec.europa.eu/scientific-activities-z/critical-infrastructure-protection.

298. Critical Infrastructure Resilience – 2023: collection of materials of the scientific and practical conference, Kyiv, June 21, 2023, PIMEE of NAS of Ukraine. 2023. 109 p.

299. Cyber-Sicherheitsstrategie für Deutschland. Bundesministerium des Innern. Berlin, 2016. URL: https://www.bmi. bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf.

300. Department of Homeland Security (2013), Presidential Policy Directive. Critical Infrastructure Security and Resilience. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

301. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557.

302. Electricity Information Sharing and Analysis Center. URL: https://www.eisac.com/.

303. EMP/GMD. The Science and Technology Directorate. URL: https://www.dhs.gov/.

304. European Commission. Guidance Document on Indicators of Public Administration Capacity Building, June 2014, p. 3. URL: https:ec.europa.eu/social/BlobServlet?docId=14144.

305. Fadyeyeva I. G., Gryniuk O. I. Fuzzy modelling in risk assessment of oil and gas production enterprises' activity. Baltic Journal of Economic Studies. 2017. Vol. 3. №. 4. pp. 256-264.

306. 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.

307. Foreign Investment Risk Review Modernization Act of 2018. Src.1702.Findings;Sense of Congress. (b) Sense of Congress. (5). URL: https://www.treasury.gov/resourcecenter/international/Documents/Summary-offirrma.pdf.

308. Freeman, E. (1984), Strategic Management: A stakeholder approach. Boston: Pitman, 266 p. URL: http://bookre.org/reader?file=1164948&pg=6.

309. German Strategy for Adaptation to Climate Change. The Federal Government. URL: https://www.preventionweb.net/files/dasgesamtenbf1-63.pdf.

310. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) URL: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/BSI-Gesetz/bsi-gesetz_node.html.

311. Guidance notes on building critical infrastructure resilience in Europe and Central Asia. UNDP 2022. URL: https://www.undp.org/eurasia/publications/guidance-notes-building-critical-infrastructure-resilience-europe-and-central-asia.

312. Guide 73:2009, IDT. Київ: Мін.економ.розвитку України, 2014. ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT). Київ: Мінекономрозвитку України, 2015. 74 с.

313. Her Majesty the Queen in Right of Canada (2009) National Strategy for Critical Infrastructure. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf.

314. Hereinafter, the Directives adopted by President Bush and Obama are cited by: National Security Presidential Directives. George Bush Administration; The official website of the Federation of American Scientists. URL:

https://fas.org/irp/offdocs/nspd/index.html.

315. Improving Critical Infrastructure Cybersecurity. Executive Order №13636 of February 12, 2013. URL: https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

316. Infrastructure Investment and Jobs Act. Public Law №: 117-58. URL: https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf.

317. ISO 22316:2017 Security and resilience – Organizational resilience – Principles and attributes https://www.iso.org/obp/ui/#iso:std:iso:22316:ed-1:v1:en.

318. Josse, E., Dubois, V. (2009). Interventions humanitaires en santé mentale dans les violences de masse (1st edition) Bruxelles: Groupe De Boeck. p. 301.

319. Kaminska V., Namazova Yu., Strakhnitskyi Y. Mehanisms of formation and implementation of state policy in the field of youth protection. *Modern Science.* 2022. №1. P. 41-49.

320. Krajowego Planu Zarządzania Kryzysowego https://www.gov.pl/web/rcb/krajowy-plan-zarzadzania-kryzysowego.

321. Kubiak M. Kwestie bezpieczenstwa w europejskiej mysli filozoficznej. Wojsko i wychowanie. 2001. № 6. S. 51-55.

322. Kuhn. T.S. The Structure of Scientific Revolutions. Chicago, 1962; M., 1975. p. 210.

323. Livre Blanc sur la défense et la sécurité nationale, 2013. Офіційний веб-сайт уряду Франції: https://www.gouvernement.fr/en/white-paper-on-defense-and-national-security-2013.

324. Merton, R.K. (1968) Social Theory and Structure. London: The Free Press of Glencoe, Collier- MacMillan Limited. P. 22-216.

