## Інформаційна і національна безпека

УДК 354:340.133:340.134

**ЛЕОНОВ Б.Д.,** *доктор юридичних наук, професор,*
головний науковий співробітник МНДЦ при РНБО України.
ORCID: https://orcid.org/0000-0002-2488-7377.
**СЕРЬОГІН В.С.,** старший науковий співробітник Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.

# ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ АНТИДИВЕРСІЙНОЇ ЗАХИЩЕНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ

***Анотація.*** *Стаття присвячена аналізу проблем правового забезпечення антидиверсійної захищеності об'єктів критичної інфраструктури в умовах воєнного стану. Аналізуються законодавчі акти, які визначають особливості забезпечення захисту об'єктів критичної інфраструктури в цих умовах. Розглядається класифікація взаємозв'язків між об'єктами критичної інфраструктури. Визначається зміст системи антитерористичного та антидиверсійного забезпечення захисту критичної інфраструктури держави. Оцінюються підходи до захисту об'єктів критичної інфраструктури в провідних зарубіжних країнах. На базі аналізу позитивного досвіду окремих зарубіжних країн внесені пропозиції щодо вдосконалення Закону України "Про критичну інфраструктуру та її захист".*

***Ключові слова:*** *диверсія, антидиверсійна захищеність, об'єкти критичної інфраструктури, правове забезпечення, методичне забезпечення, воєнний стан.*

***Summary****. The article is devoted to the analysis of the problems of legal provision of anti-sabotage protection of critical infrastructure facilities in the conditions of martial law. Legislation is analyzed, which determines the features of ensuring the protection of critical infrastructure facilities in these conditions. The classification of relationships between critical infrastructure facilities is considered. The content of the system of anti-sabotage protection of the critical infrastructure facilities of the state is determined. Approaches to the protection of critical infrastructure facilities in leading foreign countries are being evaluated. Based on the analysis of the positive experience of foreign countries, proposals have been made to improve the Law of Ukraine "On Critical Infrastructure and its Protection".*

***Keywords:*** *sabotage, anti-sabotage protection, critical infrastructure facilities, legal support, methodological support, martial law.*

**Постановка проблеми.** Російська агресія в Україні, яка супроводжується обстрілами та знищенням об'єктів критичної інфраструктури, є безпрецендентним викликом не тільки для України, а й для Європи та світу в цілому. У зв'язку з військовою агресією Російської Федерації проти України, Указом Президента України від 24.02.22 р. № 64 в Україні введено воєнний стан. Цей стан 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.

Проблематика удосконалення захисту критичної інфраструктури ускладнюється триваючими бойовими діями, результатами аналізу нових підходів до забезпечення національної безпеки в розвинених країнах світу [1].

Відповідно до Стратегії забезпечення державної безпеки (далі – Стратегія), затвердженої Указом Президента України від 16.02.22 р. № 56/20**,** серед об'єктів державної безпеки виділяються об'єкти критичної інфраструктури. У Стратегії відзначається тенденція посилення для критичної інфраструктури загроз, пов'язаних з тимчасовою окупацією частини території України, триваючими гібридними впливами з боку суб'єктів розвідувально-підривної діяльності, погіршенням технічного стану такої інфраструктури, відсутністю інвестицій в її оновлення та розвиток, намаганнями несанкціонованого втручання в її функціонування, зокрема фізичного і кіберхарактеру (п. 19), а також триваючими бойовими діями (п. 27) [2].

Стратегія проголошує, що держава:

створить ефективну систему безпеки та стійкості критичної інфраструктури, засновану на чіткому розподілі відповідальності її суб'єктів та державно-приватному партнерстві.

модернізує транспортну інфраструктуру – дороги, залізниці, трубопроводи, аеропорти, морські і річкові порти тощо, у тому числі через механізми державно-приватного партнерства, прозорої приватизації з метою залучення внутрішніх та іноземних інвестицій в модернізацію і розвиток підприємства, сприяння зростанню продуктивності праці в економіці (п. 48) [2].

