DOI https://doi.org/10.30525/978-9934-26-279-1-5

ОСОБЛИВОСТІ СУЧАСНОЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВІЙНИ В УКРАЇНІ

Страхніцький Я. О.

ВСТУП

Сучасний розвиток демократичного суспільства оснований на гармонійному функціонуванні базових секторів забезпечення життєдіяльності. Як відомо, нормальне життєзабезпечення сьогодні неможливе без енергетики, транспорту, телекомунікації, водо- та газопостачання, медицини та ін. Дисфункція будь-якого із даних секторів загрожує країні порушенням суспільного побуту, економічними втратами та навіть руйнуваннями і техногенними катастрофами. Саме ці сфери мають назву критичної інфраструктури.

Сучасна військово-терористична ситуація в Україні становить небезпеку і для країн ЄС, що свідчить про необхідність формування спільного рішення із забезпечення комплексної системи захисту України. Об'єкти критичної інфраструктури у таких умовах стали найбільш вразливими для для диверсій, терористичних актів та несанкціонованих втручань. Країна агресор використовує сьогодні об'єкти життєзабезпечення у якості зброї для морально-психологічного терору мирного населення з метою посилення внутрішньої дестабілізації країни. У такому випадку, особливої актуальності набувають комплексні заходи загальнодержавного рівня, які мають бути узгоджені між безпековими і правоохоронними органами, зокрема і для протидії сучасним загрозам гібридного характеру. Актуальність наукового обґрунтування сучасної державної політики у сфері захисту критичної інфраструктури в умовах війни в Україні обумовлена рядом факторів:

По-перше, наслідки ракетних ударів, аварій, катастроф та інших надзвичайних ситуацій стають все більш масштабними і небезпечними для населення та стабільного функціонування економіки та життєзабезпечення населення.

По-друге, кризові явища, з якими стикнулося українське суспільство у період військової агресії є безпрецедентнним у сучасному світі, що продемонструвало значимість злагодженої державної політики усфері захисту об'єктів критичної інфраструктури та необхідність кардинальних реформ у цій галузі.

По-третє, питання забезпечення адміністративних функцій, організаційної структури, основи функціонування та напрямів розвитку системи захисту критичної інфраструктури потребує визначення місця та ролі держави. Це, перед усім, актуалізує необхідність розгляду проблем формування державної політики в галузі забезпечення захисту критичних об'єктів на території держави у мирний та військовий час**.** Створення системи спеціально уповноважених органів управління у сфері захисту критичної інфраструктури від надзвичайних ситуацій на всіх рівнях організації державної влади та місцевого самоврядування, їхніх завдань та функцій слід відзначити як пріоритетну сферу державної політики.

1. Теоретичне обґрунтування сутності критичної інфраструктури як об'єкту державної політики

Пріоритетність у актуалізації непорушності базових принципів і фундаментальних засад забезпечення національної безпеки має непересічне значення для будь-якої суверенної держави світу. Нині, в умовах військової агресії, для Україні це питання номер один у сфері державного управління. Згідно чинного українського законодавства у п. 9 ст. 1 Закону України «Про національну безпеку України», національна безпека визначається як «захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз»[1]. Згідно п. 10 ст. 1 цього ж Закону, 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»[1]. При цьому акцент зроблено саме на забезпеченні фундаментальних національних інтересів України, до яких враховано:

1. Державний суверенітет і територіальну цілісність, демократичний конституційний лад, недопущення втручання у внутрішні справи України;

2. Сталий розвиток національної економіки, громадянського суспільства і держави для забезпечення зростання рівня та якості життя населення;

3. Інтеграція України в європейський політичний, економічний, безпековий, правовий простір, набуття членства в Європейському Союзі та в Організації Північноатлантичного договору, розвиток

[1] Закон України «Про національну безпеку України» від 21.06.2018 № 2469-VIII.

рівноправних взаємовигідних відносин з іншими державами[1]. Аналіз фундаментальних постулатів Закону дає підстави стверджувати, що національна безпеку визначає баланс трьох складових: життєво важливих національних інтересів, загроз і захисту. Отже саме на цих трьох «китах» варто закладати фундамент державної політики у сфері захисту критичної інфраструктури.

До життєво важливих інтересів держави Домарецький М. Б.[2] відносить:

– забезпечення ефективного захисту населення та критично важливих об'єктів на території Україні при надзвичайних ситуаціях і терористичних актах;

– забезпечення захисту та виживання населення у воєнний час;

– збереження об'єктів, істотно необхідних для стійкого функціонування економіки та виживання населення.

Отже, на першому місці встановлено саме забезпечення захисту об'єктів критичної інфраструктури на території Україні. Варто відзначити, що Закон «Про критичну інфраструктуру» також регламентує захист критичної інфраструктури у якості складової частини забезпечення національної безпеки України. Враховуючи це, перелік загроз національній безпеці, який визначено Стратегію національної безпеки України[3], варто враховувати при формуванні державної політики захисту критичної інфраструктури:

1. Зміни клімату та ризик надзвичайних ситуацій природного і техногенного характеру, виникнення і поширення інфекційних хвороб.

2. Чергова гонка озброєнь на основі нових фізичних принципів.

3. Поширення міжнародного тероризму та злочинності у кібер-просторі, наркоторгівлі, торгівлі людьми, сепаратизму, розповсюдження зброї та ін.

4. Поширення коронавірусної хвороби (COVID-19) що детрмінує каскад негативних наслідків таких як: криза охорони здоров'я та соціального захисту, зростання безробіття, зниження продовольчої безпеки, обмеження руху, товарів та робочої сили, розвиток глобальної фінансово-економічної кризи.

[2] 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.

[3] Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14.09.2020 р. «Про Стратегію національної безпеки України» № 392/2020.

5. Посилення міжнародної конкуренції із демонстрацією «національної сили», у тому числі збройна експансія проти України Російської Федерації.

6. Дефіцит фінансування на модернізацію систем озброєння радянського виробництва, які вичерпали свій ресурс.

7. Недостатня ефективність і корумпованість державних органів влади.

8. Низький рівень добробуту населення.

9. Недостатній рівень конкуренції, низька правова захищеність у ключових сферах (зокрема в енергетиці) та значна доля державного сектору в економіці, що гальмує її інвестиційну діяльність.

10. Погіршення середовища життєдіяльності громадян (якість повітря, води, продуктів харчування, нераціональне використання природних ресурсів).

11. Погіршення демографічної ситуації та прогресуюча еміграція кадрів.

Варто також відзначити посилення ролі загроз для критичної інфраструктури, які законотворці виділили в окремий пункт та пов'язали із погіршенням її технічного стану, відсутністю інвестицій та модернізації, несанкціоновані фізичні- або кібервтручання, пролонговані бойові дії на Сході країни, а також тимчасову окупацію частини території.

