Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2024. № 8.

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

УДК 35.088.6:[004:007:351.86] (477)

Л. А. Арсенович,

доктор філософії з публічного управління та адміністрування, заступник начальника управління – начальник відділу Департаменту кадрової роботи та управління персоналом, Адміністрація Держспецзв'язку

ORCID ID: https://orcid.org/0000-0001-7081-2838

ПАРАДИГМА ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

L. A. Arsenovych,

PhD in Public Management and Administration, Deputy Head – Head of Division at the HR Management Department of the Administration of the State Service for Special Communication and Information Protection of Ukraine, Derzhspetszviazok

PARADIGM OF CRITICAL INFRASTRUCTURE PROTECTION IN THE NATIONAL SECURITY SYSTEM OF UKRAINE

Повномасштабне вторгнення російської федерації на територію України актуалізували для країни питання захисту критичної інфраструктури, об'єктів та систем важливих для життєдіяльності суспільства і громадськості, та сформували потребу у створенні ефективної та дієвої системи захисту критичної інфраструктури в Україні. Гармонізація національних підходів щодо створення системи захисту критичної інфраструктури з європейськими та євроатлантичними підходами сприятиме

удосконаленню механізмів забезпечення національної безпеки та посилить потенціал України щодо інтеграції до європейського безпекового простору.

Прагнення нашої держави до європейського простору відкриває перед Україною напрям додаткових можливостей та перспектив для скорішого зменшення відставання від провідних країн Європи та світу і для знаходження свого місця у векторній системі європейської та євроатлантичної безпеки.

Як і в інших країнах світу, на сьогодні в Україні функціонують відповідні системи, об'єкти та ресурси, пошкодження або знищення яких нанесе істотний негативний вплив на громадян, суспільство, національну безпеку, державні інституції, а також на публічне управління в цілому. На теперішній час вже почала діяти ціла низка законодавчих, нормативно-правових та організаційно-розпорядчих актів, які визначають повноваження та компетенцію суб'єктів національної системи захисту критичної інфраструктури, а також встановлюють особливості забезпечення охорони та безпечного функціонування зазначених об'єктів і систем. Разом з тим, в Україні й досі відсутній системний підхід на національному рівні, а також відповідний алгоритм щодо управління захистом та безпекою усього комплексу систем, об'єктів та ресурсів, які відносяться до критичної інфраструктури.

У статті розглянуто підґрунтя започаткування поняття «критична інфраструктура», зарубіжний досвід його використання, а також нормативно-правові підстави щодо впорядкування термінології у сфері захисту критичної інфраструктури, у тому числі щодо забезпечення національної безпеки України у зазначеній сфері. Крім цього, запропоновано напрями удосконалення захисту критичної інфраструктури в системі національної безпеки України шляхом впровадження в умовах воєнного стану «моделі взаємодії і координації» для суб'єктів національної системи захисту критичної інфраструктури, яка вказує на необхідність подальшої розбудови державної системи захисту критичної інфраструктури.

The full-scale invasion of Ukraine by the Russian Federation has raised the issue of protecting critical infrastructure, facilities and systems important for the life of society and the public and invoked the need to provide for an effective system of critical infrastructure protection in Ukraine. Harmonization of national approaches to the creation of a critical infrastructure protection system with European and Euro-

Atlantic approaches will help improve national security mechanisms and strengthen Ukraine's potential for integration into the European security space.

Our country's aspirations for the European space open up additional opportunities and prospects for Ukraine to quickly reduce the gap with the leading countries of Europe and the world and to find its place in the vector system of European and Euro-Atlantic security.

As in other countries, Ukraine currently has the systems, facilities and resources, which damage or destruction would considerably affect the citizens, society, national security, government institutions, and public administration overall. To date, a number of legislative, regulatory, organizational and administrative acts have already come into force that define the powers and competence of entities of the national critical infrastructure protection system, as well as outline the nature of ensuring the protection and safe operation of these facilities and systems. At the same time, Ukraine still lacks a systematic approach at the national level, as well as an appropriate algorithm for managing the protection and security of the entire complex of systems, facilities and resources related to critical infrastructure.

The article analyzes the basis for introducing the concept of "critical infrastructure", foreign experience of its use, as well as the legal and regulatory framework for organizing the terminology in the area of critical infrastructure protection, including ensuring Ukraine's national security in this area. In addition, the article proposes ways to improve the protection of critical infrastructure in the national security system of Ukraine by introducing a "model of interaction and coordination" for the entities of the national critical infrastructure protection system under martial law, which indicates the need for further development of the state system of critical infrastructure protection.

Ключові слова: *безпека критичної інфраструктури, державна політика у сфері захисту критичної інфраструктури, критична інфраструктура, національна система захисту критичної інфраструктури, сфера захисту критичної інфраструктури.*

Keywords: *critical infrastructure security, government policy in the area of critical infrastructure protection, critical infrastructure, national system of critical infrastructure protection, critical infrastructure protection.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Сучасні тенденції розвитку інформаційно-комунікаційних технологій спричинили виняткову залежність громадськості та суспільства від послуг та технологій, які надають різні сфери та галузі інфраструктури. Якість та доступність таких послуг (технологій) є одним з основних показників розвитку інфраструктури країни, а забезпечення їх захисту та функціонування є найважливішою складовою національної безпеки розвинених держав.

Але разом із впровадженням нових технологій і відкриттям величезного інформаційного простору з'являються й невідомі до цього моменту проблеми, серед яких слід назвати, зокрема, кібернетичні злочини, правопорушення, що становлять загрозу не лише для окремих громадян, а й для державної безпеки країн (з урахуванням сфери впливу технологій) [1, с. 10].

Збільшення концентрації ресурсів та засобів для захисту інфраструктур різних типів зумовило необхідність послідовного розміщення та класифікації інфраструктурних об'єктів та появи поняття критична інфраструктура.

Зазвичай, до цієї категорії відносять енергетичні та транспортні магістральні мережі, нафто- та газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення мегаполісів, високотехнологічні підприємства та підприємства військово-промислового комплексу, а також центральні органи влади. Тому, першочерговим аспектом стає визначення об'єктів, які є критичними, оцінювання рівня їх важливості для забезпечення постійного функціонування, запобігання виникненню переривань роботи та збоїв в автоматизованих системах, що забезпечують їх роботу [2, с. 28].