Сьогодні в Україні діє ціла низка законодавчих актів, що визначають особливості забезпечення захисту об'єктів критичної інфраструктури. Проте в державі досі відсутній загальний механізм управління захистом та безпекою цих об'єктів, спостерігаються непоодинокі випадки дублювання функцій уповноважених органів. Немає єдиних узгоджених підходів стосовно проблем національного масштабу. До того ж, загрози таким об'єктам розглядаються в суто "відомчому" розрізі.

Все це свідчить про необхідність впровадження на державному, регіональному та галузевому рівнях низки суттєвих заходів з: правового та організаційно-методичного забезпечення; координації та консолідованого забезпечення ресурсами систем забезпечення державної безпеки; спільного використання засобів безпеки, які перебувають в підпорядкуванні окремих міністерств, інших центральних органів виконавчої влади.

**Результати аналізу наукових публікацій**. Дослідження критичної інфраструктури є надзвичайно актуальними в багатьох країнах світу у зв'язку з суттєвим підвищенням рівня терористичних загроз в сучасних умовах. Вагомий внесок у розроблення методів, засобів і технологій ідентифікації об'єктів критичної інфраструктури внесено дослідженнями, проведеними зарубіжними вченими. Це, зокрема, праці Дуденхофера Д., Педерсена П., Пермана М., Маніка М. [1], Дженкінса Р. та Хофмана Б. [3]. Серед російських вчених, які опікувалися цією проблемою, слід виділити роботи Алексеєва О. [4] та Кондратьєва О. [9], які розглядали сучасні тенденції розвитку антитерористичного захисту критичної інфраструктури в зарубіжних країнах. В Україні дослідженням проблемних питань захищеності об'єктів критичної інфраструктури займалися такі науковці, як Антипенко В. [5], Кондратов С., Крутов В. [6], Кудінов С. [7], Рижов І. [8] та інші.

Незважаючи на те, що останнім часом з'явилася значна кількість публікацій, присвячених проблемам антитерористичної захищеності об'єктів критичної інфраструктури, залишається недостатньо дослідженим питання методології забезпечення антидиверсійної захищеності таких об'єктів, на підставі якої може бути впроваджений методологічний апарат для аналізу критичної інфраструктури та оцінки

захищеності об’єктів критичної інфраструктури з метою забезпечення національної безпеки та відсічі збройної агресії в умовах воєнного стану.

**Метою статті** є удосконалення на базі аналізу досліджень захисту об’єктів критичної інфраструктури нормативно-правового забезпечення антидиверсійної захищеності об’єктів критичної інфраструктури України в умовах воєнного стану.

**Виклад основного матеріалу.** Сучасні війни та збройні конфлікти не обмежуються лише бойовим зіткненням збройних сил (формувань) протиборчих сторін. Під час такого зіткнення особливого захисту потребують об’єкти критичної інфраструктури. Частину цивільної інфраструктури, зміст якої складає сукупність важливих для держави фізичних або віртуальних систем і засобів, знищення або виведення з ладу яких може заподіяти тяжкі наслідки у сфері оборони, економіки, охорони здоров’я та безпеки нації, прийнято називати критичною [9].

На думку зарубіжних експертів [10; 11], критична інфраструктура являє собою складну систему, яка характеризується атрибутами, серед яких виділяється: 1) необмежена кількість варійованих об’єктів та параметрів системи; 2) важко прогнозована поведінка об’єктів, для яких характерна велика кількість взаємозв’язків, які класифіковано по різних секторах [12].

У роботі “Розкриття, розуміння й аналіз взаємозв’язків об’єктів критичної інфраструктури” [13] представлена класифікація взаємозв’язків між об’єктами критичної інфраструктури, зміст якої складають: фізичний, кібернетичний, географічний (топологічний), логічний.

У роботах інших зарубіжних дослідників [1] зустрічається більш уточнена класифікація взаємозв’язків за характером:

фізичний – визначає інженерну взаємозалежність між об’єктами;

інформаційний – залежність від інформаційного обміну (потоку інформації) між об’єктами;

геопросторовий – взаємозалежність виникає в результаті спільного розташування компонентів інфраструктури на місцевості.