Аналізуючи окремі приклади у законодавчій базі іноземних держав[4,5] зазначимо що спільною рисою є розподіл загроз критичній інфраструктурі на три основні категорії:

1) надзвичайні ситуації природного характеру;

2) надзвичайні ситуації техногенного характеру;

3) зловмисні дії.

Бобро Д. Г.[6] пропонує додати до цього переліку ще комбіновані загрози, які учений вважає особливо небезпечними, оскільки вони можуть спричинити «ефект доміно» у вигляді різноманітних каскадних ефектів внаслідок синергії елементів критичної інфраструктури між собою.

Термін «критично-важливі об'єкти» введений в нормативно-законодавчих актах багатьох держав, його термінологія дещо відрізняється, але ці відмінності не істотні. Категорія критичності

[4] Commission of the European Communities (2005), Green Paper on a European programme for critical infrastructure protection. URL: https://www.ab.gov.tr.

[5] Department of Homeland Security (2013), Presidential Policy Directive. Critical Infrastructure Security and Resilience. URL: https://www.obamawhitehouse.archives.gov.

[6] Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. *Стратегічні пріоритети. Серія: Економіка.* 2015. № 4. С. 83–93.

(критерії) об'єкта критичної інфраструктури визначені у Законі 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. Під критично важливою інфраструктурою колектив авторів на чолі із С. П. Азаровим та В. Л. Сидоренко[7] 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. Як показали результати досліджень, у нормативно-правових актах та практиці міжнародного спілкування перші згадки поняття «критична інфраструктура» почали з'являтись у середині 90-х років минулого століття. До сьогодні у наукових, ділових та урядових колах дана дефініція постійно коригується та удосконалюється, однак «спільним знаменником» у різноманітті трактувань можна вважати зв'язок із державними та приватними об'єктами, які прямо чи опосередковано впливають на рівень обороноздатності та національної безпеки країни й підтримують життєво важливі функції держави у суспільстві. Виходячи із цього, можна погодитись із переконанням учених[8], які до критичної інфраструктури відносять енергетичні та транспортні мережі, нафто- та газопроводи, інфраструктуру морського і річкового транспорту, канали зв'язку, системи життєзабезпечення, вивезення й утилізації небезпечних відходів, служби екстреного реагування на надзвичайні ситуації, оборонний комплекс і органи влади[9]. 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)[10].

---

[7] 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.

[8] Єрменчук О. П. Складові національної інфраструктури. *Науковий вісник ДДУВС*. 2017. № 4. С. 109–115.

[9] Теленик С. С. Досвід правового регулювання системи захисту критичної інфраструктури в США. *Науковий вісник НАВС*. 2018. № 2 (107). С. 358–370.

[10] Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М. Організаційні та правові аспекти забезпечення безпеки і стій кості критичної інфраструктури України. К. : НІСД, 2019. 224 с.

Урядами більшості розвинених країн напрацьовано автентичні підходи до ідентифікації поняття критичної інфраструктури у нормативно-правовій базі. 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[11]. 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»[11]. Представлене визначення однозначно підтверджує факт, що безпека критичної інфраструктури є детермінантою національної безпеки.

Важливим у процесі подальшого вивчення предмету дослідження, є аналіз підходів до визначення інтенції критичної інфраструктури як об'єкту державного управління у європейських країнах. Так, у процесі роботи Євроатлантичної ради НАТО у 2002 р. було зазначено, що «критична інфраструктура включає в себе фізичні та кібернетичні системи забезпечення важливих і необхідних видів діяльності економіки та державного управління». У Директиві Європейської Комісії 2008/114 критичну інфраструктуру 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»[12].

У законодавстві Німеччини визначення «критична інфраструктура» можна віднайти у Національній стратегії захисту критичної інфраструктури[13]. Там її визначено 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». Наведене вище

[11] USA Patriot Act of 2001. URL: https://www.gpo.gov

[12] 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.

[13] National Strategy for Critical Infrastructure Protection (CIP Strategy). URL: https://www.kritis.bund.de

визначення у своїй основі збігається із американським визначенням та трактуванням Європейської Комісії, за єдиним виключенням, – у німецькому варіанті зроблено акцент на важливості забезпечення стійких поставок, як можна розуміти мова йде про стабільність постачання товарів життєвої необхідності та надання відповідних послуг.

У Польщі даний термін теоретизовано в законі «Про антикризове управління» (Ustawa o zarządzaniu kryzysowym), у якому під критичною інфраструктурою 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»[14]. Аналізуючи дане формулювання варто відзначити акцент на важливості стабільної роботи органів державної влади.

У законодавстві Великобританії термін «критична інфраструктура» визначено як «критичні елементи інфраструктури, а саме активи, засоби, системи, мережі чи процеси та основні працівники, які керують ними, втрата або компрометація яких може призвести до значних шкідливих впливів на доступність, цілісність або надання основних послуг, включаючи ті послуги, дестабілізація яких, може призвести до значних людських жертв з урахуванням значних економічних або соціальних наслідків; та/або значний вплив на національну безпеку, національну оборону чи функціонування держави»[15]. Ключова відмінність даного формулювання полягає у відокремленні в окрему категорію фахівців, які забезпечують роботу критичних секторів держави та в перерахунку наслідків на першому місці враховано безпеку людини. Важливо також зауважити, що в іноземній практиці визначення критичної інфраструктури акцент зміщується із фізичного виміру об'єктів більше до їх функцій та послуг, які забезпечують потреби суспільства, держави та її економіки[16].

Із аналізу представленого розмаїття дефініцій можемо зробити узагальнення, що у більшості з них простежується спільна риса – ключове значення даного сектору для безпеки громадян, суспільства й держави. Погодимось із думкою вчених С. Гнатюка, В. Сидоренка,

[14] Ustawa o zarządzaniu kryzysowym. Dz. U. 2007 Nr 89 poz. 590. URL: http://isap.sejm.gov.pl/isap.nsf/

[15] Офіційний веб-сайт Centre for the Protection of National Infrastructure. URL: http://www.cpni.gov.uk/

[16] 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.

Н. Сєйлової[17], які уніфікують критичну інфраструктуру будь-якої держави − яке велику складну систему стратегічно-важливого значення, яка є сукупністю чисельності елементів різного типу, об'єднаних зв'язками різної природи і яка володіє загальною властивістю (призначенням, функцією), відмінною від властивостей окремих елементів усієї сукупності. З наведених визначень видно, що відмінності у терміні «критична інфраструктура» в різних країнах світу не суттєві, вони, очевидно, відображають національну або організаційну специфіку сфери застосування терміну, особливості їх нормативно-правових систем.

Акцентуємо увагу ще на одному важливому питанні – віднесенні об'єктів національної інфраструктури до критичної відповідно до важливості функцій та послуги які вони виконують. Аналіз вітчизняних нормативно-правових актів дає підстави всі потенційні об'єкти критичної інфраструктури, які потребують захисту, узагальнити у квадро-комплекс:

1. Великі об'єкти критичної інфраструктури загальнодержавного значення.
2. Життєво важливі об'єкти критичної інфраструктури.
3. Важливі об'єкти критичної інфраструктури.
4. Необхідні об'єкти критичної інфраструктури.