Суспільство будь-якої країни потребує надання своєчасних послуг та обслуговування життєдіяльності на протязі всього свого циклу існування. Для цього необхідно створити таку інфраструктуру, яка би забезпечувала постійне і безперебійне функціонування, а також унеможливила різноманітні антропогенні небезпеки і природні явища, які можуть привести до економічних

втрат, екологічних катастроф, а також до збою роботи життєво важливих об’єктів.

Аналіз останніх досліджень і публікацій. Слід підкреслити, що сучасну парадигму захисту критичної інфраструктури в системі національної безпеки України, тим більше в умовах воєнного стану, у теоретичному плані достатньо не вивчено. Цю тезу у своїх роботах підтверджують і сучасні науковці. Так, вчені Гора І.В., головний науковий співробітник науково-організаційного центру Національної академії Служби безпеки України, та Батюк О.В., доцент кафедри політології, управління та державної безпеки Волинського національного університету імені Лесі Українки, у своїй науковій статті зазначають, що порушення функціонування або руйнування об’єктів, систем, мереж або їх частин критичної інфраструктури може призвести до найсерйозніших наслідків для соціальної та економічної сфери держави, негативно вплинути на рівень її обороноздатності та національної безпеки. Науковці дійшли висновку, що захист об’єктів критичної інфраструктури вийшов на загальноєвропейський чи навіть міжконтинентальний формат, а необхідність впровадження національної концепції захисту об’єктів критичної інфраструктури є важливою для модернізації системи національної безпеки України [3, с. 132, 137].

Так само міркують проректор Львівського державного університету внутрішніх справ Франчук В.І., директор Департаменту з питань безпеки, оборони, діяльності органів юстиції та запобігання корупції Секретаріату Кабінету Міністрів України Пригунов П.Я. та заступник декана факультету № 2 Львівського державного університету внутрішніх справ Мельник С.І., які у спільному дослідженні розкривають теоретичні засади функціонування об’єктів критичної інфраструктури, у межах якого основна увага приділена критичному аналізу змісту понять «критична інфраструктура» та «безпека критичної інфраструктури». Посадовці приходять до висновку, що відсутність у країні об’єктів критичної інфраструктури або дестабілізація їхньої діяльності може становити загрозу національній безпеці. У зв’язку з цим формування

національної системи безпеки об’єктів критичної інфраструктури – це обов’язок насамперед влади [4, с. 142, 148].

Питання парадигми захисту критичної інфраструктури в системі національної безпеки України вивчали також начальник кафедри Інституту Управління державної охорони України Київського національного університету імені Тараса Шевченка Павлов Д.М. та професор зазначеної кафедри Микитюк М.А., якими сформульовано й обґрунтовано тезу про те, що розгляд національної безпеки спонукає звернутися до національної ідеї, яка визначає свої національні цінності та інтереси. Офіцери зазначають, що на відміну від попередніх парадигм національної безпеки нова парадигма, крім розгляду безпеки крізь призму захисту буття особи, суспільства та держави, передбачає лікування не якоїсь окремої хвороби, а організму загалом, ставить наголос на боротьбі не з наслідками, а з причинами цієї хвороби. Саме у такому контексті має формуватися політика захисту критичної інфраструктури держави [5, с. 70].

Вищезазначені дослідження ще раз підказують, що для формування доцільних структур управління у сфері захисту критичної інфраструктури необхідно зрозуміти стан і складність реальних проблем України в період повномасштабного вторгнення російської федерації і врахувати їх при формуванні майбутньої державної політики у зазначеній сфері.

Формулювання цілей статті (постановка завдання). Метою статті є проведення аналізу та вивчення стану впровадження державної політики у сфері захисту критичної інфраструктури в контексті розбудови національної системи захисту критичної інфраструктури.

Виклад основного матеріалу дослідження. Потреба постійно захищати критичну інфраструктуру від усіх видів фізичних загроз і небезпек, в тому числі кіберзагроз, обумовлює необхідність побудови системи управління критичною інфраструктурою, спрямованої на забезпечення її захисту, безпеки та стійкості з залученням до відповідних зусиль і заходів усього суспільства:

від окремих громадян, місцевих громад, суб'єктів господарювання до органів державної влади [6, с. 64].

Останніми десятиріччями у світі спостерігається стійка тенденція до зростання кількості надзвичайних ситуацій та подій різного походження. Це вказує на неспроможність здійснення прогнозування в сучасних державних механізмах управління в сфері безпеки та їх нездатність попереджати надзвичайні ситуації і події комплексного характеру. Наприклад: терористична атака на території США у 2001 році, ураган Катріна в США у 2005 році, різноманітні землетруси і цунамі, технологічні аварії та збройні агресії.

Захист критичної інфраструктури як безпековий напрям був започаткований у США ще у період «холодної війни», а на початку нинішнього століття став активно розвиватися у провідних країнах світу як відповідь на різке зростання терористичних загроз. Цей безпековий напрям є пріоритетним і для таких міжнародних структур, як ЄС і НАТО, оскільки поруч з тими перевагами та благами, які несуть з собою процеси глобалізації та інформатизації, посилюється економічна, фінансова, технологічна, ресурсна взаємопов'язаність та взаємозалежність між окремими державами, їх об'єднаннями, а також між регіонами світу, що робить сучасне суспільство дуже вразливим до загроз, особливо тих, що спрямовані на «вузлові» пункти згаданих взаємозв'язків [7, с. 3–4].

Поняття «критична інфраструктура» було введено у середині 90-х років XX століття як в нормативно-правовому напрямку, так і на рівні міжнародного та дипломатичного спілкування, а також в науковому та діловому колах. Причому прикметник «критичний» почав з'являтися у документах та нормативно-правових актах у поєднанні із такими поняттями як «стан» та «ситуація», що сигналізує про запровадження низки нововведень нормативного та організаційного характеру в систему забезпечення національної безпеки України.

Слід визнати, що дана дефініція постійно трансформується та видозмінюється, а також має одну спільну рису – постійний зв'язок із

державними та приватними об’єктами, які в тій чи іншій мірі впливають на рівень національної безпеки країни й підтримують життєвоважливі важливі функції держави у суспільстві.

Флагманом у інтеграції в державну політику концепції захисту критичної інфраструктури можна вважати США. Саме у цій країні вперше було офіційно визнано предикат «критична інфраструктура» та остаточно його утверджено 23.10.2001 р., законом USA Patriot Act. Так, законодавством США 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». 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). Представлене визначення однозначно підтверджує факт, що безпека критичної інфраструктури є детермінантою національної безпеки [8].