325. MITRE. Cyber Resiliency Engineering Framework. Deborah J. Bodeau & Richard Graubart. https://www.mitre.org/sites/default/files/media/publicat2.pdf.

326. Modernization of the system of public management and administration in Ukraine: the experience of the Republic of Latvia: SECTION 5. Features of the current state policy in the sphere of protection of critical infrastructure in the conditions of war in Ukraine (Strahnitskyi Ya. O.). Scientific monograph. Riga,

Latvia : “Baltija Publishing”, 2023. 232 p.

327. Mu S., Cheng H., Chohr M., and Peng W. (2014) Assessing riskmanagement capability of contractors in subway projects in mainland China. International Journal of Project Management. vol.32. pp. 452-460.

328. Narodowy Program Ochrony Infrastruktury Krytycznej. URL: https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej.

329. National Infrastructure Protection Plan – NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. URL: https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf.

330. National Risk Assessments: A Cross Country Perspective The evolving practice of National Risk Assessments in OECD countries. URL: https://read.oecd-ilibrary.org/governance/national-risk-assessments/the-evolving-practice-of-national-risk-assessments-in-oecd-countries_9789264287532-3-en#page1.

331. National Strategy for Critical Infrastructure Protection (CIP Strategy). URL: https://www.kritis.bund.de.

332. National strategy for homeland security. Office of homeland security. July 2002. URL: https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf.

333. National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. URL: https://georgewbush-whitehouse.archives.gov/pcipb/physical.html.

334. Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) BMI, 2009. URL: http://www.kritis.bund.de.

335. NIST Special Publication 800-160. Vol. 2. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach URL: https://nvlpubs.nist.gov/nistpubs/Special Publications/NIST.SP.800-160v2r1.pdf 2.

336. Peters B. G. (2000) Institutional Theory: Problems and Prospects. Political Science Series. 18 p. URL:

https://www.ihs.ac.at/publications/pol/pw_69.pdf.

337. Posen B. R. The Security Dilemma and Ethnic Conflict. Survival. Spring 1993. Vol 35. № 1. P. 28.

338. Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

339. Public Management Reviews. Towards an Integrated Public Service. OECD. Ireland. 2008. 377 P. DOI: https://doi.org/10.1787/ 9789264043268-en.

340. Public-Private Partnership Handbook. Asian Development Bank. URL: https://www.adb.org/sites/default/files/institutional-document/31484/public-private-partnership.pdf.

341. Public-Private Partnerships: Reference Guide Version 3. Washington, DC: World Bank, 2017. URL: https://openknowledge.worldbank.org/handle/10986/2905 2.

342. Rehak D., Senovsky P., Slivkova S. (2018) Resilience of Critical Infrastructure Elements and Its Main Factors. Systems. vol 6. pp. 21-30.

343. Rød, B., A. Barabadi, and M. Naseri (2020). “Recoverability modeling of power distribution systems using accelerated life models: Case of power cut due to extreme weather events in Norway. Manage. Eng. vol. 36 (5). pp. 15-33.

344. Rød, B., D. Lange, M. Theocharidou, and C. Pursiainen (2020). From risk management to resilience management in critical infrastructure. Manage. Eng. vol. 36 (4). pp. 1-13.

345. Rotfeld A. D. Europejski system bezpieczenstwa in statu nascendi. Warszawa: PISM, 1990. P. 18.

346. Øien K.та Bodsberg L. Safety and Reliability – Safe Societies in a Changing World: Proceedings of ESREL. Trondheim, Norway. 2018. 2018. pp. 12-25.

347. Sicherheitsstrategie für die Güterverkehrs - und Logistikwirtschaf. Das Bundesministerium für Digitales und Verkehr (BMDV). URL: https://bmdv.bund.de/SharedDocs/DE/Publikationen/DG/sicherheitsstrategie.pdf?_

_blob=publicationFile.

348. Strahnitskyi Ya. O. Institutional aspects of state policy implementation in the sphere of critical infrastructure protection in Ukraine. International Scientific Conference Development of Scientific Space in the Context of Global Changes: Conference Proceedings, November 25-26, 2022. Riga, Latvia: «Baltija Publishing», P. 26-30.

