УДК 351.862.4:340.13+338.583(477)

Д. М. Павлов

М. А. Микитюк

ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У КОНТЕКСТІ ФОРМУВАННЯ НОВОЇ БЕЗПЕКОВОЇ ПАРАДИГМИ УКРАЇНИ

Проведено аналіз правових та організаційно-управлінських проблем підвищення ефективності забезпечення захисту критичної інфраструктури держави в Україні у контексті формування нової безпекової парадигми, що базується на пріоритеті загальнолюдських, базових цінностей та ідеалах людської спільноти. Розглянуто вплив підвищення ефективності державно-приватного партнерства на рівень безпеки та стійкості критичної інфраструктури. Сформульовано й обґрунтовано тезу про те, що розгляд національної безпеки, передусім, як захисту буття нації спонукає її звернутися до національної ідеї, крізь призму якої народ осмислює своє буття і відповідно до якої визначає свої національні цінності та національні інтереси. За таких умов філософська категорія безпеки і національна ідея можуть стати методологічною основою нової парадигми національної безпеки та організаційно-правових заходів щодо її забезпечення.

Ключові слова: *державно-приватне партнерство, кібербезпека, критична інфраструктура, національна безпека, об'єкт критичної інфраструктури, тероризм, цивільний захист.*

Постановка проблеми. В Україні дедалі активніше відбувається формування нової парадигми національної безпеки, що базується на пріоритеті загальнолюдських, базових цінностей та ідеалах людської спільноти. Національна безпека в сучасних умовах характеризує можливості та здатність суспільства забезпечувати захист національних інтересів від різних за змістом і характером небезпек і загроз, підтримувати необхідний рівень безпеки особистості, суспільства і держави. Така соціальна роль національної безпеки означає, що вона є складним за структурою явищем, яке охоплює і систему умов та факторів захисту національних інтересів, і процес використання ресурсів та можливостей суспільства для збереження, підтримки й удосконалення цих умов і факторів [1, с. 36–43]. Державам, у яких реформування безпекового сектора відбувається на тлі збройних конфліктів (в активній чи замороженій стадіях), важливо уникнути спокуси відкласти питання безпеки людини до "кращих часів" і сфокусуватися лише на традиційній державній безпеці. І хоча традиційні загрози залишаються життєво важливими, що підтверджує в тому числі й агресія Росії проти України, парадигма людської безпеки, яка ставить людину в центр уваги, має бути знаменником реформування безпекового сектора в державах, які обрали сучасну демократичну модель розвитку. Державна безпека і безпека людини мають не протиставлятися, а взаємно доповнювати одна одну, адже лише ті суспільства можуть бути стійкими, де людина належно захищена від усього комплексу загроз, де гарантована безпека людини в сучасному, всеохоплюючому сенсі цього концепту [2].

У наукових джерелах наголошується, що результатом складної трансформації поняття "безпека" у сучасному світі стало поповнення безпекового дискурсу концепцією "людська безпека" (human security), що знаменує собою перенесення фокуса у міжнародних відносинах від держави до окремих індивідуумів та спільнот. Твердження, що безпека кожного індивідуума автоматично походить від безпеки

держави, більше не розцінюється як аксіома. Відбувається заміна (а точніше, доповнення) державоцентричного поняття "національна безпека" більш гуманістичним, мікроорієнтованим поняттям "людська безпека". Той факт, що цей концепт успішно інкорпорується в зовнішньополітичні стратегії багатьох країн і стає звичним терміном у безпековому наративі ООН та її агенцій, ЄС, інших міжнародних організацій і держав, є важливим показником її цінності й своєчасності. Людська безпека як захист індивідуума від критичних загроз його існуванню та добробуту є актуальною у глобальному масштабі. Загрози людській безпеці численні: від міжнародного тероризму до асиметричних конфліктів зі значними жертвами серед цивільного населення; від стихійних явищ до проблем економічної й екологічної деградацій. З огляду на взаємопов'язаний характер усіх цих загроз людська безпека об'єднує їх у єдину систему, пропонуючи вирішувати їх комплексно, координуючи діяльність усіх тих агенцій, які займаються цими питаннями. Незалежно від критичного ставлення деяких представників академічних та політичних кіл цей концепт уже неможливо ігнорувати, адже він активно увійшов у безпековий дискурс [3].