Необхідно також розглянути досвід Європейських країн, якими теж здійснено аналіз підходів до визначення дефініції критичної інфраструктури як об’єкту державного управління. Так, директива Ради Європейського Союзу від 8 грудня 2008 року № 2008/114/ЕС «З ідентифікації та позначення критично важливих європейських інфраструктур та оцінки необхідності покращення їх захисту» встановила процедуру ідентифікації та позначення критично важливих європейських інфраструктур, а також загальний підхід до оцінки необхідності покращення захисту таких інфраструктур з метою сприяння захисту людей.

Директива визначила, що «критична інфраструктура» означає актив, систему або їх частину, розташовані в державах-членах, які необхідні для підтримки життєво важливих суспільних функцій, здоров’я, безпеки, захисту, економічного чи соціального благополуччя людей, і порушення чи руйнування яких може мати значні наслідки для держави-члена в результаті нездатності

підтримувати ці функції. Разом з тим, «Європейська критична інфраструктура» або «ECI» означає критично важливу інфраструктуру, розташовану в державах-членах, порушення або руйнування якої вплине як мінімум на дві держави Європейського Союзу.

У Німеччині під поняттям «критична інфраструктура» розуміють організації чи об'єкти, що мають важливе значення для національної спільноти, вихід з ладу чи пошкодження яких може призвести до тривалих перебоїв у постачанні, значних порушень громадської безпеки чи інших драматичних наслідків. При цьому план реалізації критичних інфраструктур є співпрацею між операторами критичних інфраструктур, їх асоціаціями та державними установами. Основною метою плану є підтримка постачання критично важливих інфраструктурних послуг у Німеччині. Забезпечення захисту критично важливих інфраструктур є основним завданням державних та корпоративних заходів безпеки. Метою Федерального управління цивільного захисту та допомоги за стихійних лих є сприяння максимально можливому захисту критично важливої інфраструктури і, таким чином, забезпечення постачання населення [9].

А у Республіці Польща під поняттям «критична інфраструктура» розуміють систему функціонально пов'язаних об'єктів, у тому числі будівель, пристроїв, установок і послуг, що мають вирішальне значення для безпеки держави та її громадян, та які забезпечують ефективне функціонування органів влади, а також установи та приватних підприємців. При цьому, критична інфраструктура включає системи енергопостачання, енергетичної сировини та палива, комунікації, мережі ІКТ, фінансові мережі, постачання продуктів харчування, водопостачання, охорону здоров'я, транспорт, порятунок, а також забезпечення безперервності діяльності державного управління [10].

У Великобританії національну інфраструктуру представляють об'єкти, системи, сайти, інформація, люди, мережі та процеси, які необхідні для функціонування країни і від яких залежить повсякденне життя. Вона також включає деякі функції, сайти та організації, які не є критично важливими для

підтримки основних послуг, але які потребують захисту через потенційну небезпеку для населення (наприклад, цивільні ядерні та хімічні об'єкти). В країні існує 13 національних інфраструктурних секторів, а саме: Уряд, комунікації, енергія, фінанси, здоров'я, транспорт, вода, захист, їжа, космос, хімікати, громадянська ядерна енергетика та аварійні служби. Крім цього, у кожному секторі є один або кілька провідних державних департаментів (LGD), які відповідають за сектор та забезпечують захист та безпеку критично важливих активів [11].

Проведений аналіз засвідчує, що зазначені дефініції об'єднують такі риси як відповідальність та безпека громадян, суспільства й держави в цілому. Із вищенаведених визначень видно, що відмінності у терміні «критична інфраструктура» в різних країнах не суттєві, відображаючи при цьому національну специфіку сфери застосування терміну, а також особливості їх нормативно-правових систем.

Впровадження захисту критичної інфраструктури в країні є амбіційним завданням, вирішення якого потребує як матеріальних ресурсів, так і ґрунтовної науково-технічної та експертної підтримки, кадрових ресурсів, і мабуть ключовий момент – політичної волі. Відносно останнього потрібно сказати, що країна, яка виявиться нездатною організувати ефективно захист власної критичної інфраструктури не тільки закриває собі шлях розвитку, а приречена на загибель. Без сумніву захист критичної інфраструктури може розглядатися як комплексна наукова проблема. Результати досліджень мають забезпечити вирішення питань нормативно-правового, організаційного, методологічного, технологічного, інженерного, кадрового забезпечення [12, с. 157].

Питання про впорядкування термінології у сфері захисту критичної інфраструктури, у тому числі щодо забезпечення національної безпеки України у зазначеній сфері, на порядок дений поставлено тільки останнім часом. І основним документом із зазначеного питання є Закон України від 16 листопада 2021 року № 1882-IX «Про критичну інфраструктуру» [13], який визначає правові та організаційні засади створення та функціювання національної

системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки. Законом визначено, що критична інфраструктура – це сукупність об'єктів критичної інфраструктури, а національна система захисту критичної інфраструктури – це сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади, органів місцевого самоврядування, операторів критичної інфраструктури, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури. При цьому безпека критичної інфраструктури – це стан захищеності критичної інфраструктури, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури.

Державна політика у сфері захисту критичної інфраструктури направлена на формування комплексу ресурсних, організаційних, методологічних, інженерно-технічних, нормативно-правових та інформаційно-аналітичних заходів, спрямованих на:

– визначення суб'єктів національної системи захисту критичної інфраструктури та законодавчих вимог до принципів, стратегічних завдань, пріоритетів та підходів щодо захисту критичної інфраструктури;

– створення умов спрямованих на ефективне зниження і контроль за ризиками безпеки та швидке відновлення надання життєво важливих функцій та послуг у разі реалізації загроз і порушення функціонування критичної інфраструктури;

– запровадження державно-приватного партнерства, а також взаємодію суб'єктів господарювання та населення з питань забезпечення захисту та стійкості критичної інфраструктури;

– створення системи раннього виявлення загроз критичній інфраструктурі, а також на забезпечення міжнародного співробітництва у сфері захисту критичної інфраструктури;

– визнання необхідності забезпечення безпеки та стійкості критичної інфраструктури.