349. Strahnitskyi Ya. O. Organizational and legal mechanisms of modern state policy in the field of critical infrastructure protection in Ukraine. International scientific conference «Influence of Europeanization on public management and administration in Ukraine» : conference proceeding*s* (October 5-6, 2022. Riga, the Republic of Latvia). Riga, Latvia: "Baltija Publishing". 2022. P. 91-95.

350. Trucco P., Cagno E., and Ambroggi M. De, (2012) Dynamic functionalmodelling of vulnerability and interoperability of Critical Infrastructures, Reliability Engineering and System Safety. vol. 105. pp. 51–63

351. UNISDR Terminology on Disaster Risk Reduction: https://tinyurl.com/59tdbxb

352. Urie Bronfenbrenner. The Ecology of Human Development. Harvard University Press, 1979. 330 p.

353. USA Patriot Act of 2001. URL: https://www.gpo.gov/

354. Ustawa «O zarządzaniu kryzysowym» z dnia 26 kwietnia 2007 r. URL: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20070890590

355. 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. vol. pp. 6-12.

356. Yang Z., Barroca B., Bony-Dandrieux A., Dolidon H. (2022) Resilience Indicator of Urban Transport Infrastructure A Review on Current Approaches. Infrastructures. vol. 7. URL: https://doi.org/10.3390/infrastructures7030033

357. Zollo M., Winter S. (2002) Deliberate learning and the evolution of dynamic capabilities. Organization science. Vol.13. № 3. P. 3-8.

358. Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme. URL: https://www.bsi.bund.de/

ДОДАТКИ

ДОДАТОК А

Опис показників Національного індексу кібербезпеки (NCSI)

№ п/п	Назва показника
1	2
1. Розробка політики кібербезпеки	
1.1.	Відділ політики кібербезпеки
1.2.	Формат координації політики кібербезпеки
1.3.	Стратегія кібербезпеки
1.4.	План реалізації стратегії кібербезпеки
2. Аналіз кіберзагроз та інформація	
2.1.	Підрозділ аналізу кіберзагроз
2.2.	Публічні звіти про кіберзагрози публікуються щорічно
2.3.	Веб-сайт із кібербезпекою та безпекою
3. Освіта та професійний розвиток	
3.1.	Компетентності кібербезпеки в початковій або середній освіті
3.2.	Програма кібербезпеки рівня бакалавра
3.3.	Магістерська програма кібербезпеки
3.4.	Програма кібербезпеки рівня PhD
3.5.	Професійна асоціація кібербезпеки
4. Внесок у глобальну кібербезпеку	
4.1.	Конвенція про кіберзлочинність
4.2.	Представництво у форматах міжнародного співробітництва
4.3.	Міжнародна організація з кібербезпеки, розміщена в країні
4.4.	Розвиток потенціалу кібербезпеки для інших країн
5. Захист цифрових сервісів	
5.1.	Відповідальність за кібербезпеку для постачальників цифрових послуг
5.2.	Стандарт кібербезпеки для державного сектору
5.3.	Компетентний наглядовий орган
6. Захист основних послуг	
6.1.	Визначено операторів життєво необхідних послуг
6.2.	Вимоги до кібербезпеки для операторів основних послуг
6.3.	Компетентний наглядовий орган
6.4.	Регулярний моніторинг заходів безпеки
7. Електронна ідентифікація та довірчі послуги	
7.1.	Унікальний постійний ідентифікатор
7.2.	Вимоги до криптосистем
7.3.	Електронна ідентифікація
7.4.	Електронний підпис

7.5.	Позначення часу
7.6.	Служба електронної рекомендованої доставки
1	**2**
7.7.	Компетентний наглядовий орган
8. Захист персональних даних	
8.1.	Законодавство про захист персональних даних
8.2.	Орган із захисту персональних даних
9. Реагування на кіберінциденти	
9.1.	Підрозділ реагування на кіберінциденти
9.2.	Відповідальність за звітність
9.3.	Єдина контактна точка для міжнародної координації
10. Управління кіберкризою	
10.1.	План управління кіберкризою
10.2.	Навчання з управління кіберкризою національного рівня
10.3.	Участь у міжнародних навчаннях з кіберкризи
10.4.	Оперативна підтримка волонтерів у кіберкризах
11. Боротьба з кіберзлочинністю	
11.1.	Кіберзлочини криміналізовані
11.2.	Підрозділ боротьби з кіберзлочинністю
11.3.	Підрозділ цифрової криміналістики
11.4.	Цілодобовий контактний пункт для боротьби з міжнародною кіберзлочинністю
12. Військові кібероперації	
12.1.	Підрозділ кібероперацій
12.2.	Навчання з кібероперацій
12.3.	Участь у міжнародних кібернавчаннях