Наприклад, повінь або пожежа виводить з ладу всі розміщені на площі стихійного лиха об’єкти мережі; процедурний (політичний) – подібна взаємозалежність виникає при будь-якій зміні (події) в одному з компонентів сектору інфраструктури й спричиняє вплив на об’єкти інших секторів; соціальний – така взаємозалежність може мати вираження через соціальні фактори: суспільна думка, суспільна довіра, страх тощо.

З наведеної класифікації випливає, що критична інфраструктура будь-якої держави є не що інше, як велика складна система стратегічного масштабу, що представляє собою сукупність значної кількості елементів різного типу, об’єднаних зв’язками різної природи, для яких характерна загальна властивість (призначення, функція), яка відмінна від властивостей окремих елементів усієї сукупності, що й вимагає розробки спеціальних методів дослідження [9].

В Україні ще за радянських часів існувала збалансована система управління техногенною безпекою об’єктів підвищеної небезпеки, в основу якої покладено методологічний підхід аналізу ризиків, які обумовлювалися надійністю функціонування елементів, складових, об’єктів тощо. Іншими словами, ризик виникнення надзвичайної ситуації визначався вірогідністю відмов природнього характеру, аварій, інших надзвичайних подій (ймовірність виникнення та розвитку подій внаслідок умисного пошкодження елементів не враховувалась та не розглядалася взагалі). Проте, антитерористичне (антидиверсійне) забезпечення передбачає інший підхід, в основу якого покладено оцінку можливих сценаріїв вчинення диверсій та терористичних актів

(та їх прогнозованих наслідків), спрямованих в найбільш уразливе місце об'єкта (що призводить до максимально можливих втрат з мінімальними витратами ресурсів), в найбільш незручний час з точки зору функціонування (виробничого циклу) об'єкта і стану його системи фізичного захисту. Оцінка можливих сценаріїв вчинення терористичних актів потребує, в свою чергу, отримання результатів розрахунку прогнозованих людських, економічних, екологічних, суспільно-політичних, культурних та інших втрат внаслідок події можливих впливів на об'єкт терористичного чи диверсійного характеру [14, с. 92]. Зауважимо, що реалії сьогодення свідчать, що окремі прояви збройної агресії РФ мають елементи як диверсії, так і терористичного акту.

Створення системи забезпечення антитерористичного та антидиверсійного захисту критичної інфраструктури держави зумовлює:

– законодавче визначення повноважень уповноваженого органу з питань захисту критичної інфраструктури України з науково-технічного забезпечення процедур захисту об'єктів критичної інфраструктури (у т.ч. реалізації функцій з координації, здійснення контролю та нагляду, експертної оцінки, організації заходів компенсаційного та превентивного характеру тощо);

– створення науково-дослідних установ, які будуть забезпечувати науково-технічне супроводження функціонування системи аналізу стану критичної інфраструктури та здійснювати експертизу з оцінки прогнозування наслідків впливів на стійкість об'єктів критичної інфраструктури;

– розробку та впровадження необхідного методичного та нормативного забезпечення аналізу та прогнозування наслідків диверсії або терористичних актів [14, с. 92].

Питання правового врегулювання у сфері захисту критичної інфраструктури в Україні досить нагальне. Проблемою є фактична відсутність дієвої узгодженої політики у сфері захисту об'єктів критичної інфраструктури, що зумовлюється як відсутністю системного підходу на національному рівні, так і законодавчою невизначеністю форм взаємодії державних органів між собою. Незважаючи на низку законів та інших нормативно-правових актів, що визначають повноваження й компетенцію державних органів у цій сфері, в Україні досі бракує системного підходу до управління комплексом таких систем та об'єктів. Відсутні й будь-які узгоджені прояви здійснення державно-приватного партнерства у сфері захисту критичної інфраструктури, що є одним з пріоритетних напрямів з огляду на на світовий досвід.

Вочевидь, держава не зможе ефективно боротися з можливою небезпекою, знаходячись у правовому вакуумі, тож необхідно якнайшвидше заповнити цю прогалину.