Разом з тим, державна політика у сфері захисту критичної інфраструктури спрямовує свій напрям на запобігання проявам несанкціонованого втручання в безпеку об’єктів критичної інфраструктури шляхом:

– розроблення нормативно-правової бази з питань забезпечення безпеки об’єктів критичної інфраструктури, державних цільових програм із захисту критичної інфраструктури, заходів з контролю за ризиками безпеки, виявлення, запобігання та ліквідації наслідків інцидентів безпеки на об’єктах критичної інфраструктури, а також методології аналізу результативності державної політики у сфері захисту критичної інфраструктури;

– встановлення вимог із забезпечення безпеки об’єктів критичної інфраструктури, а також проведення аналізу викликів та загроз, що впливають на стійкість критичної інфраструктури;

– підготовки, перепідготовки, підвищення кваліфікації та тренування працівників національної системи захисту критичної інфраструктури;

– запобігання проявам несанкціонованого втручання в її функціонування, а також шляхом попередження кризових ситуацій, що порушують безпеку критичної інфраструктури;

– забезпечення взаємодії національної системи захисту критичної інфраструктури з європейськими та євроатлантичними системами.

Крім цього, до основних принципів функціонування національної системи захисту критичної інфраструктури належать безпека, захист та охорона інформації з обмеженим доступом, державно-приватне партнерство, координованість, єдність методологічних засад, а також міжнародне співробітництво.

Необхідно зазначити, що до життєво важливих функцій (послуг), порушення яких призводить до негативних наслідків для національної безпеки України, належать інформаційні та фінансові послуги, правопорядок, електронні комунікації, дослідницька та космічна діяльність, оборона, державна безпека, продовольче та транспортне забезпечення, фармацевтична та хімічна

промисловість, цивільний захист населення, водопостачання (водовідведення), охорона здоров'я, стале функціонування біолабораторій, енергозабезпечення, а також урядування та надання найважливіших публічних (адміністративних) послуг.

Національна система захисту критичної інфраструктури, відповідно до Закону України «Про критичну інфраструктуру», має:

– загальнодержавний рівень, управління на якому здійснюється Кабінетом Міністрів України, Державною службою захисту критичної інфраструктури та забезпечення національної системи стійкості України, що утворена постановою Кабінету Міністрів України від 12 липня 2022 року № 787 [14] (а під час дії воєнного стану – Держспецзв'язку, що передбачено Законом України від 18 жовтня 2022 року № 2684-IX [15]), органами державної влади, іншими центральними органами виконавчої влади та Національним банком України;

– регіональний та галузевий рівні, управління на яких здійснюється центральними та місцевими органами виконавчої влади;

– місцевий рівень, управління на якому здійснюється місцевими органами виконавчої влади та органами місцевого самоврядування;

– об'єктовий рівень, управління на якому здійснюється оператором критичної інфраструктури.

Суб'єктами національної системи захисту критичної інфраструктури є:

– Кабінет Міністрів України, Апарат Ради національної безпеки і оборони України, Центральна виборча комісія та Національний банк України;

– Збройні Сили України, інші військові формування, Служба безпеки України, Адміністрація Держспецзв'язку, ДСНС, правоохоронні та розвідувальні органи, а також суб'єкти оперативно-розшукової та контррозвідувальної діяльності;

– Національна комісія з цінних паперів та фондового ринку, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації,

Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг та Фонд державного майна України;

– міністерства, інші центральні органи виконавчої влади, секторальні та функціональні органи, місцеві органи виконавчої влади, органи місцевого самоврядування, оператори критичної інфраструктури, підприємства, установи та організації, які провадять діяльність, пов'язану із забезпеченням безпеки та стійкості критичної інфраструктури.

Серед актів Уряду, які розкривають питання забезпечення національної безпеки України у сфері захисту критичної інфраструктури, слід виділити:

– Концепцію створення державної системи захисту критичної інфраструктури (розпорядження Кабінету Міністрів України від 6 грудня 2017 року № 1009-р [16]), положення якої, у тому числі, направлені на створення державної системи захисту критичної інфраструктури (як комплексу організаційних, нормативно-правових, інженерно-технічних, наукових та інших заходів) та спрямовані на забезпечення безпеки та стійкості критичної інфраструктури;

– Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури (постанова Кабінету Міністрів України від 19 червня 2019 року № 518 [17]), які затвердили поняття «системи інформаційної безпеки» (сукупність заходів, а також засобів і методів захисту інформації, які впроваджуються на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури) та «політики інформаційної безпеки» (політика, що визначає підхід відповідного підприємства (установи та організації), яке віднесено до об'єктів критичної інфраструктури);

– Порядок формування переліку об'єктів критичної інформаційної інфраструктури (постанова Кабінету Міністрів України від 9 жовтня 2020 року № 943 [18]), який визначає механізм формування національного та секторальних переліків об'єктів критичної інформаційної інфраструктури та затвердив поняття безпеки об'єкта критичної інфраструктури, під яким мається на увазі стан захищеності об'єкта критичної інфраструктури, за якого

забезпечується функціональність і безперервність його роботи та/або можливість надання ним основних послуг;

– Порядок проведення моніторингу рівня безпеки об’єктів критичної інфраструктури (постанова Кабінету Міністрів України від 22 липня 2022 року № 821 [19]), який передбачає здійснення контролю за ризиками безпеки та удосконалення заходів, які здійснюються для забезпечення безпеки та стійкості об’єкта критичної інфраструктури, а також визначає перспективи подальшого функціонування і розвитку національної системи захисту критичної інфраструктури;

– Порядок проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури (постанова Кабінету Міністрів України від 24 березня 2023 року № 257 [20]), який визначає механізм організації та проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури та вимоги до його проведення;

– Порядок ведення Реєстру об’єктів критичної інфраструктури, включення таких об’єктів до Реєстру, доступу та надання інформації з нього (постанова Кабінету Міністрів України від 28 квітня 2023 року № 415 [21]), який визначає процедури формування і ведення Реєстру об’єктів критичної інфраструктури, відповідно до якого забезпечується оброблення інформації про критичну інфраструктуру, щодо якої встановлюються особливі вимоги із забезпечення її безпеки та стійкості;

– Порядок розроблення та погодження паспорта безпеки на об’єкт критичної інфраструктури (постанова Кабінету Міністрів України від 4 серпня 2023 року № 818 [22]), який визначає вимоги до розроблення оператором критичної інфраструктури паспорта безпеки на об’єкт критичної інфраструктури та його складових, а також механізм його погодження секторальними і функціональними органами у сфері захисту критичної інфраструктури;

– Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури (розпорядження Кабінету Міністрів України від 19 вересня 2023 року № 825-р [23]), який затвердив строки:

проведення моніторингу рівня безпеки об’єктів критичної інфраструктури;

підготовки пропозицій до проєктів документів стратегічного планування щодо забезпечення безпеки та стійкості критичної інфраструктури, здійснення її захисту;

розроблення, оновлення та забезпечення виконання об’єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, правил управління ризиками безпеки, планів локалізації та ліквідації наслідків аварій, а також заходів щодо забезпечення кіберзахисту;

затвердження секторальних планів проведення моніторингу рівня безпеки об’єктів критичної інфраструктури;

розроблення та затвердження місцевих програм забезпечення безпеки та стійкості критичної інфраструктури.