Людська безпека – це не просто лейтмотив поведінки або аналітичний ярлик, це, швидше, "активний стратегічний наратив" [4], точка відліку чи загальні рамки для дій у сфері безпеки. Власне кажучи, наявність такого концепту спричинила переосмислення безпекової парадигми в сучасному світі й у нашій державі.

Автори статті поділяють думку В. М. Пасічника про доцільність перегляду існуючої парадигми національної безпеки як стану захищеності тільки інтересів та цінностей. Осмислення поняття "безпека" крізь призму філософської категорії "буття" дає змогу поєднати загальноприйнятий статистичний підхід з апофатичним, діяльнісним і нормативним підходами. У свою чергу, розгляд національної безпеки, передусім, як захисту буття нації спонукає її звернутися до національної ідеї, крізь призму якої народ осмислює своє буття і відповідно до якої визначає свої національні цінності та національні інтереси. За таких умов філософська категорія безпеки й національна ідея можуть стати методологічною основою нової парадигми національної безпеки та організаційно-правових заходів щодо її забезпечення.

Практичне значення зміни парадигм національної безпеки полягає у тому, що попередня парадигма була зорієнтована на забезпечення безпеки у якійсь сфері, коли вже реально виникла загроза національній безпеці. На відміну від неї нова парадигма національної безпеки, що розглядає безпеку крізь призму захисту буття особи, суспільства, держави, нації, людства загалом, передбачає лікування не якоїсь окремої хвороби, а організму загалом, ставить наголос на боротьбі не з наслідками, а з причинами цієї хвороби [5]. Саме у такому контексті має формуватися політика захису критичної інфраструктури держави.

Аналіз останніх досліджень і публікацій. Дослідженню проблематики правового регулювання та організації забезпечення національної безпеки увагу приділяли у своїх працях такі вітчизняні вчені, як Ю. Азаров, В. Антонов, А. Берлач, В. Богуш, В. Горбулін, С. Засунько, В. Колпаков, С. Константінов, О. Копан, С. Кузніченко, О. Кузьменко, Л. Жукова, О. Маркєєва, В. Настрадін, Н. Нижник, В. Білоус, В. Ліпкан, І. Рижов, Б. Розвадовський, Г. Ситник, О. Суходоля, О. Труш, А. Чубенко та інші. Водночас з урахуванням складного та багатоаспектного характеру проблематики правового й організаційного забезпечення національної безпеки, динамічного характеру безпекових відносин зберігається нагальна потреба поглибленого аналізу питань захисту критичної інфраструктури.

Метою статті є теоретико-правовий аналіз особливостей забезпечення захисту критичної інфраструктури в умовах формування в Україні нової парадигми національної безпеки, розроблення на цій основі пропозицій до законодавства.

Виклад основного матеріалу. Формування в Україні дієвої системи захисту критичної інфраструктури у контексті зміни парадигми національної безпеки має відбуватися шляхом максимального залучення до цього процесу не лише органів публічної адміністрації, а й представників громади. Світовий досвід свідчить, що одним із головних елементів забезпечення належного рівня безпеки та стійкості критичної інфраструктури є, зокрема, ефективне державно-приватне партнерство. Його налагодження у сфері захисту критичної

інфраструктури в Україні має стати невід'ємним напрямом забезпечення національної безпеки [6].