Проблемою у реалізації державної політики у сфері захисту критичної інфраструктури учені вбачають складність ідентифікації об'єктів критичними на національному, регіональному або локальному рівнях інфраструктури[18]. Ключ до відповіді на дане питання вітчизняні законотворці надали у Законі України «Про критичну інфраструктуру»[19] де зазначили перелік життєво важливих функцій та послуг, представники з надання яких потребують захисту, як об'єкти критичної інфраструктури. До таких послуг нележить: енергозабезпечення; водопостачання та водовідведення; продовольче забезпечення; охорона здоров'я; фармацевтична промисловість; виготовлення вакцин, стале функціонування біолабораторій; інформаційні послуги; електронні комунікації; фінансові послуги; транспортне забезпечення; оборона, державна безпека; правопорядок, здійснення правосуддя, тримання під

[17] 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.

[18] Постанова КМУ «Деякі питання об'єктів критичної інфраструктури» від 09.10.2020 № 1109 URL: https://zakon.rada.gov.ua/laws/show/1109-2020п#Text

[19] Закон України «Про критичну інфраструктуру». від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20

вартою; цивільний захист населення та територій, служби порятунку; космічна діяльність, космічні технології та послуги; хімічна промисловість; дослідницька діяльність. Вважаємо, що даний перелік є не є вичерпним та достатньо деталізованим, він здатний варіювати залежно від розміру країни та може досягати декількох тисяч пунктів.

Отже, проведено аналіз існуючих міжнародних нормативних документів, що регламентують поняття захисту критичної інфраструктури, були визначені критичні об'єкти, які у майбутньому можуть бути використанні як базові для більш обширної класифікації. Визначення характеристик віднесення елементів до критичної інфраструктури на базі нормативно-правових документів різних держав дасть Україні змогу встановити вимоги до забезпечення їх безпеки з урахуванням ступеня потенційної небезпеки та можливих наслідків.

Крапку у інституційній полеміці законодавчого врегулювання дефініції «критична інфраструктура» поставив Президент України, підписавши Закон «Про критичну інфраструктуру», прийнятий Верховною Радою 16.02.2021 р.[19]. Визначення 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»[20].

Критичні інфраструктури за їх технічними, структурними та функціональними особливостями можна класифікувати як життєво необхідну базову технічну інфраструктуру, з одного боку, і життєво важливу (абсолютно суттєву) інфраструктуру соціально-економічних послуг, з іншого боку.

2. Структурно-функціональна характеристика державної політики у сфері захисту критичної інфраструктури в Україні

Ґрунтуючись на положеннях загальної теорії державного управління[21], державну політику у сфері безпеки слід розглядати в рамках певної соціально-економічної системи, що об'єднує:

- стабільні внутрішні зв'язки населення;
- об'єкти економіки, інфраструктури, території;
- управлінські структури[22].

[20] Офіційний веб-сайт Національного інституту стратегічних досліджень. URL: http://old.niss.gov.ua/articles/2213.

[21] Енциклопедія державного управління: у 8 томах. Нац. акад. держ. упр. при Президентові України. Київ : НАДУ, 2011.

Аналізуючи сучасну структурно-функціональну характеристику державної політики у сфері захисту критичної інфраструктури в Україні, відзначимо що у цьому напрямку існує ряд паралельно функціонуючих систем:

1. Єдиної державної системи цивільного захисту, що являє собою сукупність органів управління, сил і засобів центральних та місцевих органів виконавчої влади, Ради міністрів Автономної Республіки Крим, виконавчих органів рад, підприємств, установ та організацій, які забезпечують реалізацію державної політики у сфері цивільного захисту; Керівництво єдиною державною системою цивільного захисту здійснює Кабінет Міністрів України. Безпосереднє керівництво діяльністю даної державної системи здійснює ДСНС.

Функціональні підсистеми єдиної державної системи цивільного захисту створюються у відповідних сферах суспільного життя центральними органами виконавчої влади з метою захисту населення і територій від надзвичайних ситуацій у мирний час та в особливий період, забезпечення готовності підпорядкованих їм сил і засобів до дій, спрямованих на запобігання і реагування на надзвичайні ситуації. Безпосереднє керівництво діяльністю функціональної підсистеми здійснюється керівником органу чи суб'єкта господарювання, що створив таку підсистему.

Територіальні підсистеми єдиної державної системи цивільного захисту створюються в Автономній Республіці Крим, областях, мм. Києві та Севастополі з метою здійснення заходів щодо захисту населення і територій від надзвичайних ситуацій у мирний час та в особливий період у відповідному регіоні. Безпосереднє керівництво діяльністю територіальної підсистеми, її ланок здійснюється посадовою особою, яка очолює орган, що створив таку підсистему, ланку.

Постійно діючими органами управління цивільного захисту, до повноважень яких належать питання організації та здійснення заходів цивільного захисту, є:

– на державному рівні – Кабінет Міністрів України, ДСНС, а також центральні органи виконавчої влади, що створюють функціональні підсистеми, та підрозділи з питань цивільного захисту у складі їх апаратів;

– на регіональному рівні – Рада міністрів Автономної Республіки Крим, обласні, Київська та Севастопольська міські держадміністрації, підрозділи з питань цивільного захисту, які утворюються у їх складі, територіальні органи ДСНС;

---

[22] Інституціоналізація публічного управління в Україні : наук.-аналіт. доп. Київ : НАДУ, 2019. 210 с.

– на місцевому рівні – районні, районні у м. Києві та Севастополі держадміністрації, виконавчі органи міських (міст республіканського Автономної Республіки Крим, міст обласного і районного значення) рад, підрозділи з питань цивільного захисту, які утворюються у їх складі, виконавчі органи селищних та сільських рад, підрозділи територіальних органів ДСНС;

– на об'єктовому рівні – керівні органи підприємств, установ та організацій, а також підрозділи (посадові особи) з питань цивільного захисту, які утворюються (призначаються) такими органами відповідно до законодавства.

2. Єдина державна система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків. Одним із ключових органів у цій системі є Служба безпеки України (СБУ). Для цього при СБУ діє Антитерористичний центр (АТЦ), створений у грудні 1998 року Указом Президента України [23]. Саме АТЦ координує діяльність усіх суб'єктів боротьби з тероризмом. Зокрема, для протидії терактам, які несуть загрозу життю і здоров'ю людей, а також для запобігання диверсіям на об'єктах критичної інфраструктури. Правовою основою діяльності АТЦ є Конституція України, закон «Про боротьбу з тероризмом», положення «Про Антитерористичний центр та його координаційні групи при регіональних органах СБУ», інші нормативні акти. Антитерористичний центр складається з міжвідомчої координаційної комісії, штабу АТЦ та координаційних груп та їхніх штабів при регіональних органах СБУ.