Джерело: узагальнено автором за даними [157]

ДОДАТОК Б

Перелік секторів критичної інфраструктури

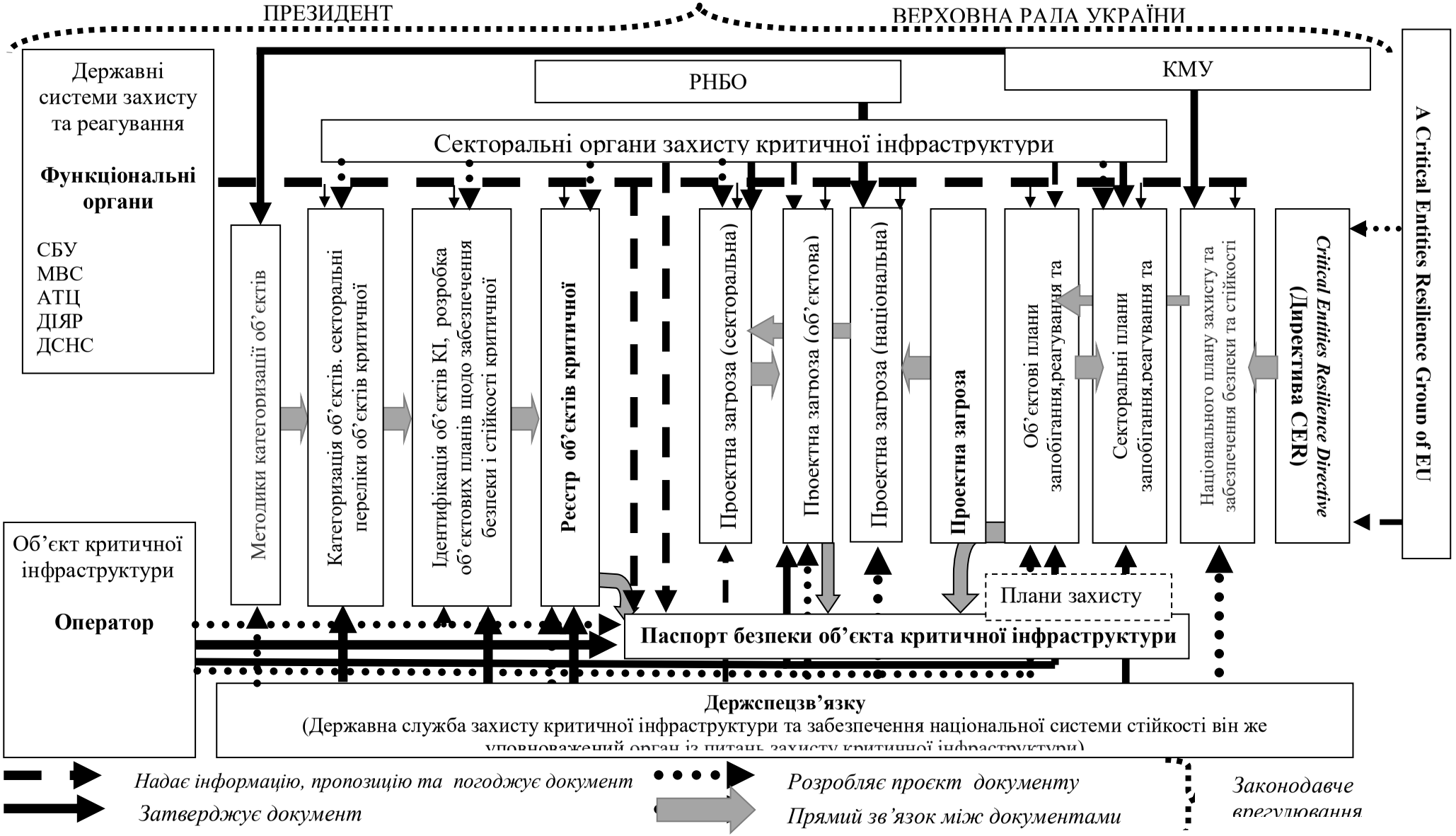
Б№ п\п	Сектор	Підсектор	Секторальний орган
1	**2**	**3**	**4**
1	Паливно-енергетичний сектор	електро-енергетика, вугільно-промисловий комплекс, торфодобування, нафтова промисловість, газова промисловість, ядерна енергетика,	Міненерго
2	Цифрові технології	електронні довірчі послуги та електронна ідентифікація; електронні комунікації; електронне урядування	Мінцифри
3	Захист інформації	-	Держспецзв'язку
4	Системи життєзабезпечення	комунальні послуги	Мінрегіон
5	Харчова промисловість та агропромисловий комплекс	-	Мінагрополітики
6	Державний матеріальний резерв	-	Мінекономіки
7	Охорона здоров'я	медична допомога; громадське здоров'я; фінансове забезпечення охорони здоров'я; інформаційні технології у сфері охорони здоров'я; фармацевтична промисловість; медична наука	МОЗ
8	Ринки капіталу та організовані товарні ринки	-	НКЦПФР
9	Фінансовий сектор	-	Мінфін
10	Транспорт і пошта	авіаційний транспорт; автомобільний та міський електротранспорт, у тому числі метрополітен; залізничний транспорт; морський та річковий транспорт; поштовий зв'язок;	Мінінфраструктури
11	Промисловість	хімічна промисловість; металургійна промисловість; оборонна промисловість; космічна промисловість; авіаційна промисловість; суднобудівна промисловість	Мінстратегпром
12	Сектор громадської безпеки	громадська безпека; екстрена допомога населенню за єдиним телефонним номером 112	МВС
13	Цивільний захист населення і територій	служби порятунку (атестовані аварійно-рятувальні служби згідно із законодавством)	МВС