Терміном "критична інфраструктура" зазвичай охоплюють об'єкти, системи, мережі або їх частини, порушення функціонування або руйнування яких призведе до найтяжчих наслідків для соціальної й економічної сфер держави, негативно вплине на рівень її обороноздатності та національної безпеки. Крім того, функціонування критичної інфраструктури в мирний час пов'язується із підтримуванням життєво важливих функцій у суспільстві, захистом базових потреб його членів і формуванням у них відчуття безпеки й захищеності [7]. У законодавстві США під терміном "критична інфраструктура" розуміють "системи та ресурси, фізичні чи віртуальні, настільки життєво важливі для Сполучених Штатів, що недієздатність або знищення таких систем або ресурсів підриває національну безпеку, національну економіку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з переліченого" (Patriot Act, 2001) [8]. Європейський Союз визначає критичну інфраструктуру як системи, які мають важливе значення для підтримки життєво важливих соціальних функцій. Пошкодження критичної інфраструктури, її руйнування або порушення в результаті стихійних лих, тероризму, злочинної діяльності чи зловмисної поведінки може істотно негативно вплинути на безпеку ЄС і добробут громадян [9, 10, 11]. У наукових публікаціях термін "критична інфраструктура" визначають як фізичні й віртуальні системи, об'єкти і ресурси, руйнування, знищення або зниження дієздатності яких призведе до суттєвих загроз країні (регіону або місту), її національній безпеці, безпеці й здоров'ю населення [12].

В Україні термін "критична інфраструктура" використовували в нормативно-правових актах, проте його легальне визначення й досі відсутнє. Уперше в офіційних документах цей термін з'явився у 2006 р. у тексті Рекомендацій парламентських слухань з питання розвитку інформаційного суспільства, на жаль, без подальшого розвитку. У Стратегії національної безпеки України "Україна у світі, що змінюється" (2012 р.) цей термін згадувався під час визначення способів зміцнення енергетичної безпеки та напрямів забезпечення інформаційної безпеки. У Стратегії національної безпеки України (2015 р.) термін "критична інфраструктура" використовувався більш деталізовано. Вперше поміж "актуальних загроз національній безпеці" виокремлювалися загрози критичній інфраструктурі. Крім того, окремо в підрозділі "Загрози кібербезпеці і безпеці інформаційних ресурсів" згадується вразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак. Також уперше одними з "основних напрямів державної політики в сфері національної безпеки" названо забезпечення безпеки критичної інфраструктури та визначено пріоритети такого напряму [7].

Закон України "Про основні засади забезпечення кібербезпеки України" визначає критично важливі об'єкти інфраструктури (об'єкти критичної інфраструктури), до яких відносить підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки і промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може негативно вплинути на стан національної безпеки й оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей.

У Стратегії національної безпеки України "Безпека людини – безпека країни", затвердженій Указом Президента України від 14.09.2020 р. № 392, у розділі ІІ "Поточні та прогнозовані загрози національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов" констатується, що посилюються загрози для критичної інфраструктури, пов'язані з погіршенням її технічного стану, відсутністю інвестицій в її оновлення та розвиток, несанкціонованим втручанням у її функціонування, зокрема фізичним і кіберхарактеру, триваючими бойовими діями, а також тимчасовою окупацією частини території України. У розділі ІІІ "Основні напрями зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки" наголошується на тому, що держава має створити ефективну систему безпеки та стійкості критичної інфраструктури, яка ґрунтується на чіткому розподілі відповідальності її суб'єктів і державно-приватному партнерстві.

Слід зазначити, що останньою після ухвалення нової Стратегії національної безпеки України активізувалася робота щодо нормативно-правового врегулювання окремих напрямів захисту об'єктів критичної інфраструктури. Так, Кабінет Міністрів України схвалив постанови (зокрема Постанову від 09.10.2020 р. № 943 "Деякі питання об'єктів критичної інформаційної інфраструктури"), які посилюють кібербезпеку об'єктів критичної інфраструктури – стратегічно важливих для держави підприємств, установ, організацій незалежно від форми власності, ініціатором розроблення яких виступило Міністерство цифрової трансформації України. Зазначені нормативні акти дадуть змогу провести аудит інформаційної безпеки об'єктів та оцінити рівень потенційної небезпеки для кожного з них, створити Держреєстр об'єктів критичної інформаційної інфраструктури, визначити єдину систему обліку та зберігання даних про них, сформувати механізми і критерії віднесення об'єктів до критичної інфраструктури. Це стосується підприємств та установ у сферах енергетики, хімічної промисловості, транспорту, технологій та електронних комунікацій, банківського й фінансового секторів. Порушення їх систем спричинить надзвичайні ситуації та матиме негативний вплив на стан екологічної, економічної, енергетичної безпеки й обороноздатність. Тому такі об'єкти потребують особливої уваги кіберзахисту [13].