Сьогодні в Україні функціонують три окремі системи захисту :

1) Єдина система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (Положення про яку затверджено постановою Кабінету Міністрів України від 15.08.07 р. № 1051);

2) Єдина державна система запобігання і реагування на надзвичайні ситуації техногенного та природного характеру (Положення про яку затверджено постановою Кабінету Міністрів України від 03.08.98 р. № 1198, зі змінами від 29.07.99 р. № 1376, від 09.08.01 р. № 1006, від 15.05.03 р. № 717, від 04.09.03 р. № 1402, від 08.12.06 р. № 1700),

3) Єдина державна система цивільного захисту населення і територій (Закон України "Про правові засади цивільного захисту" від 24.06.04 р. № 1859-IV).

Ці системи, які діють паралельно, створені, в тому числі для захисту життєво важливих для держави об'єктів від окремих видів загроз. Це створює ситуацію, яка свідчить про домінування відомчих підходів до розв 'язання безпекових проблем національного масштабу.

За цих умов неможливо уникнути, з одного боку, дублювання функцій уповноважених органів та розпорошення їх ресурсів, а з іншого – неузгодженостей у розподілі повноважень щодо захисту об'єктів та систем, критично важливих для існування держави, захисту національних інтересів, забезпечення безпеки населення та довкілля. Не сприяє виробленню єдиних підходів до захисту таких об'єктів слабкість та брак існуючих механізмів координації зусиль міністерств, інших центральних органів виконавчої влади із забезпечення захисту об'єктів, які у світі прийнято відносити до критичної інфраструктури.

Внаслідок цього, у державі зростають ризики шкідливих та небезпечних дій стосовно об'єктів критичної інфраструктури.

Особливої уваги потребує вирішення цих питань в умовах воєнного стану.

У зв'язку з цим потребують переосмислення концепції захисту критичної інфраструктури України, методології оцінки загроз критичній інфраструктурі та механізмів реалізації режиму реагування на виникнення кризової ситуації при проведені військових операцій з метою формування плану невідкладних заходів із захисту критичної інфраструктури в умовах воєнного стану.

Під час такої роботи слід взяти до уваги результати зарубіжних військово-теоретичних досліджень, зокрема таке базове понятя, як "центр ваги".

Свого часу німецький військовий теоретик К. Клаузевиц одним з перших запропонував теорію, зміст якої полягав у тому, що "центр ваги" – це певна "центральна точка" збройних сил та держави, навколо якої все й обертається [15].

У подальшому у підходах зарубіжних вчених до захисту об'єктів критичної інфраструктури поступово відбувалися зміни під впливом тих чи інших подій.

Враховуючи, що більшість систем критичної інфраструктури мають мережеву архітектуру, Т. Льюісом була висунута гіпотеза, що захищати, у першу чергу, слід ключові "вузли" цих систем[16]. Саме у такий спосіб з'являється можливість слідувати так званому "правилу 80 – 20 %", коли 80 % ресурсів мають витрачатися на 20 % території країни, а також використовувати теорію мереж для організаційних і фізичних структур, призначених для організації захисту критичної інфраструктури.

В іншій роботі "Розуміння центрів ваги та вразливих елементів" зазначається, що "центральна точка", яка має відношення до збройних сил противника, може бути як фізичною, так і моральною [17]. Така точка може бути на стратегічному, оперативному чи тактичному рівні. У доктрині НАТО [18] "центр ваги" описується як потенціал або місце, де держави, альянси, бойові формування чи інші типи збройних угруповань концентрують свої можливості для досягнення свободи дій, фізичної сили та готовності вести боротьбу.

Схожий підхід запропонував у своїй роботі "Центри ваги у військових операціях" співробітник коледжу Королівських ЗС Швеції Д. Варден в контексті реалізації можливостей щодо: термінового зосередження сил та засобів на ключових напрямках наступу або критичних місцях оборони військових формувань [19]; створення моделі захисту критичної інфраструктури в умовах воєнного стану (так званого "воєнізованого суспільства").