Єдина державна система складається з постійно діючих територіальної і функціональної підсистем. Суб'єкти даної підсистеми організовують діяльність щодо запобігання, реагування, припинення терористичних актів та мінімізації їх наслідків. Управління здійснюється координаційними групами Антитерористичного центру при регіональних органах СБУ[23].

Управління функціональною підсистемою єдиної державної системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків здійснюється суб'єктами боротьби з тероризмом у межах повноважень, координація діяльності якої здійснюється Міжвідомчою координаційною комісією Антитерористичного центру. У разі необхідності У складі АТЦ можуть створюватися і діяти військово-цивільні адміністрації. Ці тимчасові державні органи не лише беруть участь у протидії диверсійним проявам і терактам, а й

[23] Указ Президента України. «Про Антитерористичний центр» № 1343/98 від 11.12.1998 р.

забезпечують дотримання законів України, безпеки та правопорядку в районі проведення антитерористичної операції[24].

Єдина державна система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків дозволяє у цілодобовому режимі здійснювати моніторинг, аналіз та оцінку даних про тенденції поширення тероризму в Україні та за її межами. Відоповідно, головними її завданнями є:

– запобігання терористичній діяльності, у тому числі своєчасне виявлення та усунення причин і передумов для терактів;

– інформування населення про рівні загроз щодо можливого вчинення терактів;

– безпека потенційних об'єктів терористичних посягань, до яких належать: важливі державні об'єкти та ті, що перебувають під державною охороною, об'єкти підвищеної небезпеки, об'єкти єдиної транспортної системи України та електроенергетики, закордонні дипломатичні установи, консульські та інші представництва іноземних держав на території України, установи Державної кримінально-виконавчої служби, місця масового перебування людей.

З метою виконання перелічених завдань, учасники системи розробляють стратегічні програми боротьби з тероризмом і більш локальні рекомендації, формують плани запобігання терористичним проявам.

3. Державна система фізичного захисту (функціонує відповідно до Закону України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання»[25].

Фізичний захист ядерних матеріалів, ядерних установок, радіоактивних відходів, інших джерел іонізуючого випромінювання спрямований на захист інтересів національної безпеки, попередження та припинення диверсій, крадіжки або будь-якого іншого незаконного вилучення ядерного матеріалу, радіоактивних відходів, інших джерел іонізуючого випромінювання, а також зміцнення режиму нерозповсюдження ядерної зброї[26].

---

[24] Офіційний веб-сайт Служби безпеки України. URL: https://ssu.gov.ua/antyterorystychnyi-tsentr-pry-ssu

[25] Постанова Кабінету Міністрів України «Про затвердження Порядку функціонування державної системи фізичного захисту» № 1337 від 21.12.2011 р.

[26] Закон України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» № 2064-III від 19.10.2000 р.

Відповідно до тексту Закону України 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» [26].

Функціонування державної системи фізичного захисту ґрунтується на результатах оцінки загрози вчинення диверсії, крадіжки або будь-якого іншого неправомірного вилучення радіоактивних матеріалів.

Завданнями державної системи фізичного захисту визначено:

– нормативно-правове регулювання питань фізичного захисту;

– забезпечення захищеності ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання з урахуванням проектної загрози;

– створення та забезпечення функціонування єдиної системи захищеного зв'язку між органами державної влади і юридичними особами, до повноважень яких належить здійснення функцій обліку, контролю, фізичного захисту та протидії нападу на ядерні установки, об'єкти, призначені для поводження з радіоактивними відходами, іншими джерелами іонізуючого випромінювання, транспортні засоби, що перевозять радіоактивні матеріали;

– здійснення державного нагляду та контролю за станом фізичного захисту;

– організація роботи з обміну інформацією про стан фізичного захисту та її збереження.

Порядок функціонування державної системи фізичного захисту встановлюється Кабінетом Міністрів України. До суб'єктів державної системи фізичного захисту належать:

– Орган державного регулювання ядерної та радиаційної безпеки;

– Центральні органи виконавчої влади, які здійснюють державне управління, та Національна академія наук України щодо фізичного захисту;

– Служба безпеки України;

– Національна гвардія України;

– Центральні органи виконавчої влади, які здійснюють правоохоронну діяльність.

– Інші центральні та місцеві органи виконавчої влади, а також ліцензіати беруть участь у забезпеченні фізичного захисту у межах своїх повноважень, визначених цим Законом та іншими актами законодавства.

До об'єктів державної системи фізичного захисту віднесено ядерні установки, об'єкти, призначені для поводження з радіоактивними

відходами, ядерні матеріали, радіоактивні відходи, інші джерела іонізуючого випромінювання, радіоактивні матеріали, виявлені в незаконному обігу.

4. Національна система кібербезпеки. Згідно ст..8 Закону України «Про основні засади забезпечення кібербезпеки України» 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[27]. Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які виконують основні завдання відповідно до Конституції і законів України. Координатором реалізації цієї Стратегії є робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки.

Реалізація Стратегії безпосередньо здійснюється основними суб'єктами національної системи кібербезпеки, Міністерством закордонних справ України, Міністерством цифрової трансформації України, Міністерством освіти і науки України та іншими суб'єктами забезпечення кібербезпеки в межах їх компетенції.

Кібербезпека України забезпечується шляхом проведення виваженої державної політики відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм. Національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів 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[28].

[27] Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 р.

[28] Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» № 447/2021 від 26.08.2021 р.

Основними напрямами державної політики у сфері кібербезпеки України визначено:

– створення захищеного національного сегмента кіберпростору, що сприятиме підтриманню відкритого суспільства і забезпечуватиме безпечне використання цього простору суспільством;

– запобігання втручанню у внутрішні справи України і нейтралізація посягань на її інформаційні ресурси з боку інших держав;

– посилення обороноздатності держави у кіберпросторі;

– боротьба з кіберзлочинністю та кібертероризмом;

– зниження рівня уразливості об'єктів кіберзахисту;

– забезпечення повноправної участі України в загальноєвропейській та регіональних системах забезпечення кібербезпеки;

– дотримання міжнародних зобов'язань щодо боротьби з кіберзлочинністю та кібертероризмом[28].

Очевидною є необхідність створення Національної системи кібербезпеки, коли нею будуть займатися відповідні підрозділи СБУ, кіберзахистом – відповідні підрозділи ДССЗЗІ (Державної служби спеціаль-яного зв'язку та захисту інформації), а боротьбою з кіберзлочинністю – відповідні підрозділи МВС. Координацію та ефективну взаємодію буде забезпечувати відповідний підрозділ РНБО[29].