У багатьох країнах світу значна частина об'єктів критичної інфраструктури перебуває у приватній власності, що потребує відповідного правового регулювання державно-приватного партнерства. У Німеччині положення щодо доцільності зміцнення державно-приватного партнерства закріплене у Стратегії кібербезпеки від 2011 р. У Великій Британії основи взаємодії державного та приватного секторів закладені Стратегією національної безпеки, Антитерористичною стратегією, Стратегією захисту кіберпростору та в урядовому Плані розвитку національної інфраструктури [6].

В офіційному повідомленні № 786 за 2006 р. Європейська Комісія рекомендувала державам ЄС розробити національну програму (план) захисту критичної інфраструктури як документ, що має правову силу. При цьому рекомендується створити умови для ефективної взаємодії й обміну інформацією, даними і досвідом між урядовими структурами та приватним сектором, а також зробити внесок у створення гармонізованої методології на рівні ЄС та загальноєвропейської системи аналізу ризиків. Отже, під час розроблення системи захисту критичної інфраструктури в Україні, враховуючи євроінтеграційний курс нашої держави, необхідно спрямувати зусилля на досягнення узгодженості національного законодавства з нормативними актами ЄС та впровадження чинних в ЄС стандартів захисту критичної інфраструктури, включаючи державно-приватне партнерство [6].

В Україні діє низка законів та інших нормативних актів, що визначають повноваження й компетенцію державних органів у цій і суміжних сферах, встановлюють особливості забезпечення охорони та безпечного функціонування зазначених об'єктів і систем. Проте в Україні на національному рівні досі бракує системного підходу до управління захистом і безпекою усього комплексу таких систем, об'єктів, ресурсів та залучення до цього приватних партнерів. Крім того, законодавством не врегульовано здійснення державно-приватного партнерства у сфері захисту критичної інфраструктури. Чинний Закон України "Про державно-приватне партнерство" регулює державно-приватне партнерство, головним чином, у галузі економіки [6]. Водночас можна констатувати, що на підзаконному рівні вживаються окремі заходи, спрямовані на підвищення ефективності регулювання відносин у сфері державно-приватного партнерства, наприклад, за рахунок внесення змін до Постанови Кабінету Міністрів України від 11.04.2011 р. № 384 "Деякі питання організації здійснення державно-приватного партнерства", зокрема, внаслідок внесення змін до Порядку проведення аналізу ефективності здійснення державно-приватного партнерства, затвердженого Постановою № 384 (зміни, внесені Постановою Кабінету Міністрів України від 09.10.2020 р. № 937).

На сьогодні у державі готовність до реагування на комплексні загрози й ризики до цього часу забезпечується за умов наявності цілої низки державних/національних систем захисту, безпеки та кризового реагування, за функціонування яких несуть відповідальність окремі державні органи, що створює умови для домінування відомчих підходів, під впливом яких уповноважені державні органи виявляють

схильність опікуватися лише певним спектром загроз і ризиків. Ще однією характерною ознакою наявного стану речей у цій сфері є те, що в Україні об'єкти, системи і мережі, які відповідно до світової практики прийнято відносити до критичної інфраструктури, "розпорошені" по більш ніж 10 різноманітних переліках і списках об'єктів, включаючи "особливо важливі"; "важливі"; такі, які підлягають "охороні та обороні" або "обов'язковій охороні"; "об'єкти підвищеної небезпеки", "радіаційно-небезпечні об'єкти" тощо. Зазначена ситуація неминуче створює міжвідомчі бар'єри для опрацювання питань, які перебувають поза межами конкретних систем, і це, зокрема, перешкоджає врахуванню загроз і ризиків, реалізація яких може викликати так звані каскадні ефекти, тобто випадки, коли надзвичайні та кризові ситуації, які можуть бути в одній галузі (одному секторі критичної інфраструктури), спричиняють швидкий негативний вплив на інші галузі, сектори і сегменти національної економіки, національної безпеки й оборони.