Погоджуючись з тим, що супротивник має вивчатися як система, яка складається з різноманітної кількості взаємозалежних об'єктів, Д. Варден вважає, що базовий об'єкт такої системи – це енергія різного виду: фізична (люди, будівлі, системи зв'язку та зброї) або психологічна (сила волі, можливості та здібності) [19]. І якщо є можливість направити спеціальний потік енергії до центральної частини такої системи, то вона може бути знищена або виведена з ладу. В подібній системі, побудованій з певної

кількості об’єктів та об’єднаних певною мережею, як правило, є кілька ключових, вплив на які може призвести до виходу всієї системи з ладу.

До ключових секторів критичної інфраструктури, які безпосередньо впливають на забезпечення військових операцій, та захист яких вважається пріоритетним в умовах воєнного стану, відносять два сектори – це енергетика і транспорт. До сектору енергетики були включені такі системи та об’єкти: електромережі та об’єкти із генерування та передачі електроенергії; нафтовидобувна та нафтопереробна промисловість, нафтопроводи та сховища; газовидобувна промисловість, газопроводи, термінали зрідженого газу. До сектору транспорту віднесли такі його види та об’єкти: автодорожній транспорт; залізничний транспорт; авіаційний транспорт; річковий флот; океанічний і морський флот; порти [20].

“Центри ваги” в кожному секторі критичної інфраструктури формуються відповідно до економічних законів, законів соціального розвитку, еволюції та військової стратегії, що дозволяють формуватися самоорганізуючим мережам. Саме поява подібних “центрів ваги” може призвести до самоорганізації мережі та можливості її ефективного функціонування.

Зважаючи на досвід провідних країн світу, питання побудови ефективних механізмів реагування на загрози, небезпеки і ризики має стати невід’ємною частиною системи національної безпеки. Цей досвід, а також постійний пошук механізмів удосконалення сфери захисту об’єктів критичної інфраструктури мають спонукати вітчизняного законодавця до активних дій в цьому напрямку.

Адже діюча сьогодні нормативно-правова база у сфері захисту об’єктів критичної інфраструктури є вочевидь недостатньою. Закон України “Про основні засади забезпечення кібербезпеки України” впроваджує визначення об’єкта критичної інфраструктури, визначає повноваження для переліку об’єктів критичної інфраструктури, проте не встановлює критеріїв ідентифікації таких об’єктів. І хоча держава намагається робити певні кроки у цьому напрямку (зокрема, почато процес вступу України до Об’єднаного центру передових технологій з кібероборони НАТО; затверджена Стратегія кібербезпеки України), цих зусиль явно не достатньо.

З метою підвищення ефективності правового регулювання в контексті захисту критичної інфраструктури 16 листопада 2021 року Верховною Радою України прийнято Закон України “Про критичну інфраструктуру та її захист”, який набув чинності з 15.06.22 р. [21]. Цей Закон визначає основні терміни, принципи, засади та діяльність у сфері захисту критичної інфраструктури.

Водночас, незважаючи на його прогресивний характер, нагальною є потреба його вдосконалення для того, щоб:

визначити критерії й методологію ідентифікації об’єктів критичної інфраструктури, а також запровадити комплексний підхід до їх захисту;

визначити уповноважений орган з питань захисту критичної інфраструктури України та забезпечити реалізацію режиму реагування на виникнення кризової ситуації в умовах воєнного стану;

Не менш важливим напрямом є ефективна міжнародна співпраця, адже оптимізація механізмів забезпечення захисту об’єктів критичної інфраструктури має базуватися на формуванні ефективної моделі забезпечення безпеки.

Ще одним питанням, яке виникає при системному впровадженні концепції захисту критичної інфраструктури в Україні, є залучення до цієї діяльності Збройних Сил України в умовах воєнного стану та надзвичайної ситуації. Низка законів України, серед яких виділяються закони України “Про правовий режим надзвичайного стану”, “Про

правовий режим воєнного стану", "Про мобілізаційну підготовку та мобілізацію", містять положення про координацію дій та концентрацію зусиль державних органів у певних умовах особливого періоду часу (охоплює час мобілізації, воєнний час і частково відбудовний період) або надзвичайного стану, зміст яких спрямований на організацію діяльності державних органів у разі воєнної загрози або захисту від наслідків надзвичайних ситуацій техногенного, екологічного, природного та воєнного характеру. Однак у цих законах не згадуються терористичні загрози.