1	2	3	4
14	Міграція (імміграція та еміграція)	-	МВС
15	Охорона навколишнього природного середовища	управління, використання та відтворення поверхневих водних ресурсів, розвиток водного господарства; поводження з радіоактивними відходами; охорона, раціональне використання і відтворення об'єктів природно-заповідного фонду	Міндовкілля
16	Сектор оборони	зберігання боєприпасів; виробництво боєприпасів	Міноборони
17	Національна безпека	-	СБУ
18	Правосуддя	-	ДСА
19	Тримання під вартою	-	Мін'юст
20	Наукові дослідження та розробки	дослідницька інфраструктура наукових установ та закладів вищої освіти	МОН
21	Фінансовий сектор	банківська система; ринок небанківських фінансових послуг (крім ринків капіталу та організованих товарних ринків); ринок платіжних послуг	Національний банк
22	Вибори та референдуми	-	Центральна виборча комісія
23	Соціальний захист	пенсійне забезпечення; соціальне страхування; соціальна допомога і соціальні послуги; інформаційна система соціальної сфери	
24	Інформаційні послуги	засоби масової інформації	МКІП
25	Державна влада та місцеве самоврядування	-	Держспецзв'язку

Джерело: [193]

ДОДАТОК В

Інституційна модель стійкості критичної інфраструктури



Джерело: узагальнено автором

ДОДАТОК Г

Відомості про апробацію результатів дисертації

1. Міжнародна науково-практична конференція «Публічне управління в Україні: виклики сьогодення та глобальні імперативи», м. Хмельницький, Хмельницький університет управління та права імені Леоніда Юзькова, 11 лютого 2022 року. (очна участь).
2. Міжнародна науково-практична конференція «Управління інноваційним процесом в Україні: напрями розвитку», м. Львів, Національний університет «Львівська політехніка», 19-21 травня 2022 року. (очна участь).
3. Міжнародна науково-практична конференція «Наука, освіта, технології та суспільство: актуальні проблеми теорії та практики», м. Полтава, Центр фінансово-економічних наукових досліджень, 25 травня 2022 року. (заочна участь).
4. Міжнародна науково-практична конференція «Influence of Europeanization on public management and administration in Ukraine», Riga, Latvia, Publishing House «Baltija Publishing», 5-6 жовтня 2022 року. (заочна участь).
5. Міжнародна науково-практична конференція «Сучасна парадигма публічного управління», м. Львів, Львівський національний університет імені Івана Франка, 10-12 листопада 2022 року. (очна участь).
6. Міжнародна науково-практична конференція «Development of Scientific Space in the Context of Global Changes: Conference Proceedings», Riga, Latvia, Publishing House «Baltija Publishing», 25-26 листопада 2022 року. (заочна участь).
7. Круглий стіл «Глобальні тенденції та національні особливості публічного управління та адміністрування», м. Вінниця, Вінницький державний педагогічний університет імені Михайла Коцюбинського, 22 грудня 2023 р. (очна участь).