Аналіз нинішньої ситуації у сфері захисту об'єктів, які мають бути віднесені до критичної інфраструктури, свідчить, що відомчі оцінки стосовно достатньої урегульованості процедур і механізмів координації дій, взаємодії й обміну інформацією між системами у чинному правовому полі не зовсім відповідають дійсному стану речей, і це особливо яскраво проявляється в ситуаціях, пов'язаних із проблематикою реагування на реалізацію комплексних загроз.

Варто зазначити, що у провідних країнах світу ефективна взаємодія систем реагування на загрози, небезпеки і ризики є важливим елементом забезпечення національної безпеки. Наприклад, у США для характеристики здатності систем взаємодіяти широко використовують спеціальний термін "interoperability", а забезпечення оптимальної здатності систем, персоналу й обладнання отримувати і надавати функціональну підтримку, дані, інформацію та послуги визначено як найбільш важливу вимогу для Міністерства внутрішньої безпеки США під час реагування на інциденти. Натомість у законодавстві України щодо національної безпеки таких або аналогічних за змістом термінів бракує [14].

На сьогодні в Україні діють відокремлено такі державні системи:

– Єдина державна система цивільного захисту (ЄДСЦЗ);

– Єдина система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (ЄСЗРПТА);

– Державна система фізичного захисту (ДСФЗ).

Наявність відокремлених, хоча і пов'язаних між собою, систем призводить до неефективного реагування на загрози комплексного характеру. В сучасних безпекових умовах в Україні у геометричній прогресії зростає загроза виникнення надзвичайних ситуацій "техногенного тероризму", особливо на гідротехнічних об'єктах, хімічних складах, підприємствах хімічної промисловості, у технологічному процесі яких використовують небезпечні хімічні речовини. Об'єктом атак терористів може стати такий елемент критичної інфраструктури держави, як газотранспортна система. Якщо згадати гідротехнічні об'єкти (зокрема шлюзи Дніпровського каскаду) та ядерні об'єкти, розташовані на території нашої держави, то негативні наслідки від потенційних терористичних загроз можуть бути без перебільшення жахливими [15]. Реагування на такі загрози з огляду на різні режими функціонування ЄДСЦЗ, ЄСЗРПТА та ДСФЗ може відбуватися асинхронно.

Таким чином, національна нормативно-правова база в її сучасному вигляді не може бути надійною основою для розроблення й реалізації планів і процедур координації дій, взаємодії й обміну інформацією між наявними в Україні системами захисту, безпеки та кризового реагування. Розроблення дієвих планів і процедур координації дій, взаємодії й обміну інформацією потребує щонайменше прийняття спільної термінології, визначення співвідношень між режимами, рівнями та умовами функціонування систем, узгодження принципів управління комплексною кризою, яка пов'язана з дією кількох небезпечних факторів (у розглянутому випадку це тероризм і радіація) тощо. Запровадження єдиних підходів, термінології, процедур і форматів координації дій, взаємодії й обміну інформацією на національному рівні має бути враховано під час розроблення та коригування документів оперативного і тактичного рівнів [14].

Підвищення ефективності організаційно-правового регулювання захисту критичної інфраструктури у контексті формування нової парадигми національної безпеки можливе

внаслідок прийняття базового закону "Про критичну інфраструктуру та її захист". В Україні було розроблено кілька подібних законопроєктів. На сьогодні на стадії погодження перебуває законопроєкт, розроблений Мінекономрозвитку на виконання доручення Кабінету Міністрів України від 21.02.2017 р. № 1835/4/1-17 до Указу Президента України від 16.01.2017 р. № 8/2017 «Про рішення Ради національної безпеки і оборони України від 29.12.2016 р. "Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури"».