3. Сучасна парадигма державної політики у сфері захисту критичної інфраструктури в умовах військового стану в Україні

Для розуміння логіки наукового обґрунтування ключових постулатів державної політики у сфері захисту критичної інфраструктури в Україні, обумовлених радикальними змінами безпекового середовища та виникненням нових стратегічних загроз, ми обрали теоретичну конструкцію запропоновану Томасом Куном і названу тим терміном «парадигма». Дане теоретизування також підтримав у своїх дослідженнях Р. К. Мертон [30]. Обґрунтуємо доцільність застосування даного конструкту у напрямку вивчення питання безпеки критичної інфраструктури, опираючись на тезис М. Цюрупи, який стверджує, що звернення до парадигми дає можливість охопити у єдиній теоретичній конструкції конкретних гіпотез-відповідей на проблемні питання. Тобто, це надасть можливість згенерувати надійний інструмент наукового

[29] Ліпкан В. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України / В. Ліпкан, І. Діордіца // *Підприємництво, господарство і право.* 2017. № 5. С. 174–180.

[30] Merton, R.K. (1968). Social Theory and Structure. London: The Free Press of Glencoe, Collier- MacMillan Limited: 22-216

дослідження актуальних векторів формування державної безпекової політики на основі наукового колективізму, організованого скептицизму стосовно «легких шляхів» вирішення дослідницьких завдань і певна усталеність, висловлених положень[31].

Необхідно підкреслити, що сучасна парадигма державної політики у сфері захисту критичної інфраструктури в умовах військового стану в Україні в теоретичному плані достатньо не вивчено. В цьому випадку для формування раціональних структур управління надзвичайно важливо осягнути глибину і складність реальних проблем України в період активних бойових дій та актів тероризму на об'єктах критичної інфраструктури у реальному часі і врахувати їх при формуванні майбутньої державної політики у сфері захисту. При цьому, як зазначає Бєлоусов А. В. необхідним є зважений погляд на стан суспільства, його можливості та перспективи, ресурси, резерви, потенціал і джерела зростання[32].

Варто зазначити, що у теорії державного управління не існує універсального інституційного кліше, яке б визначало алгоритм захисту об'єктів критичної інфраструктури. Отже, уряд має опитатися на характеристики поточної ситуації в країні з погляду на наступні базові показники:

- спектр поточних і прогнозних критичних загроз та ризиків;
- стану і структури економіки;
- культури нації та суспільно-політичної ситуації в країні;
- загальної інституційної практики державного управління;
- основи конституційного ладу країни.

Прислухаємось до наукового погляду вчених Бірюкова Д. С. та Кондратова С. І.[33] на архітектуру державної політики захисту об'єктів критичної інфраструктури. Учений пропонує дуальну парадигму державного управління у сфері захисту об'єктів критичної інфраструктури, як варіацію двох основних моделей:

1. Модель основана на принципах саморегулювання, стимулах та добровільному дотриманні стандартів («добровільний підхід»), яка

[31] Цюрупа М. Зміна парадигм воєнно-політичного мислення у доктринах та стратегіях воєнної безпеки України XX–XXI ст. *Українознавчий альманах.* 2021. Вип. 28. С. 120–126.

[32] 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

[33] Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Аналітична доповідь. К. : ПП «Видавництво «ФЕНІКС», 2012. 92 с.

передбачає політику, спрямовану на лібералізацію упавління. Відповідно до цієї моделі усі стейкхолдери інфраструктурних об'єктів (державного чи приватного сектору) мають право докласти зусиль задля формування та реалізації політики захисту критичної інфраструктури. Можуть бути як дорадчі так і фізичні дії зі сприяння досягненню спільної мети. Дія нормативно-правової бази чинить влив додаткового інструменту (за винятком певних небезпечних секторів).

2. Модель, основана на принципах обов'язковості та відповідальності. Головна ідея полягає у тому, що державна політика у сфері захисту критичної будується на обов'язковості дотримання правових рамок та супроводжується заходами покарання операторів об'єктів критичної інфраструктури за порушення у сфері безпеки.

Варто зазначити, що здебільшого країни не трансплантують у державну політику жодну із зазначених моделей у базовій формі, а комбінують елементи обох. Проблематику розбудови парадигми державної політики захисту критичної інфраструктури на основі світового досвіду вивчав учений Бобро Д. Г.[34], який виокремив ключові кроки у цьому напрямі:

1. Розробка нормативно-правової бази та її регулярна модернізація.

2. Визначення координуючого органу. Наприклад, у США це Department of Homeland Security (Департамент внутрішньої безпеки). До його складу входять 22 федеральних агентства та відомства із загальною чисельністю близько 170 тис. чол.).

3. Розробка методологічних підходів до формування переліку об'єктів критичної інфраструктури, оцінки загроз та ризиків.

4. Розробка планів оперативного реагування та регулярна оцінка їх дієвості. Наприклад, у США цим опікується Національний центр аналізу та імітаційного моделювання інфраструктури (National infrastructure simulation and analysis center)[35].

4. Забезпечення підготовки кваліфікованих кадрів у сфері захисту критичної інфраструктури.

5. Організація оперативної співпраці, обміну інформацією та кращими практиками.

[34] 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

[35] Офіційний веб-сайт National Infrastructure Simulation and Analysis Center. URL: https://www.cisa.gov

6. Розвиток державно-приватного партнерства[36].

Парадигма державної політики у сфері захисту критичної інфраструктури в умовах військового стану в Україні неможлива без здійснення специфічних функцій управління спеціальних державних органів.

Україна сьогодні зіткнулася із необхідністю адаптації своєї державної політики до умов протидії численним інструментам ведення гібридної війни з боку країни агресора, спрямованих на руйнацію суверенітету та цілісності нашої країни. Розпочата російською федерацією повномасштабна війна, несе суттєву загрозу та руйнування як для військових та промислових об'єктів, так і для життєво-важливих об'єктів критичної інфраструктури. Очевидно, що наявні випадки знищення критичних об'єктів, мають на меті завдати значної шкоди нормальним умовам життєдіяльності цивільного населення.

У зв'язку з військовою агресією російської федерації, Президент України, на підставі пропозиції Ради національної безпеки і оборони України, відповідно до п. 20 ч. 1 ст.106 Конституції України та Закону України «Про правовий режим воєнного стану»[37] 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[37].

Варто зазначити, що прояви російського військового вторгнення систематично порушують міжнародні нормативно-правові акти, у тому числі й у сфері захисту критичної інфраструктури. Так, частина об'єктів критичної інфраструктури в умовах війни знаходиться під захистом Додаткового протоколу до Женевських конвенцій від

[36] Бобро Д. Г. Удосконалення методології ранжування об'єктів критичної інфраструктури та їх віднесення до критичної інфраструктури: аналітична записка. URL: http://www.niss.gov.ua/content/articles/files/krutuchna.pdf

[37] Закон України «Про правовий режим воєнного стану». № 389-VIII від 12.05.2015.