Продовжуючи дослідження слід актуалізувати увагу на непорушності базових принципів і фундаментальних засад забезпечення національної безпеки у сфері захисту критичної інфраструктури, що має непересічне значення для будь-якої суверенної держави світу, у тому числі для України. На теперішній час, в умовах військової агресії російської федерації на території Україні, це питання номер один у сфері публічного управління.

Згідно Закону України «Про національну безпеку України» [24] національна безпека – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз, а національні інтереси України – це 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.

Відповідно до Закону державна політика у сферах національної безпеки і оборони спрямована на захист людини і громадянина, суспільства, держави та території, у тому числі навколишнього природного середовища – від надзвичайних ситуацій. При цьому, основними принципами, що визначають порядок формування державної політики у сферах національної безпеки і оборони, є верховенство права, законність та прозорість, дотримання норм міжнародного права, а також розвиток сектору безпеки і оборони як основного інструменту реалізації державної політики у сферах національної безпеки і оборони.

Враховуючи зазначене можна зробити висновок, що акцент забезпечення національної безпеки спрямований на забезпечення державної, інформаційної, воєнної, економічної, зовнішньополітичної, екологічної безпеки, безпеки критичної інфраструктури, а також кібербезпеки України, а фундамент державної політики у сфері захисту критичної інфраструктури будується на трьох складових – національних інтересах, безпеці та захисті.

Разом з тим, враховуючи положення вищезазначених нормативно-правових актів, необхідно відзначити що безпека критичної інфраструктури забезпечується шляхом: формування системи захисту критичної інфраструктури, а також суб'єктного складу державної політики у сфері захисту критичної інфраструктури; удосконалення інституційного забезпечення; створення відповідного реєстру (об'єктів критичної інфраструктури); визначення загроз для об'єктів критичної інфраструктури; ідентифікації секторів критичної інфраструктури; вжиття відповідних заходів із ліквідації наслідків руйнувань об'єктів критичної інфраструктури.

Необхідно зазначити, що у теорії публічного управління не існує універсального стандарту, який би встановлював порядок організації захисту об'єктів критичної інфраструктури. Таким чином, Офіс Президента України, Верховна Рада України або Уряд при прийнятті будь якого рішення щодо поліпшення або відновлення системи критичної інфраструктури має враховувати ту чи іншу ситуацію або стан в країні, а також такі показники як:

стан економіки, культури нації та суспільно-політичної ситуації, основи конституційного ладу, загальну інституційну практику публічного управління, а також спектр критичних загроз та ризиків.

На сьогодні, сучасні вчені розглядають парадигму захисту критичної інфраструктури в системі національної безпеки України як варіанти двох моделей, а саме:

– «модель добровільного підходу», яка передбачає політико-лібералізаційне управління, добровільне дотримання стандартів, саморегулювання, а також самостійне формування та реалізацію політики захисту критичної інфраструктури;

– «модель відповідальності», яка передбачає обов'язкове дотримання нормативно-правових актів, а також заходи впливу на операторів об'єктів критичної інфраструктури за порушення у сфері безпеки.

Необхідно зазначити, що більшість країн не застосовують зазначені моделі у базовій формі, а комбінують їх разом. Так, вчений Бобро Д.Г., який вивчав світовий досвід розбудови парадигми державної політики захисту критичної інфраструктури, у своїй роботі виокремлює такі основоположні кроки у цьому напрямі, а саме: розробку нормативно-правової бази, методологічних підходів до формування переліку об'єктів критичної інфраструктури, планів оперативного реагування; визначення координуючого органу; забезпечення підготовки кваліфікованих кадрів у сфері захисту критичної інфраструктури; організацію оперативної співпраці; розвиток державно-приватного партнерства [25].

Разом з тим, на нашу думку, зазначені моделі за своєю суттю можуть бути дієвими та ефективними тільки в умовах мирного часу, а значить, в умовах воєнного стану, не можуть «стояти на чолі» парадигми захисту критичної інфраструктури в системі національної безпеки України. В умовах воєнного стану, введеного Указом Президента України від 24 лютого 2022 року № 64/2022 «Про введення воєнного стану в Україні» [26], затвердженим Законом України «Про затвердження Указу Президента України «Про введення

воєнного стану в Україні» [27], такі моделі не можуть в повній мірі забезпечувати єдину загальнодержавну систему захисту критичної інфраструктури, методологію проведення оцінки загроз критичній інфраструктурі, державно-приватне партнерство у сфері захисту критичної інфраструктури, а також достатній рівень міжнародного співробітництва у зазначеній сфері.

Натомість, удосконалення захисту критичної інфраструктури в системі національної безпеки України шляхом впровадження в умовах воєнного стану «моделі взаємодії і координації» для суб'єктів національної системи захисту критичної інфраструктури надало би змогу забезпечити:

– у сфері оборони:

загальнодержавні заходи живучості об'єктів критичної інфраструктури, національної економіки, а також публічного управління в умовах воєнного стану;

підготовку органів державної влади, військового управління, об'єктів критичної інфраструктури, національної економіки, а також населення до дій в особливий період;

проведення заходів щодо розвитку об'єктів критичної інфраструктури, системи зв'язку, транспорту, шляхів, а також території держави до оборони;

готовність органів державної влади, органів місцевого самоврядування, а також єдиної державної системи цивільного захисту об'єктів критичної інфраструктури до виконання завдань цивільного захисту в особливий період;

– у сфері кіберзахисту:

координацію суб'єктів кіберзахисту під час здійснення заходів щодо забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури;

кіберзахист інформаційно-телекомунікаційних систем, що обробляють національні електронні інформаційні ресурси, комунікаційних систем та об'єктів критичної інформаційної інфраструктури;

створення систем управління ризиками інформаційної безпеки на об'єктах критичної інфраструктури;

розвиток та постійне вдосконалення систем кіберзахисту об’єктів критичної інфраструктури з урахуванням результативності та ефективності процесів, що виконуються в рамках впровадження системи інформаційної безпеки на об’єктах критичної інфраструктури;

– у сфері мобілізаційної підготовки та мобілізації:

бронювання військовозобов’язаних, які працюють або проходять службу на підприємствах, в установах і організаціях, які є критично важливими для забезпечення потреб Збройних Сил України та інших військових формувань;

функціонування економіки та життєдіяльність населення в особливий період;

– у сфері грошово-кредитної політики:

формування та реалізацію державної політики у сфері захисту критичної інфраструктури щодо банків;

формування та ведення переліку об’єктів критичної інфраструктури, а також реєстру об’єктів критичної інформаційної інфраструктури у банківській системі України;

– у сфері місцевого самоврядування: необхідні заходи щодо захисту критичної інфраструктури, відновлення функціонування важливих державних об’єктів національної економіки, об’єктів критичної інфраструктури та об’єктів, які забезпечують життєдіяльність населення;

– у сфері хімічної безпеки: запобігання вчиненню терористичних актів з використанням небезпечних хімічних речовин, диверсій у суб’єктів господарювання хімічної промисловості та на об’єктах критичної інфраструктури;

– у сфері електронних комунікацій: цілісність і безпеку мереж електронних комунікацій, а також об’єктів критичної інформаційної інфраструктури;

– у сфері електричної енергії: безпеку критичної енергетичної інфраструктури та добробут населення, виведення з ладу або руйнування яких матиме суттєвий вплив на національну безпеку та оборону, а також на

навколишнє природне середовище та може призвести до значних фінансових збитків і людських жертв.

Крім цього, введення вищезазначеної моделі для захисту критичної інфраструктури в системі національної безпеки України надало би змогу реалізувати:

– створення, впровадження, розвиток та забезпечення функціонування національної системи захисту критичної інфраструктури;

– відповідні пропозиції суб'єктів національної системи захисту критичної інфраструктури щодо формування та ведення реєстру об'єктів критичної інфраструктури;

– проведення оцінки захищеності об'єктів критичної інфраструктури, а також їх аналізу та оцінювання загального стану;

– координацію секторальних органів, а також підготовку пропозицій до проєктів стратегічних документів щодо забезпечення безпеки та стійкості;

– створення бази даних щодо загроз і вразливостей критичній інфраструктурі;

– державні цільові програми із захисту критичної інфраструктури, а також комплекс заходів з контролю за ризиками безпеки на об'єктах критичної інфраструктури;

– обов'язкові вимоги із забезпечення безпеки об'єктів критичної інфраструктури, а також взаємодію національної системи захисту критичної інфраструктури з відповідними європейськими та євроатлантичними міжнародними системами.

Продовжуючи дослідження необхідно зазначити, що державна політика у сфері захисту критичної інфраструктури, в умовах воєнного стану, потребує подальшого вдосконалення шляхом:

– впровадження новітніх наукових розробок у сфері безпеки об'єктів критичної інфраструктури;

– забезпечення безпеки критичної інфраструктури за рахунок підтримки міжнародних партнерів;

– поетапного введення для суб'єктів національної системи захисту критичної інфраструктури «моделі взаємодії і координації».

Із зазначеною думкою погоджується старший дослідник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України Мельник Д.С., який у своїй статті висвітлює сучасні проблемні питання захисту критичної інфраструктури України, актуальні загрози її безпеки та потреби організації належної протидії в умовах воєнного стану. Науковець зазначає, що в умовах повномасштабної російської військової агресії перед державою постають нові завдання, спрямовані на протидію загрозам і викликам, захист критичної інфраструктури від знищення/пошкодження. При цьому, важливим елементом алгоритму вирішення вказаних завдань нині вбачається формування базової моделі загроз для об'єктів критичної інфраструктури, що має включати взаємопов'язані моделі об'єкта, обстановки та порушника [28, с. 248].

В цьому ж напрямку досліджував зазначене питання науковець Страхніцький Я.О., який у своїй статті аналізує особливості державної політики у сфері захисту критичної інфраструктури в умовах воєнного стану. Автор констатує, що військове вторгнення військ російської федерації в Україну причинило ряд складних випробувань державної політики, однією із основних – ефективність забезпечення захисту критичної інфраструктури. В таких умовах виникає нагальна потреба розробки стратегії протидії. Для подолання даної дилеми Страхніцький Я.О. вносить пропозицію розробки концепції кластерного підходу до забезпечення захисту та стійкості критичної інфраструктури в умовах воєнного стану в Україні. Головна ідея даного концепту передбачає створення навколо важливих інфраструктурних об'єктів кластерів стійкості критичної інфраструктури, які забезпечуватимуть синергію безпекових заходів реалізованих в межах співпраці державних інститутів влади з інфраструктурними об'єктами та їх стейкхолдерами [29, с. 168].

Проблему розбудови сфери захисту критичної інфраструктури в умовах воєнного стану розглядали також старший науковий співробітник сектору

промислової політики та інноваційного розвитку відділу промислової політики та енергетичної безпеки Науково-дослідного центру індустріальних проблем розвитку Національної академії наук України Трушкіна Н.В. та директор видавничої групи «Наукові перспективи» Жукова І.В. Науковці дійшли до висновку, що задля ефективної відбудови та модернізації критичної інфраструктури в Україні доцільно застосовувати передовий досвід різних країн світу шляхом розроблення відповідної стратегії розвитку критичної інфраструктури та плану її реалізації, у якому визначити фінансові інструменти (безоплатна фінансова допомога міжнародних фінансових і неурядових організацій, грантові кошти, позики, краудінвестинг, публічно-приватне партнерство, репарація тощо) та інститути (Фонд відновлення майна та зруйнованої інфраструктури, Фонд відновлення та трансформації економіки, Агенція з гарантування інвестицій, Багатосторонній трастовий фонд для спрямування донорської підтримки Україні, Цільовий фонд підтримки, відновлення, відбудови та реформування України) [30, с. 380–381].

Отже, на сучасному етапі реформування національної системи захисту критичної інфраструктури слід вважати за доцільне подальшу розбудову державної системи захисту критичної інфраструктури на основі існуючих систем захисту та кризового реагування. Практичної реалізації даної пропозиції можна досягнути на основі розроблення та впровадження «моделі взаємодії і координації», що передбачає, зокрема, узгодження питань щодо забезпечення:

– дієвої та ефективної взаємодії представників органів виконавчої влади, реального сектору економіки та громадськості у формуванні та реалізації єдиної державної політики у сферах забезпечення захисту національних інтересів України та об’єктів критичної інфраструктури;

– координації секторальних органів у підготовці пропозицій до реалізації стратегічних документів у сфері забезпечення національної безпеки України, а саме: Стратегії національної безпеки України, Стратегії кібербезпеки України та Стратегії громадської безпеки та цивільного захисту України.