Визнаючи в цілому прогресивний характер зазначеного законопроєкту, маємо констатувати, що він може бути доопрацьований та вдосконалений.

Наприклад, у ст. 9 законопроєкту визначено, що вимогами щодо формування та реалізації державної політики у сфері захисту критичної інфраструктури є забезпечення таких життєво важливих функцій і послуг, як урядування та надання найважливіших державних послуг; енергозабезпечення; водопостачання та водовідведення; продовольче забезпечення; охорона здоров'я; інформаційні, комунікаційні та цифрові послуги; фінансові та банківські послуги; транспортне забезпечення; оборона; правопорядок; постачання теплової енергії.

Відповідно до ст. 14 законопроєкту суб'єктами державної системи захисту критичної інфраструктури є: 1) Кабінет Міністрів України; 2) Уповноважений орган у сфері захисту критичної інфраструктури України; 3) міністерства та інші центральні органи виконавчої влади; 4) Служба безпеки України; 5) правоохоронні та розвідувальні органи; 6) Збройні Сили України, інші військові формування, утворені відповідно до законів України; 7) місцеві державні (військові, у разі утворення) адміністрації; 8) органи місцевого самоврядування; 9) оператори критичної інфраструктури незалежно від форми власності; 10) підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки та стійкості критичної інфраструктури. Водночас у законопроєкті не деталізовано завдання й функції окремих важливих суб'єктів захисту критичної інфраструктури.

Важливо, що законопроєкт містить низку положень щодо державно-приватної взаємодії. Державно-приватну взаємодію у сфері захисту критичної інфраструктури віднесено до основних принципів функціонування державної системи захисту критичної інфраструктури (ст. 6). У ст. 32 законопроєкту визначено шляхи державно-приватної взаємодії у сфері захисту критичної інфраструктури. Проте проєкт Закону України "Про критичну інфраструктуру та її захист" не враховує повною мірою вимоги у частині державно-приватного партнерства, оскільки правові норми, встановлені Законом України "Про державно-приватне партнерство", взагалі не регулюють державно-приватне партнерство у сфері безпеки, і тому вже не відповідають сучасним безпековим підходам. Зазначене обумовлює необхідність урахування цього у проєкті Закону України "Про критичну інфраструктуру та її захист", зокрема щодо внесення відповідних змін до Закону України "Про державно-приватне партнерство", а також у документах планування у сферах національної безпеки і оборони, які будуть розроблені на виконання рішення РНБО України від 14.09.2020 р. "Про Стратегію національної безпеки України" [6].

Висновки

Процес удосконалювання механізму правового забезпечення захисту критичної інфраструктури в Україні в цілому відбувається з урахуванням передового досвіду країн ЄС та США. При цьому нагальною потребою сьогодення є доопрацювання та прийняття закону "Про критичну інфраструктуру та її захист", що дасть змогу чітко визначити критерії й методологію віднесення тих чи інших об'єктів інфраструктури до критичної інфраструктури, запровадити комплексний підхід до захисту об'єктів критичної інфраструктури та уніфікувати термінологію у цій сфері. Водночас зберігається потреба внесення змін і доповнення до чинного Закону України "Про національну безпеку України", який доволі деталізовано регламентує засади функціонування сектору безпеки і оборони. При цьому, хоча у зазначеному законі й міститься норма про те, що "державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо", він фактично не визначає особливостей забезпечення цих важливих складників національної безпеки. Особлива увага законодавця у контексті реалізації

концепції "людської безпеки" має бути приділена саме забезпеченню соціальної, економічної й екологічної безпеки, адже саме ці складники національної безпеки мають не лише величезне гуманітарне значення, а також визначають потенціал держави у питаннях забезпечення воєнної, інформаційної та зовнішньополітичної безпеки. Відповідно, потребує уточнення і положення законопроєкту "Про критичну інфраструктуру та її захист" у частині захисту об'єктів критичної інфраструктури у цих сферах.