ДОДАТОК Д

Довідки про впровадження результатів дисертаційного дослідження

ДЕРЖАВНА ІНСПЕКЦІЯ ЕНЕРГЕТИЧНОГО НАГЛЯДУ УКРАЇНИ
(ДЕРЖЕНЕРГОНАГЛЯД)
Управління Держенергонагляду у Вінницькій області
вул. І. Богуна, 5, м. Вінниця, 21010
ел.пошта: vinnytska@sies.gov.ua, оф. вебсайт: sies.gov.ua, код з ЄДРПОУ 42578602

13.11.2023 № 10/14/751-23 на № _____ від _____

ДОВІДКА
про впровадження результатів дисертаційного дослідження
Страхніцького Ярослава Олександровича
на тему «Особливості формування та реалізації державної політики у сфері захисту критичної інфраструктури» на здобуття наукового ступеня доктора філософії зі спеціальності 281 Публічне управління та адміністування

Належна організація роботи Управління Державної інспекції енергетичного нагляду України у Вінницькій області, його ефективна робота й досягнення визначених законодавством завдань забезпечують стале функціонування об'єднаної енергетичної системи країни, сфери теплопостачання та енергетичну безпеку країни. Відповідно, маючи пряме відношення до функціонування окремих об'єктів критичної інфраструктури, адміністрація Управління Державної інспекції енергетичного нагляду України у Вінницькій області розглянула цінність пропозицій підготовлених Страхніцьким Я. О. у дисертаційному дослідженні «Особливості формування та реалізації державної політики у сфері захисту критичної інфраструктури».

Оцінюючи практичну значимість наукових розробок автора, варто відзначити перспективність використання в управлінському процесі на об'єктах критичної енергетичної інфраструктури (які зазнають найбільшого цілеспрямованого руйнування з боку ворога) запропонованого алгоритму ризик-менеджменту та превентивного управління безпекою на принципах стійкості.

Окремі елементи наукових результатів враховано у процесі реалізації державної політики у сфері нагляду (контролю) у галузях електроенергетики та теплопостачання. Зокрема при організації роботи комісій з перевірки знань працівників об'єктів критичної інфраструктури, під час планових перевірок готовності електричних мереж до роботи в кризових умовах та плануванні роботи.

Даною довідкою засвідчуємо, що результати наукового дослідження викладені у дисертаційному дослідженні аспіранта Страхніцького Я. О. прийнято до уваги у діяльності Управління Державної інспекції енергетичного нагляду України у Вінницькій області

Начальник
Управління Держенергонагляду
у Вінницькій області **В'ячеслав КМЕТЮК**

ДЕРЖАВНА ІНСПЕКЦІЯ ЕНЕРГЕТИЧНОГО НАГЛЯДУ УКРАЇНИ
Управління Держенергонагляду у Вінницькій області
УКРАЇНА

СЛУЖБА БЕЗПЕКИ УКРАЇНИ
Управління Служби безпеки України у Вінницькій області
вул. Грушевського, 27, м. Вінниця, 21050, тел. (0432) 53-13-09
www.ssu.gov.ua, e-mail: usbu_vin@ssu.gov.ua, Код ЄДРПОУ 20001473