12 серпня 1949 року[38]. У документі відсутнє саме формулювання терміну «критична інфраструктура», однак зазначається, що «будь які цивільні об'єкти не повинні бути об'єктом нападу або репресалій». Відповідно, можемо зробити висновок, що оскільки об'єкти критичної інфраструктури не відносяться до військових, тому підпадають під дію даного документу. Окрім цього, документ забороняє піддавати нападу, знищувати чи виводити з ладу об'єкти, необхідні для виживання цивільного населення. Також у Додатковому протоколі є чіткий перелік установок і споруд, що містять небезпечні сили, які заборонено піддавати нападам, а саме: греблі, дамби й атомні електростанції. Однак Збройні Сили України підтверджують, що за одну із стратегічних цілей ворог обрав саме об'єкти критичної інфраструктури міст України, що розташовані у глибокому тилу. Це підтверджено фактами періодичних групових ракетних ударів з акваторії Чорного моря, рубежів пуску над Каспійським морем, а також стратегічної авіації із використанням різних типів ракет (Х-101, Х-555, Калібр, Іскандер, С-300, Торнадо), а також безпілотних літальних апаратів, в тому числі іранських дронів-камікадзе «Shahed 136» та Mohajer 6. Внаслідок збройної агресії на території України було пошкоджено уже близько 30% об'єктів критичної інфраструктури[39]. Можемо дійти висновку, що руйнуючи об'єкти критичної інфраструктури, всупереч міжнародним правилам війни, ворог намагається маніпулювати психологічним та моральним станом цивільного населення. Формуючи внутрішній страх потенційних проблем (відсутність взимку тепла, електроенергії, питної води, транспортного сполучення, медичного обслуговування та ін.), намагається доповнити процес активних бойових дій та змусити прийняти свої умови.

Аналізуючи напрямки державної політики у сфері захисту критичної інфраструктури в умовах воєнного стану, зазначимо, що ключовим напрямком залишається нормативно-правове регулювання інституційної складової. Ключовими законами в умовах воєнного стану у сфері захисту об'єктів критичної інфраструктури залишаються Конституція України, закони України «Про оборону України», «Про мобілізаційну підготовку та мобілізацію», «Про критичну інфраструктуру», «Про правовий режим воєнного стану» та ін. Відповідно до Закону «Про правовий режим воєнного стану»[37], на територіях, де введено воєнний стан, з метою захисту критичної інфраструктури, охорони прав, свобод і законних

[38] Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року.

[39] Офіційний веб-сайт Збройних Сил України. URL: https://www.zsu.gov.ua.

інтересів громадян можуть утворюватися тимчасові державні органи – військові адміністрації. Спрямування, координацію та контроль за діяльністю обласних військових адміністрацій з питань забезпечення оборони, громадської безпеки і порядку, захисту критичної інфраструктури, здійснення заходів правового режиму воєнного стану здійснює Генеральний штаб Збройних Сил України, а з інших питань – Кабінет Міністрів України та обласні державні адміністрації у межах своїх повноважень.

З метою захисту об'єктів критичної інфраструктури, військове командування разом із військовими адміністраціями (у разі їх утворення) може: встановлювати (посилювати) охорону об'єктів критичної інфраструктури та об'єктів, що забезпечують життєдіяльність населення, і вводити особливий режим їх роботи (порядок встановлення (посилення) охорони таких об'єктів та їх перелік, що із введенням воєнного стану підлягають охороні, а також порядок особливого режиму їх роботи затверджуються Кабінетом Міністрів України); запроваджувати трудову повинність для працездатних осіб, не залучених до роботи в оборонній сфері та захисту критичної інфраструктури з метою виконання робіт, що мають оборонний характер забезпечення функціонування національної економіки та захисту критичної інфраструктури; порушувати у порядку, визначеному Конституцією та законами України, питання про заборону діяльності політичних партій, громадських об'єднань, якщо вона спрямована на посягання на стійкість критичної інфраструктури. У межах своїх повноважень військові адміністрації населених пунктів здійснюють делеговані повноваження органів виконавчої влади, можуть встановлювати посилену охорону об'єктів критичної інфраструктури та об'єктів, які забезпечують життєдіяльність населення[37].

Актуальним заходом державної політики у сфері захисту критичної інфраструктури в умовах воєнного стану сьогодні вважаємо затверджений Постановою Кабінету Міністрів України 22 липня 2022 р. № 821 Порядок проведення моніторингу рівня безпеки об'єктів критичної інфраструктури [40], який визначає механізм проведення моніторингу із встановлення відповідності стану захищеності об'єкта критичної інфраструктури вимогам законодавства, достовірності наданої інформації визначеним суб'єктам національної системи захисту критичної інфраструктури, надання методичної допомоги операторам об'єктів критичної інфраструктури в удосконаленні системи захисту критичної інфраструктури.

[40] Порядок проведення моніторингу рівня безпеки об'єктів критичної інфраструктури. URL: https://zakon.rada.gov.ua/laws/show/821-2022-п#Text

У даному напрямку слушною вважаємо пропозицію учених Дзюба Т. М., Опанасенко М. І.[41] та Резнікової О. О.[42] по формуванню паспорта загроз для об'єктів критичної інфраструктури. Паспорт загроз учені визначають як документ, який передбачає оцінку подій, що створюють небезпеку[41]. Погоджуємось із думкою Резнікової О. О.[42], що дана ініціатива забезпечить раннє попередження осіб, що приймають управлінські рішення, про нові потенційні загрози та ризики, з метою їх об'єктивної та всебічної оцінки, підготовлення та здійснення відповідного рішення та реагування. Паспорт загроз учена рекомендує сформувати із трьох основних блоків: характеристики загроз; спроможності і ефективності держави з реагування на загрозу; оцінки масштабу загрози, тенденції її розвитку та наслідків реалізованих заходів. Тобто розроблення паспорта загроз для об'єктів критичної інфраструктури дасть можливість переорієнтувати існуючі можливості цільового моніторингу у необхідне русло в межах функціонування системи раннього виявлення та попередження загроз критичним об'єктам.

Ключовим нормативно-правовим актом, який визначає основи сучасної парадигми державної політики у сфері захисту критичної інфраструктури в умовах військового стану в Україні є Закон «Про критичну інфраструктуру»[19]. Стаття 7 даного Закону визначає рівні державного управління національною системою захисту критичної інфраструктури:

1) загальнодержавний рівень – здійснюється Кабінетом Міністрів України, уповноваженим органом у сфері захисту критичної інфраструктури України, органами державної влади відповідно до розподілу повноважень згідно з цим Законом, іншими центральними органами виконавчої влади та державними органами, Національним банком України;

2) регіональний та галузевий рівні, управління – здійснюється центральними та місцевими органами виконавчої влади, визначеними в установленому законом порядку відповідальними за забезпечення формування та реалізацію державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури та відповідальними за функціонування окремих державних систем захисту та реагування;

[41] Дзюба Т. М., Опанасенко М. І. Розроблення паспорту загрози для системи раннього виявлення загроз національній безпеці України. *Кібербезпека: освіта, наука, техніка.* 2021. № 4 (12). С. 61–68.