Отже, оптимізація механізму забезпечення захисту критичної інфраструктури у контексті формування нової парадигми забезпечення національної безпеки має базуватися на формуванні активної, превентивної, соціально-економічної, ефективної та орієнтованої на результат моделі забезпечення безпеки.

Дослідження загальних питань організації та правового регулювання захисту критичної інфраструктури виступає підґрунтям для подальшого аналізу проблем визначення специфіки пріоритетних секторів критичної інфраструктури та критичного переосмислення загроз критичній інфраструктурі з урахуванням світового досвіду. У подальшому планується розробити відповідні методи реагування на загрози критичній інфраструктурі, передусім, у контексті реалізації завдань щодо здійснення ефективної державної охорони органів державної влади України та посадових осіб.

Перелік джерел посилання

1. Сацута А. А. Национальная безопасность как социальное явление: современная парадигма. *Вестник Военного университета*. 2007. № 3. С. 36–43.
2. Маттес Бубе. Безпека людини в фокусі уваги. *Питання безпеки людини в контексті реформування безпекового сектору країн Східної Європи*. URL: https://library.fes.de/pdf-files/bueros/ukraine/07749.pdf (дата звернення: 20.08.2020).
3. Воротнюк М. Людська безпека як імператив сучасної епохи: переніс фокусу з держави на людину. *Питання безпеки людини в контексті реформування безпекового сектору країн Східної Європи*. URL: https://library.fes.de/pdf-files/bueros/ukraine/07749.pdf (дата звернення: 20.08.2020).
4. Kaldor M., Martin M., Selchow S. Op. cit. P. 273–281.
5. Пасічник В. М. Філософська категорія безпеки як основа нової парадигми державного управління національною безпекою. *Демократичне врядування*. 2011. Вип. 7. URL: http://nbuv.gov.ua/UJRN/DeVr_2011_7_7 (дата звернення: 20.08.2020).
6. Маркєєва О. Д., Розвадовський Б. Л. Актуальні проблеми правового забезпечення державно-приватного партнерства у сфері захисту критичної інфраструктури. URL: https://niss.gov.ua/sites/default/files/2020-09/derzhavno-pryvatne-partnerstvo.pdf (дата звернення: 20.08.2020).
7. 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. Київ : НІСД, 2015. 176 с.
8. Кондратов С. Про деякі проблеми правового та організаційного забезпечення протидії тероризму на сучасному етапі. Державна політика протидії тероризму: пріоритети та шляхи реалізації : зб. матеріалів "круглого столу" / за ред. М. Г. Гуцало. Київ : НІСД, 2011. С. 18–22.
9. European Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF (дата звернення: 20.08.2020).
10. European Programme for Critical Infrastructure Protection (EPCIP). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33260 (дата звернення: 20.08.2020).
11. Кідалова Н. О. Правові проблеми захисту критичних об'єктів інфраструктури стратегічного значення в Україні. *Право. Людина. Довкілля* / *Law. Human. Environment*. Vol. 10. № 3. 2019. С. 124–131. URL: http://journals.nubip.edu.ua/index.php/Pravo/article/viewFile/law2019.03.016/11128 (дата звернення: 20.08.2020).
12. Zaplatynskyi V., Uriadnikova I. Анализ отдельных элементов критической инфраструктуры на примере Украины. *Bezpieczenstwo w administracji i biznesie jako czynnik Europejskiej integracji i rozwoju*.Wyzsza Szkola Administracji i Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni, 2015. S. 414–438.
13. В Україні посилили захист об'єктів критичної інфраструктури. URL: https://www.unian.ua/economics/telecom/v-ukrajini-posilili-zahist-ob-yektiv-kritichnoji-infrastrukturi-novini-11177084.html (дата звернення: 20.08.2020).
14. Аналіз регуляторного впливу до проекту Закону України "Про критичну інфраструктуру

та її захист". URL: http://www.drs.gov.ua/wp-content/uploads/ 2020/07/5854-ob.pdf (дата звернення: 20.08.2020).