Аналогічний підхід спостерігається й у законах "Про оборону України", "Про цивільну оборону України", "Про функціонування єдиної транспортної системи України в особливий період", "Про транспорт" (ст. 15 "Організація роботи транспорту у надзвичайних умовах"), "Про трубопровідний транспорт", (ст. 18 "Організація роботи підприємств, установ та організацій трубопровідного транспорту в умовах надзвичайного стану"). У новій редакції Воєнної доктрини України (п. 23) серед пріоритетних напрямів підготовки держави до збройного захисту національних інтересів згадується "розвиток інфраструктури регіонів з урахуванням потреб підготовки території держави до оборони" [22].

Зазначені законодавчі акти не містять єдиного підходу до залучення Збройних Сил України до забезпечення захисту обєктів критичної інфраструктри в умовах воєнного стану.

Визначення такого підходу на законодавчому рівні було б цілком логічним, зважаючи на об'єктивні реалії сьогодення, коли відбуваються бойові зіткнення збройних сил України та Росії.

У державі необхідно запровадити єдину термінологію з урахуванням узгоджених підходів до створення системи антитерористичного забезпечення захисту критичної інфраструктури держави.

Одним з важливих елементів цієї системи є створення та впровадження єдиного методичного апарату для проведення технічної та судової експертизи у даній галузі, який має враховувати взаємозв'язки різного рівня між елементами окремого об'єкта, об'єктів між собою, об'єкта та системи, а також різних систем.

Для вирішення цього завдання в Українському науково-дослідному інституті спеціальної техніки та судових експертиз СБУ впроваджено нові експертні спеціальності. Зокрема, до основних завдань експертизи за спеціальністю 5.3 "Оцінка можливих наслідків застосування вибухового пристрою (вибуху)" належать: надання висновку щодо здатності досліджуваного вибухового пристрою (вибухової системи) до вибуху; надання оцінки щодо потужності вибуху, наслідків дії вибуху (у т.ч. параметрів вибухової хвилі, фугасної та бризантної дії, радіусу та ступеня осколкових уражень, термічної дії); оцінка ступеня ураження факторами вибуху існуючих (розташованих) в межах дії безпосередніх факторів вибуху об'єктів (в т.ч. будівель, споруд, машин, механізмів, транспортних засобів, обладнання тощо), а також людей та інших об'єктів, а за наявності, негативних наслідків іншого характеру; оцінка достатності існуючого рівня захищеності об'єктів дослідження до впливу безпосередніх факторів вибуху; у разі необхідності обґрунтування рекомендацій з підвищення рівня живучості (стійкості) об'єктів дослідження та систем в цілому; встановлення причинових зв'язків між існуючим станом захисту об'єктів дослідження та настанням наслідків в результаті впливу факторів прогнозованого вибуху; встановлення причинових зв'язків між діями (бездіяльністю) певних відповідальних осіб та настанням негативних наслідків в результаті застосування вибухових пристроїв (вибуху).

До основних завдань судової експертизи за спеціальністю 5.5 “Оцінка наслідків впливу технічних факторів диверсії (терористичного акту) іншої надзвичайної ситуації” належать: визначення ступеня впливу на об’єкт дослідження (систему) технічних факторів диверсії, терористичного акту чи іншої надзвичайної ситуації з оцінкою можливості їх подальшого функціонування; надання прогнозу розвитку та наслідків каскадної аварії в результаті взаємозалежності суміжних систем об’єктів та впливу на них технічних факторів диверсії, терористичного акту чи іншої надзвичайної ситуації; визначення необхідних та достатніх вимог забезпечення функціонування об’єкта (системи в цілому) з урахуванням прогнозованого рівня загроз, а також відповідності існуючого стану захисту об’єктів вимогам діючих нормативних актів; за потреби надання рекомендацій з підвищення рівня захисту об’єктів дослідження та систем в цілому; встановлення причинових зв’язків між діями чи бездіяльністю певних відповідальних осіб та настанням негативних наслідків в результаті можливої реалізації диверсії чи терористичного акту.