19.03.2024 № 53/2/52-2101ВІ На № _____ від _____

ДОВІДКА
про впровадження результатів дисертаційного дослідження Страхніцького Ярослава Олександровича на тему «Особливості формування та реалізації державної політики у сфері захисту критичної інфраструктури» на здобуття наукового ступеня доктора філософії зі спеціальності 281 Публічне управління та адміністрування

Спеціалісти Управління Служби Безпеки України у Вінницькій області, розглянувши наукову роботу Страхніцького Я. О. на тему «Особливості формування та реалізації державної політики у сфері захисту критичної інфраструктури», дійшли висновку, що результати досліджень автора мають значну актуальність, оскільки захист критичної інфраструктури є однією з важливих складових безпекової політики України. Йдеться про об'єкти стратегічно важливі для функціонування суспільства, соціально-економічного розвитку та безпеки держави.

Проведені у дисертації дослідження інституційної спроможності національної системи захисту критичної інфраструктури, дозволяють проаналізувати її рівень у розрізі спроможностей структурних, організаційних, технічних систем, зокрема місця у ній Служби Безпеки України та визначити резерви для розвитку навичок і компетенцій на всіх рівнях провадження державної політики у сфері захисту критичної інфраструктури.

На особливу увагу та детальне вивчення перспектив реалізації заслуговують обгрунтовані автором пропозиції залучення представників Служби Безпеки України на основі механізмів державно-приватного партнерства до міжсекторальної взаємодії в сфері захисту критичної інфраструктури. В межах інституційних перетворень у напрямку посилення стійкості критичної інфраструктури автором запропоновано розмежування відповідальності за проєктні загрози для об'єктів критичної інфраструктури та посилення активності у забезпеченні проведення регулярних міжсекторальних навчань із оперативного реагування на надзвичайні ситуації на об'єктах з метою підвищення рівня міжвідомчої взаємодії у формі кластерного підходу.

Перспективність зазначених елементів новизни підтверджено застосуванням окремих результатів дослідження Страхніцького Я. О. при погодженні планів захисту об'єктів критичної інфраструктури I-IV категорії критичності за проектними загрозами національного рівня «Терористичний акт або диверсія».

Даною довідкою засвідчуємо, що результати наукового дослідження викладені у дисертаційному дослідженні аспіранта Страхніцького Я. О. прийнято до уваги у діяльності Управління Служби Безпеки України у Вінницькій області.

Перший заступник начальника Управління **Петро МАЙДАНЮК**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІННИЦЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
імені Михайла Коцюбинського
вул. Острозького, 32, м. Вінниця, 21001, Україна, тел. (0432) 616-620, факс (0432) 612-812, E-mail: info@vspu.edu.ua код ЄДРПОУ 02125094

26.12.2023 № 06/39 на №

ДОВІДКА
про впровадження результатів дисертаційного дослідження Страхніцького Ярослава Олександровича на тему «Особливості формування та реалізації державної політики у сфері захисту критичної інфраструктури» на здобуття наукового ступеня доктора філософії зі спеціальності 281 Публічне управління та адміністрування

Результати дисертаційної роботи Страхніцького Ярослава Олександровича з теми «Особливості формування та реалізації державної політики у сфері захисту критичної інфраструктури» є актуальними в умовах активної трансформації сектору безпеки та інтенсивного реформування системи державного управління в контексті європейського вектору інтеграції.

Оцінюючи значимість наукових розробок автора, варто відзначити перспективність використання наукових напрацювань аспіранта, які використовувалися викладачами кафедри публічного управління та адміністрування в процесі здійснення освітньої діяльності. Зокрема, впроваджувалися елементи теоретичних досліджень аспіранта до розробки навчально-методичних комплексів навчальних дисциплін «Публічне управління та адміністрування у сфері цивільної безпеки» та «Публічне управління національною безпекою».