15. Павлов Д. М. Правові й організаційні проблеми протидії техногенному (технологічному) та ядерному тероризму і шляхи їх вирішення. *Науковий вісник Міжнародного гуманітарного університету*. 2014. № 10-2. Т. 1. С. 68–71.

Стаття надійшла до редакції 27.08.2020 р.

УДК 351.862.4:340.13+338.583(477)

Д. Н. Павлов, Н. А. Микитюк

ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ В КОНТЕКСТЕ ФОРМИРОВАНИЯ НОВОЙ БЕЗОПАСНОСТНОЙ ПАРАДИГМЫ УКРАИНЫ

Проведен анализ правовых и организационно-управленческих проблем повышения эффективности обеспечения защиты критической инфраструктуры государства в Украине в контексте формирования новой безопасностной парадигмы, которая базируется на приоритете общечеловеческих базовых ценностей и идеалах человеческой общины. Рассмотрено влияние повышения эффективности государственно-частного партнерства на уровень безопасности и стойкости критической инфраструктуры. Сформулирован и обоснован тезис о том, что рассмотрение национальной безопасности прежде всего как защиты бытия нации побуждает ее к обращению к национальной идее, сквозь призму которой народ осмысливает свое бытие и соответственно определяет свои национальные ценности и национальные интересы.

При таких условиях философская категория безопасности и национальная идея могут стать методологической основой новой парадигмы национальной безопасности и организационно-правовых мероприятий ее обеспечения.

Ключевые слова: *государственно-частное партнерство, кибербезопасность, критическая инфраструктура, национальная безопасность, объект критической инфраструктуры, терроризм, гражданская защита.*

UDC 351.862.4:340.13+338.583(477)

D. Pavlov, M. Mykytiuk

LEGAL AND ORGANIZATIONAL PRINCIPLES OF ENSURING THE PROTECTION OF CRITICAL INFRASTRUCTURE IN THE CONTEXT OF THE FORMATION OF A NEW SECURITY PARADIGM OF UKRAINE

The article is devoted to the analysis of legal and organizational and managerial problems of improving the protection of critical infrastructure of the state in Ukraine in the context of forming a new security paradigm based on the priority of universal, basic values and ideals of the human community. The impact of improving the efficiency of public-private partnership on the level of security and sustainability of critical infrastructure is considered. The thesis is formulated and substantiated that the consideration of national security primarily as a protection of the nation existence motivates its appeal to the national idea, through the prism of which the people comprehend their existence and according to which they determine their national values and national interests. Under such conditions, the philosophical category of security and the national idea can become the methodological basis of the new paradigm of national security and organizational and legal measures to ensure it.

The practical significance of changing the paradigms of national security is that the previous paradigm was focused on ensuring security in an area when there was a real threat or danger to national security. The

process of improving the mechanism of legal support for the protection of critical infrastructure in Ukraine as a whole is taking into account the best practices of the EU and the United States.

Optimization of the mechanism for ensuring the protection of critical infrastructure in the context of the formation of a new paradigm of national security should be based on the formation of an active, preventive, social cost-effective and result-oriented security model

Keywords: *public-private partnership, cybersecurity, critical infrastructure, national security, critical infrastructure objects, terrorism, civil protection.*

Павлов Дмитро Миколайович – доктор юридичних наук, доцент, начальник кафедри Інституту Управління державної охорони України Київського національного університету імені Тараса Шевченка

https://orcid.org/0000-0002-4586-6399

Микитюк Микола Андрійович – доктор юридичних наук, доцент, професор кафедри Інституту Управління державної охорони України Київського національного університету імені Тараса Шевченка

https://orcid.org//0000-0002-1759-7312