Впровадження зазначених експертних спеціальностей спрямоване на всебічне експертне дослідження аспектів захисту об’єктів критичної інфраструктури, яке передбачає врахування взаємозв’язків різного рівня та різного характеру взаємозалежностей об’єктів та систем [14, с. 93].

Для вирішення широкого кола різнопланових завдань з оцінки (прогнозування) наслідків системного характеру (диверсій, терористичних актів чи інших надзвичайних ситуацій) в рамках експертних спеціальностей 5.3 та 5.5 розробляється проект методики, який містить загальний методичний підхід, зміст якого передбачає системне врахування причинових зв’язків різного рівня та характеру. Такий підхід базується на структуризації наслідків події різного характеру, а саме:

– наслідків І роду – наслідків безпосередньо фізичного впливу на об’єкт дослідження факторів диверсії або терористичного акту;

– наслідків ІІ роду – наслідки, що настають для інших пов’язаних елементів об’єкта в межах однієї системи, і є результатом опосередкованого впливу наслідків І роду на інший його елемент;

– наслідки ІІІ роду – наслідки, що настають для суміжних систем, що пов’язані зв’язками різного характеру (фізичні, інформаційні, геопросторові, процедурні (політичні), соціальні), і є результатом впливу наслідків І та ІІ роду.

Цей системний підхід може слугувати базисом для подальшого удосконалення методичного забезпечення експертних досліджень з оцінки (прогнозування) наслідків диверсії або терористичного акту та аналізу ступеня захисту об’єктів критичної інфраструктури [14, с. 93-94].

Проблема запровадження системного підходу до розв’язання проблем захищеності критичної інфраструктури, звичайно, виходить далеко за межі лише понятійного та методологічного апарату. На перше місце висувається завдання створення дієвого механізму координації зусиль органів влади, спрямованих на недопущення втрати чи завдання невиправної шкоди ключовим (вузловим) елементам критичної інфраструктури внаслідок дії негативних факторів будь-якого походження, або техногенного, або природного, або соціально-політичного, або будь-якої комбінації з їх числа [23, с. 3].

**Висновки.**

На базі аналізу досліджень у сфері антидиверсійного захисту об’єктів критичної інфраструктури можна дійти висновку, що методичне забезпечення таких об’єктів в Україні потребує вдосконалення за напрямами:

– методів ідентифікації та градації об’єктів критичної інфраструктури;

– проведення аналізу ризиків та узагальнення вимог до рівнів захищеності (обґрунтування рівнів проектних загроз) об’єктів в залежності від вразливості об’єкта та масштабів його впливу на інші об’єкти та системи;

– аналізу та визначення найбільш ймовірних сценаріїв терористичних актів та диверсій на об’єктах критичної інфраструктури в умовах воєнного стану;

– розробки правил антитерористичної безпеки для об’єктів різного функціонального призначення;

– нормативної регламентації діяльності органів і підрозділів СБУ із захисту об’єктів критичної інфраструктури;

– визначення уповноваженого органу з питань захисту критичної інфраструктури України;

– забезпечення якнайшвидшого прийняття нормативно-правових актів, необхідних для реалізації Закону України “Про критичну інфраструктуру та її захист”;

– методичного забезпечення експертних досліджень стосовно критичної інфраструктури.

## Використана література

1. Dudenhoeffer D.D., Permann M.R. and Manic M. CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis. Submitted to Proceedings of the 2006. Conference: Proceedings of the Winter Simulation Conference WSC 2006, Monterey, California, USA, December 3-6. 2006. URL: https://www.researchgate.net/publication/221527820_CIMS_A_Framework_for_Infrastructure_ Interdependency_Modeling_and_Analysis (дата звернення: 19.06.2020).