[42] Резнікова О. О. Паспорт сепаратистської загрози в Україні. *Стратегічні пріоритети*. 2018. № 2. С. 12–24.

3) місцевий рівень, управління – здійснюється місцевими органами виконавчої влади (військово-цивільними адміністраціями в умовах військового стану), органами місцевого самоврядування в межах повноважень;

4) об'єктовий рівень, управління – здійснюється оператором критичної інфраструктури на підставі нормативно-правових та регуляторних актів у сфері захисту критичної інфраструктури.

Формування та реалізація державної політики у сфері захисту критичної інфраструктури здійснюється:

1. Кабінетом Міністрів України, який забезпечує проведення державної політики у сфері захисту критичної інфраструктури України, організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи захисту критичної інфраструктури, визначає уповноважений орган з питань захисту критичної інфраструктури України, затверджує Регламент обміну інформацією для забезпечення обміну інформацією та взаємодії суб'єктів національної системи захисту критичної інфраструктури.

2. Секторальними та функціональними органами у сфері захисту критичної інфраструктури, які відповідають за формування та реалізацію державної політики в окремих секторах критичної інфраструктури.

3. Уповноваженим органом у сфері захисту критичної інфраструктури України, який відповідає за координацію діяльності суб'єктів національної системи захисту критичної інфраструктури.

Аналізуючи сучасні аспекти парадигми державної політики у сфері захисту критичної інфраструктури в умовах військового стану в Україні, відзначимо, що безпека критичної інфраструктури забезпечується на основі комплексного аналітичного процесу, архітектура якого побудована із:

– ідентифікації секторів критичної інфраструктури;

– створенні реєстру об'єктів критичної інфраструктури;

– визначенні актуальних загроз для об'єктів критичної інфраструктури;

– формування суб'єктного складу державної політики у сфері захисту критичної інфраструктури;

– удосконалення інституційного забезпечення державної політики у сфері захисту критичної інфраструктури;

– формування системи захисту критичної інфраструктури;

– вжиття відповідних заходів із ліквідації наслідків руйнувань об'єктів критичної інфраструктури.

Погоджуємось із думкою Зубко Г. Ю.[43], який наголошує на інституціональній недосконалості державної політики у розрізі захисту критичної інфраструктури в умовах військового стану в Україні. Її стратегічна рандомність, розпорошеність, а місцями фрагментарність, на переконання вченого, стає бар'єром на шляху монолітної стратегії національної безпеки. На основі даної позиції актуалізується питання щодо ефективної взаємодії і координації суб'єктів формування й реалізації державної політики у сфері захисту критичної інфраструктури. Варто зазначити, що у провідних країнах світу структурна дифузія систем реагування на ризики, загрози та небезпеки у сфері захисту критичної інфраструктури є важливим елементом державної політики. Наприклад, у США здатність таких систем взаємодіяти між собою характеризується спеціальним терміном «функціональна сумісність»[44]. Даний термін передбачає оптимальну здатність персоналу та обладнання відповідних структур оперативно отримувати та надавати функціональну підтримку, дані, інформацію та послуги при реагуванні на інциденти у сфері безпеки об'єктів критичної інфраструктури.

Отже, на сучасному етапі реформування сектору безпеки і оборони держави слід вважати доцільним формування мультиплікованої державної системи захисту критичної інфраструктури на основі існуючих систем захисту та кризового реагування. Практичної реалізації даної пропозиції можна досягнути на основі переходу до високого рівня координації дій та взаємодії між, що передбачає, зокрема, узгодження основних параметрів функціонування зазначених систем. До даної системи обов'язково має входити сектор превентивного та антикризового управління загрозами та ризиками, що застосовуватиметься у сфері захисту найважливіших об'єктів критичної інфраструктури та не обмежуватиметься лише національним рівнем. У деяких країнах уряди розробляють спеціальні галузеві плани. Даний сегмент чинитиме протидію стратегічним ризикам та загрозам критичній інфраструктурі на національному та міжнародному рівніях.

ВИСНОВКИ

Результати проведених досліджень дають підстави стверджуувати, що державна політика у сфері захисту критичної інфраструктури потребує удосконалення як мінімум у чотирьох областях:

[43] Зубко Г.Ю. Система суб'єктів реалізації державної інфраструктурної політики України. Правові новели. 2020. № 11. С. 166–178.

[44] Офіційний веб-сайт Міністерства внутрішньої безпеки США: DHS Lexicon Terms and Definitions. October 2017. URL: https://www.dhs.gov/

– урахування сьогоднішнього військового, соціально-політичного та економічного становища;

– урахування глобального аспекту завдань державного управління, у напрямку урахування світового досвіду з метою спрогнозувати світові поточні тенденції, зберегти українську самобутність і використовувати оптимальні варіанти вирішення проблемо забезпечення безпеки критичної інфраструктури за рахунок практичної підтримки міжнародних партнерів;

– використання наукового підходу до інтерпретації проаналізованого досвіду проблем державного управління з урахуванням новітніх фундаментальних наукових розробок у сфері безпеки об'єктів критичної інфраструктури;

– конструювання моделі ефективної взаємодії і координації суб'єктів формування й реалізації державної політики у сфері захисту критичної інфраструктури.

У загальному вигляді можна стверджувати, що перед державним управлінням стосовно забезпечення захисту об'єктів критичної інфраструктури поставлений ряд завдань: формування нових інститутів та оптимізація уже існуючих у сфері оборони; розвиток громадських інститутів у цій сфері та державно-громадської співпраці; формування та реалізація державної політики, спрямованої на забезпечення безпеки населення та захист об'єктів критичної інфраструктури; забезпечення безпеки регіонів України та мирних умов.

На сучасному етапі розбудови державної політики у сфері безпеки і оборони держави слід вважати доцільним формування привентивної мультиплікованої державної системи захисту критичної інфраструктури на основі існуючих систем захисту та кризового реагування, зокрема у напрямку інтеграції у міжнародний безпековий простір.

АНОТАЦІЯ

Проаналізовано міжнародні нормативно-правові акти на предмет сутнісного становлення поняття «критична інфраструктура». Спільним у множинності трактувань відзначається зв'язок із державними та приватними об'єктами, які мають певний вплив рівень обороноздатності та життєво важливі функції держави у суспільстві, а також акцентується увага на ключовому значенні даного сектору для безпеки громадян. Головною проблемою сучасного стану критичної інфраструктури, яка створила пролонгований у часі бар'єр для ефективної реалізації безпекових завдань визначено тривалу відсутність у законодавстві чіткого формулювання даного терміну та вичерпного переліку об'єктів віднесених до критичної інфраструктури. На основі аналізу

наукових підходів та іноземного досвіду теоретизування дефініції «критична інфраструктура» сформульовано авторське бачення змістовного наповнення даного терміну що відповідає принципам системності, цілеспрямованості, множинності галузей та відповідність антропоцентричному підходу.