Відзначимо, що дисертаційне дослідження Страхніцького Я. О. має практичне значення для Вінницького державного педагогічного університету імені Михайла Коцюбинського, оскільки спрямоване на удосконалення професійних компетентностей здобувачів вищої освіти. Аспірантом проаналізовано Стандарт вищої освіти України за спеціальністю 281 Публічне управління та адміністрування СВО бакалавра та відповідну йому освітньо-професійну програму на факультеті права, публічного управління та адміністрування, на основі чого виявлено відсутність серед компетенцій фахівців жодної, яка б передбачала підготовку до управління безпекою критичної інфраструктури. Враховуючи потреби ринку праці у гнучкості системи професійного навчання державних службовців, основні пропозиції аспіранта орієнтовані на удосконалення освітньо-професійної програми «Публічне управління та адміністрування» СВО бакалавра за рахунок доповнення компетентностей здобувачів пунктом «Здатність здійснювати професійну діяльність з урахуванням потреб забезпечення належного захисту об'єктів критичної інфраструктури».

Даною довідкою засвідчуємо, що результати наукового дослідження викладені у дисертаційному дослідженні аспіранта Страхніцького Я. О. прийнято до уваги у науково-педагогічній діяльності Вінницького державного педагогічного університету імені Михайла Коцюбинського, що дозволить посилити якісний розвиток кадрового потенціалу на основі формування відповідних компетентностей у ключових стейкхолдерів, представників державної влади, операторів, експертів та професіоналів відповідальних за формування політики та прийняття рішень у сфері захисту критичної інфраструктури.

Проректор з наукової роботи Алла КОЛОМІЄЦЬ

Євген ГРОМОВ (0432) 61-80-72

ВІННИЦЬКА МІСЬКА РАДА
ДЕПАРТАМЕНТ ЦИВІЛЬНОГО ЗАХИСТУ

Україна, 21050, Вінницька обл., Вінницький район, м. Вінниця, вулиця Соборна, 59,
тел. (0432) 59-50-77, факс: 59-51-45, e-mail: dcp@vmr.gov.ua

10.11.2023 № 27/00/014/69236

на № _____

ДОВІДКА
про впровадження результатів дисертаційного дослідження
Страхніцького Ярослава Олександровича
на тему «Особливості формування та реалізації державної політики у сфері захисту критичної інфраструктури» на здобуття наукового ступеня доктора філософії зі спеціальності 281 Публічне управління та адміністрування

Фахівці Департаменту цивільного захисту Вінницької міської ради, розглянувши наукову роботу Страхніцького Я. О. на тему «Особливості формування та реалізації державної політики у сфері захисту критичної інфраструктури», дійшли висновку, що представлені результати досліджень мають суттєву значущість стосовно теоретичного обгрунтування основ державної політики у сфері захисту критичної інфраструктури в умовах воєнного стану в Україні. Інформативним є аналіз інституційної спроможності складових сучасної системи державної політики у сфері захисту критичної інфраструктури, висновки якого дають можливості визначити резерви для оптимізації процесу протидії загрозам на секторальному та об'єктовому рівні. Надані у дисертаційному дослідженні висновки та пропозиції стосуються положень вітчизняного законодавства у сфері захисту критичної інфраструктури, що стосується регламенту роботи органів, відповідальних за здійснення захисту критичної інфраструктури.

На особливу увагу та детальне вивчення перспектив реалізації заслуговують обгрунтовані автором на основі аналізу закордонного досвіду пропозиції з подальшого розвитку державно-приватного партнерства та міжсекторальної взаємодії в сфері захисту критичної інфраструктури у формі кластерного підходу. Пропозиція передбачає комплекс заходів з підвищення ефективності політики, спрямованої на захист об'єктів критичної інфраструктури, зокрема ризик-менеджмент, комплекс превентивних заходів на основі принципів стійкості та посилення освітньо-наукової складової.

Перспективність зазначених елементів новизни підтверджено застосуванням окремих висновків у розробці програм та планів заходів у сфері цивільного захисту, зокрема спрямованих на захист населення і територій від надзвичайних ситуацій, пов'язаних із об'єктами критичної інфраструктури та запобігання їх виникненню.

Даною довідкою засвідчуємо, що результати наукового дослідження викладені у дисертаційному дослідженні аспіранта Страхніцького Я. О. прийнято до уваги у діяльності Департаменту цивільного захисту Вінницької міської ради.

Директор департаменту **Олег ПАРФІЛОВ**