2. Стратегія забезпечення державної безпеки: Указ Президента України від 16.02.22 р. № 56. URL: https://www.president.gov.ua/documents/562022-41377

3. Hoffman, B. Inside Terrorism. N.Y.: Columbia University Press, 1999. 465 p.

4. Алексеев О.Н. Противодействие терроризму в США: опыт и проблемы. *Теория и практика общественного развития*. 2012. № 7. С. 201-203. URL: https://cyberleninka.ru/article/n/protivodeystvie-terrorizmu-v-ssha-opyt-i-problemy (дата звернення: 19.06.2020).

5. Антипенко А.Ф. Міжнародна кримінологія: досвід дослідження тероризму : монографія. Одеса. Фенікс, 2011. 317 с.

6. Крутов В.В., Форноляк В.М. Система суб’єктів боротьби з тероризмом, їх адміністративно-правовий статус. *Інформаційна безпека людини, суспільства, держави.* 2019. Вип. 2. С. 56-64. URL: http://academy.ssu.gov.ua/ua/page/page_1581342762.htm (дата звернення: 19.06.2020).

7. Кудінов С.С. Міжнародний досвід протидії тероризму та його значення для України. *Вчені записки ТНУ імені В.І. Вернадського*. *Серія: юридичні науки*. 2019. № 1. Т. 30. С. 117-123.

8. Рижов І.М. Базові концепти антитерористичної безпеки: монографія. Київ: Нац. акад. СБУ, 2016. 327 с. С. 9; Executive Order. 13010. Critical Infrastructure Protection. Federal Register. Vol. 61, № 138. July 17. 1996. P. 3747-3750.

9. Кондратьев А. Современные тенденции в исследовании критической инфраструктуры в зарубежных странах. *Зарубежное военное обозрение*. 2012. № 1. С. 19-30. URL: http://pentagonus.ru/publ/sovremennye_tendencii_v_issledovanii_kriticheskoj_infrastruktury_v_zarubezhnoj_stranakh_2012/19-1-0-2082 (дата звернення: 19.06.2020).

10. Keating C, Rogers, R., Dryer D., Sousa-Poza A., Safford R., Peterson W., Rabadi G. System of Systems Engineering. Engineering Management Journal. 2003. Vol. 15. № 3.

11. Jackson, M. Systems Methodology for the Management Sciences. New York. Plenum, 1991. 298 p.

12. Congressional Research Service Report for Congress. Critical Infrastructures: Background, Policy and Implementation. 2002. URL: https://fas.org/sgp/crs/homesec/RL30153.pdf (дата звернення: 19.06.2020).

13. Rinaldi S., Peerenboom J. and T. Kelly. Idenlifying, Understanding and Analyzing Critical Infrastructure lnterdependencies. IEEE Control Systems Magazine, IEEE, December 2001. P. 11-25.

14. Леонов Б.Д., Шостак Р.М., Серьогін В.С. Розвиток методичного забезпечення антитерористичної захищеності об'єктів критичної інфраструктури (на прикладі США) *Інформація і право*. № 3(34)/2020. С. 92-93.

15. Clausewitz C-V. On War. Перекл. Дж.Дж. Грехем. 1997 Wordsworth Editions. 374 p.

16. Lewis T.G., Critical infrastructure protection in homeland security: defending a networked nation. New Jersey: John Wiley & Sons, 2006. 474 p.

17. Strange. J. Iron R. Understanding Centres of Gravity and Critical Vulnerabilities. 2001. 90 p. URL: https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/3B_COG_and_Critical_Vulnerabilities.pdf.

18. Военная доктрина НАТО. URL: https://www.armyua.com.ua/voennaya-doktrina-nato

19. Warden, J. Centers of gravity in military operations. Preliminary draft. Royal Swedish Defence College. 2004. 185 p.

20. Strange. J., Iron R. Understanding Centres of Gravity and Critical Vulnerabilities. 2001. 25 p.

21. Про критичну інфраструктуру та її захист: Закон України від 16.11.21 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

22. Про рішення Ради національної безпеки і оборони України від 08.06.12 р. "Про нову редакцію Воєнної доктрини України": Указ Президента України від 08.06.12 р. № 390: URL: http://zakon2.rada.gov.ua/laws/show/390/2012

23. Бірюков Д.С., Кондратов С.І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні: аналітична доповідь. 2012. 57 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~