Висновки та перспективи подальших розвідок у даному напрямі. Враховуючи зазначені висновки можна стверджувати, що перед публічним управлінням у сфері захисту критичної інфраструктури постають такі завдання як: формування та реалізація державної політики щодо забезпечення безпеки населення та захист об'єктів критичної інфраструктури; розвиток державно-приватного партнерства; формування нових інститутів у сфері оборони; розвиток громадських інститутів у зазначеній сфері, а також забезпечення безпеки регіонів України та мирних умов.

Література

1. Арсенович Л. А. Сутність кібербезпеки як напряму вироблення державної політики цифрового розвитку. *Ефективність державного управління.* 2021. № 3-4. С. 9–21.
2. Щербак Л. Метод визначення рівня важливості об'єктів критичної інформаційної інфраструктури в галузі цивільної авіації. *Безпека інформації.* 2017. № 1. С. 27–38.
3. Гора І. В. Окремі питання захисту об'єктів критичної інфраструктури: зарубіжний досвід. *Соціально-правові студії.* 2021. № 1 (11). С. 132–139.
4. Франчук В. І. Безпека об'єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. *Соціально-правові студії.* 2021. № 3 (13). С. 142–148.
5. Павлов Д. М. Правові та організаційні засади забезпечення захисту критичної інфраструктури у контексті формування нової безпекової парадигми України. *Честь і закон.* 2020. № 4 (75). С. 69–77.
6. Мельничук О. Управління критичною інфраструктурою: модель та її впровадження. *Актуальні проблеми державного управління.* 2020. № 1(81). С. 64–74.
7. Бірюков Д. С. Зелена книга з питань захисту критичної інфраструктури в Україні / Д. С. Бірюков. *Дмитро Бірюков*: Зб. мат-лів міжнар. експерт. нарад /

упоряд., С.І. Кондратов; за заг. ред. О. М. Суходолі. – К. : НІСД, 2015. 176 с.

8. Особливості сучасної державної політики у сфері захисту критичної інфраструктури в умовах війни в Україні. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/download/293/8196/17091-1?inline=1 (дата звернення: 17.07.2024).

9. National Strategy for Critical Infrastructure Protection (CIP Strategy). URL: https://www.kritis.bund.de (дата звернення: 17.07.2024).

10. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. URL: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20070890590/U/D20070590Lj.pdf (дата звернення: 17.07.2024).

11. Critical National Infrastructure. URL: https://www.npsa.gov.uk/critical-national-infrastructure-0 (дата звернення: 17.07.2024).

12. 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.

13. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. Дата оновлення: 17.07.2024. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 17.07.2024).

14. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України : постанова Кабінету Міністрів України від 12.07.2022 р. № 787. Дата оновлення: 17.07.2024. URL: https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text (дата звернення: 17.07.2024).

15. Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України : Закон України від 18.10.2022 р. № 2684-IX. Дата оновлення: 17.07.2024. URL: https://zakon.rada.gov.ua/laws/show/2684-20#Text (дата звернення: 17.07.2024).

16. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : розпорядження Кабінету Міністрів України від 06.12.2017 р. № 1009-р. Дата оновлення: 17.07.2024. URL:

https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (дата звернення: 17.07.2024).

17. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури : постанова Кабінету Міністрів України від 19.06.2019 р. № 518. Дата оновлення: 17.07.2024. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 17.07.2024).

18. Деякі питання об’єктів критичної інформаційної інфраструктури : постанова Кабінету Міністрів України від 09.10.2020 р. № 943. Дата оновлення: 17.07.2024. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text (дата звернення: 17.07.2024).

19. Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури : постанова Кабінету Міністрів України від 22.07.2022 р. № 821. Дата оновлення: 17.07.2024. URL: https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#Text (дата звернення: 17.07.2024).

20. Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури : постанова Кабінету Міністрів України від 24.03.2023 р. № 257. Дата оновлення: 17.07.2024. URL: https://zakon.rada.gov.ua/laws/show/257-2023-%D0%BF#Text (дата звернення: 17.07.2024).

21. Про затвердження Порядку ведення Реєстру об’єктів критичної інфраструктури, включення таких об’єктів до Реєстру, доступу та надання інформації з нього : постанова Кабінету Міністрів України від 28.04.2023 р. № 415. Дата оновлення: 17.07.2024. URL: https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text (дата звернення: 17.07.2024).

22. Деякі питання паспортизації об’єктів критичної інфраструктури : постанова Кабінету Міністрів України від 04.08.2023 р. № 818. Дата оновлення: 17.07.2024. URL: https://zakon.rada.gov.ua/laws/show/818-2023-%D0%BF#Text

(дата звернення: 17.07.2024).

23. Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури : розпорядження Кабінету Міністрів України від 19.09.2023 р. № 825-р. Дата оновлення: 17.07.2024. URL: https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text (дата звернення: 17.07.2024).

24. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. Дата оновлення: 17.07.2024. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 17.07.2024).

25. 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 (дата звернення: 17.07.2024).

26. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 р. № 64/2022. Дата оновлення: 17.07.2024. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text (дата звернення: 17.07.2024).

27. Про затвердження Указу Президента України «Про введення воєнного стану в Україні» : Закон України від 24.02.2022 р. № 2102-IX. Дата оновлення: 17.07.2024. URL: https://zakon.rada.gov.ua/laws/show/2102-20#Text (дата звернення: 17.07.2024).

28. Мельник Д. С. Побудова моделі загроз національній критичній інфраструктурі України як основа забезпечення її безпеки та стійкості. *Вісник Харківського національного університету внутрішніх справ*. 2024. № 1(1). С. 237–250.

29. 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.

30. Трушкіна Н. В. Економічне забезпечення організації і функціонування критичної інфраструктури. *Успіхи і досягнення у науці*. 2024. № 1. С. 372–383.

References

1. Arsenovych, L.A. (2021), “The essence of cyber security as a direction of development of the state policy of digital development”, *Efektyvnist derzhavnoho upravlinnia*, vol. 3-4, pp. 9–21.

2. Shcherbak, L. Hnatyuk, S. Sydorenko, V. and Shakhoval, O. (2017), “The method of determining the level of importance of objects of critical information infrastructure in the field of civil aviation”, *Bezpeka informatsii*, vol. 23, pp. 27–38.