Проаналізовано підходи вітчизняних та іноземних вчених до формулювання змісту поняття «загроза об'єктам критичної інфраструктури» у результаті чого помічено спільний акцент на видах ризиків і загроз, вплив яких може викликати диферентну дестабілізацію на різних ієрархічних рівнях, найвищий із яких – національна безпека.

Розглянуто зміст окремих нормативно-правових актів, що дало підстави деталізувати перелік загроз критичній інфраструктурі та підтвердити приналежність критичної інфраструктури до складових забезпечення національної безпеки України. На основі критичного аналізу узагальнено розподіл загроз критичній інфраструктурі на три основні категорії: природного походження, техногенного характеру і зловмисні дії. Запропоновано доповнити даний перелік комбінованими загрозами, які здатні викликати «каскадний ефект дестабілізації критичної інфраструктури».

Визначено прояви інституціональної недосконалості державної політики у розрізі захисту критичної інфраструктури в умовах військового стану в Україні. Її стратегічна рандомність, розпорошеність, а місцями фрагментарність розглядається як бар'єр на шляху розбудови монолітної стратегії національної безпеки. Окреслено ряд проблем у сфері державної політики захисту критичної інфраструктури та спроектовано окремі пропозиції їх вирішення.

Література

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. Аналітична записка. Проблеми забезпечення взаємодії при реагуванні на інциденти та кризи комплексного характеру на об`єктах критичної інфраструктури. URL: https://niss.gov.ua/sites/default/files/2018-09/Kondratov-81403.pdf

3. 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.;

4. Бірюков Д. С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні / Аналітична доповідь / Д. С. Бірюков, С. І. Кондратов. К. : ПП «Видавництво «ФЕНІКС», 2012. 92 с.

5. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. *Стратегічні пріоритети. Серія: Економіка.* 2015. № 4. С. 83–93.

6. Бобро Д. Г. Удосконалення методології ранжування об'єктів критичної інфраструктури та їх віднесення до критичної інфраструктури: аналітична записка. URL: http://www.niss.gov.ua/content/articles/files/krutuchna_infra-a7636.pdf

7. Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналіт. доп. за заг. ред. О. М. Суходолі. К.: НІСД, 2019. 224 с.

8. Богуцький П. П. Концептуальні засади права національної безпеки України: монографія. Київ – Одеса: Фенікс, 2020. 376 с.

9. 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.

10. 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.

11. Дзюба Т. М., Опанасенко М. І. Розроблення паспорту загрози для системи раннього виявлення загроз національній безпеці України. *Кібербезпека: освіта, наука, техніка.* 2021. № 4 (12). С. 61–68.

12. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року. URL: https://zakon.rada.gov.ua/laws/show/995_199#Text

13. 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.

14. Енциклопедія державного управління: у 8 томах. Нац. акад. держ. упр. при Президентові України. Київ : НАДУ, 2011.

15. Єрменчук О. П. Складові національної інфраструктури. Науковий вісник ДДУВС. 2017. № 4. С. 109–115.

16. Закон України «Про критичну інфраструктуру». від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20

17. Закон України «Про національну безпеку України» від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

18. 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

19. Закон України «Про правовий режим воєнного стану» № 389-VIII від 12.05.2015 р. URL: https://zakon.rada.gov.ua/laws/show/389-19#n29

20. Закон України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» № 2064-III від 19.10.2000 р. URL: https://zakon.rada.gov.ua/laws/show/2064-14#Text

21. 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.

22. Зубко Г. Ю. Система суб'єктів реалізації державної інфраструктурної політики України. *Правові новели.* 2020. № 11. С. 166–178.

23. Інституціоналізація публічного управління в Україні : наук.-аналіт. доп. Київ : НАДУ, 2019. 210 с.

24. Ліпкан В. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України / В. Ліпкан, І. Діордіца // *Підприємництво, господарство і право.* 2017. № 5. С. 174–180.

25. Офіційний веб-сайт Centre for the Protection of National Infrastructure. URL: http://www.cpni.gov.uk/

26. Офіційний веб-сайт National Infrastructure Simulation and Analysis Center. URL: https://www.cisa.gov/.

27. Офіційний веб-сайт Збройних Сил України. URL: https://www.zsu.gov.ua

28. Офіційний веб-сайт Міністерства внутрішньої безпеки США. URL: https://www.dhs.gov/

29. Офіційний веб-сайт Національного інституту стратегічних досліджень. URL: http://old.niss.gov.ua/articles/2213

30. Офіційний веб-сайт Служби безпеки України. URL: https://ssu.gov.ua/antyterorystychnyi-tsentr-pry-ssu

31. Порядок проведення моніторингу рівня безпеки об'єктів критичної інфраструктури. URL: https://zakon.rada.gov.ua/laws/show/821-2022-п#Text

32. Постанова Кабінету Міністрів України «Про затвердження Порядку функціонування державної системи фізичного захисту» № 1337 від 21.12.2011 р. URL: https://zakon.rada.gov.ua/laws/show/1337-2011-п#Text

33. Постанова КМУ «Деякі питання об'єктів критичної інфраструктури» від 09.10.2020 № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

34. Резнікова О. О. Паспорт сепаратистської загрози в Україні. *Стратегічні пріоритети.* 2018. № 2. С. 12–24.

35. Суходоля О. М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. *Стратегічні пріоритети.* 2016. № 3. С. 62–76.

36. Терещенко О. О. Антикризове управління фінансами підприємств : автореф. дис. … д-ра екон. наук. Київ, 2005. 34 с

37. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»» № 447/2021 від 26.08.2021 р. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n7

38. Указ Президента України. «Про Антитерористичний центр» № 1343/98 від 11.12.1998 р. URL: https://zakon.rada.gov.ua/laws/show/1343/98/ed19981211#Text

39. Цюрупа М. Зміна парадигм воєнно-політичного мислення у доктринах та стратегіях воєнної безпеки України XX–XXI ст. *Українознавчий альманах.* 2021. Вип. 28. С. 120–126.

40. USA Patriot Act of 2001. URL: https://www.gpo.gov/

41. 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.

42. 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/

43. 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

44. Merton, R.K. (1968). Social Theory and Structure. London: The Free Press of Glencoe, Collier-MacMillan Limited: 22-216

45. National Strategy for Critical Infrastructure Protection (CIP Strategy). URL: https://www.kritis.bund.de

46. Ustawa o zarządzaniu kryzysowym. Dz. U. 2007 Nr 89 poz. 590. URL: http://isap.sejm.gov.pl/isap.nsf/

Information about the authors:
Strahnitskyi Yaroslav Oleksandrovych
Graduate student of the Department of Public Administration
Vinnytsia Mykhailo Kotsiubynsky State Pedagogical University
32, Ostrozkoho str., Vinnytsia, 21000, Ukraine