3. Gora, I.V. and Batiuk, O.V. (2021), “Separate issues of protection of critical infrastructure objects: foreign experience”, *Sotsialno-pravovi studii*, vol. 1 (11), pp. 132–139.

4. Franchuk, V.I. Prygunov, P.Ya. and Melnyk, S.I. (2021), “Security of critical infrastructure facilities in Ukraine: organizational and normative problems and approaches”, *Sotsialno-pravovi studii*, vol. 3 (13), pp. 142–148.

5. Pavlov, D.M. and Mykytyuk, M.A. (2020), “Legal and organizational principles of ensuring the protection of critical infrastructure in the context of the formation of a new security paradigm of Ukraine”, *Chest i zakon*, vol. 4 (75), pp. 69–77.

6. Melnychuk, O. (2020), “Management of critical infrastructure: a model and its implementation”, *Aktualni problemy derzhavnoho upravlinnia*, vol. 1(81), pp. 64–74.

7. Biryukov, D.S. and Kondratov, S.I. (2015), “Green book on critical infrastructure protection in Ukraine”, *Zb. mat-liv mizhnar. ekspert. narad* [Coll. Maths International expert. meeting], *NISD*, pp. 176.

8. Strakhnits'kyj, Ya. O. (2024), “Features of modern state policy in the field of protection of critical infrastructure in the conditions of war in Ukraine”, available at: http://baltijapublishing.lv/omp/index.php/bp/catalog/download/293/8196/17091-1?inline=1 (Accessed 17 July 2024).

9. Federal Office for Civil Protection (2024), “National Strategy for Critical Infrastructure Protection (CIP Strategy)”, available at: https://www.kritis.bund.de (Accessed 17 July 2024).

10. ISAP (2007), “Act of April 26, 2007 on crisis management”, available at: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20070890590/U/D20070590Lj.pdf (Accessed 17 July 2024).

11. National Protective Security Authority (2024), “Critical National Infrastructure”, available at: https://www.npsa.gov.uk/critical-national-infrastructure-0 (Accessed 17 July 2024).

12. Biryukov, D.S. (2015), “Protection of critical infrastructure in Ukraine: from scientific understanding to development of policy principles”, *Naukovo-informatsiinyi visnyk Akademii natsionalnoi bezpeky*, vol. 3-4, pp. 155–170.

13. The Verkhovna Rada of Ukraine (2021), The Law of Ukraine “On critical infrastructure”, available at: https://zakon.rada.gov.ua/laws/show/1882-20#Text (Accessed 16 November 2021).

14. Cabinet of Ministers of Ukraine (2022), Resolution “On the establishment of the State Service for the Protection of Critical Infrastructure and Ensuring the National Stability System of Ukraine”, available at: https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text (Accessed 12 July 2022).

15. The Verkhovna Rada of Ukraine (2022), The Law of Ukraine “On making changes to some laws of Ukraine regarding the powers of the authorized body in the field of protection of critical infrastructure of Ukraine”, available at: https://zakon.rada.gov.ua/laws/show/2684-20#Text (Accessed 18 October 2022).

16. Cabinet of Ministers of Ukraine (2017), Order “On the approval of the Concept of creating a state system for the protection of critical infrastructure”, available at: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (Accessed 6 December 2017).

17. Cabinet of Ministers of Ukraine (2019), Resolution “On the approval of General requirements for cyber protection of critical infrastructure objects”, available at: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (Accessed 19 June 2019).

18. Cabinet of Ministers of Ukraine (2020), Resolution “Some issues of critical information infrastructure objects”, available at: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text (Accessed 9 October 2020).

19. Cabinet of Ministers of Ukraine (2022), Resolution “On approval of the Procedure for Monitoring the Security Level of Critical Infrastructure Objects”, available at: https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#Text (Accessed 22 July 2022).

20. Cabinet of Ministers of Ukraine (2023), Resolution “Some issues of conducting an independent audit of information security at critical infrastructure facilities”, available at: https://zakon.rada.gov.ua/laws/show/257-2023-%D0%BF#Text (Accessed 24 March 2023).

21. Cabinet of Ministers of Ukraine (2023), Resolution “On approval of the Procedure for maintaining the Register of critical infrastructure objects, inclusion of such objects in the Register, access and provision of information from it”, available at: https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text (Accessed 28 April 2023).

22. Cabinet of Ministers of Ukraine (2023), Resolution “Some issues of certification of critical infrastructure objects”, available at: https://zakon.rada.gov.ua/laws/show/818-2023-%D0%BF#Text (Accessed 4 August 2023).

23. Cabinet of Ministers of Ukraine (2023), Order “On the approval of the National Plan for the Protection and Ensuring the Safety and Stability of Critical Infrastructure”, available at: https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text (Accessed 19 September 2023).

24. The Verkhovna Rada of Ukraine (2018), The Law of Ukraine “On the national security of Ukraine”, available at: https://zakon.rada.gov.ua/laws/show/2469-19#Text (Accessed 21 June 2018).

25. Bobro, D.G. (2020), “Improvement of the methodology of ranking critical infrastructure objects and their assignment to critical infrastructure: analyst. zap”, available at: http://www.niss.gov.ua/content/articles/files/krutuchna_infra-a7636.pdf (Accessed 17 July 2024).

26. President of Ukraine (2022), Decree “On the introduction of martial law in Ukraine”, available at: https://zakon.rada.gov.ua/laws/show/64/2022#Text (Accessed 24 February 2022).

27. The Verkhovna Rada of Ukraine (2022), The Law of Ukraine “On the approval of the Decree of the President of Ukraine “On the introduction of martial law in Ukraine”, available at: https://zakon.rada.gov.ua/laws/show/2102-20#Text (Accessed 24 February 2022).

28. Melnyk, D.S. (2024), “Building a model of threats to the national critical infrastructure of Ukraine as a basis for ensuring its security and stability”, *Visnyk Kharkivskoho natsionalnoho universytetu vnutrishnikh sprav*, vol. 1 (1), pp. 237–250.

29. Strahnytskyi, Y.O. (2023), “Cluster approach to ensuring the protection of critical infrastructure in the conditions of martial law in Ukraine”, *Investytsii: praktyka ta dosvid*, vol. 23, pp. 163–169.

30. Trushkina, N.V. and Zhukova, I.V. (2024), “Economic support of organization and functioning of critical infrastructure”, *Uspikhy i dosiahnennia u nautsi*, vol. 1, pp. 372–383.

Стаття надійшла до редакції 22.07.2024 р.