

ПРИНЦИПИ ФОРМУВАННЯ ДЕРЖАВНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Загальна постановка проблеми. Національна безпека держави значною мірою ґрунтується на безперервному функціонуванні критичної інфраструктури (КІ). Відтак, формування державної системи захисту критичної інфраструктури (ДСЗКІ) є не просто першочерговим завданням, а нагальною потребою суспільства й держави. Даний процес вимагає чіткого визначення цілей, завдань і принципів формування ДСЗКІ, що в кінцевому рахунку дозволяє виробити найбільш ефективну модель функціонування системи. Тож виділення й обґрунтування зазначених принципів на перших етапах являє собою теоретичну проблему. Від успішності її розв'язання у подальшому багато в чому залежатиме характер інтеграції політики у сфері національної безпеки із відповідними процедурами, що здійснюються уповноваженими суб'єктами.

Аналіз публікацій. У зв'язку із надзвичайною актуальністю питання захисту критичної інфраструктури різні аспекти даної наукової проблеми привертають увагу широкого кола вчених. Серед найбільш вагомих публікацій у цій галузі, що побачили світ останнім часом, слід виділити наукові праці Д. С. Бірюкова, Д. Г. Бобра, О. С. Власюка, С. Ф. Гончара, В. П. Горбуліна, Д. В. Дубова, О. П. Єрменчука, С. П. Іванюти, С. І. Кондратова, М. А. Ожевана, А. І. Семенченка, О. М. Суходолі, В. М. Шемаєва та ін. Завдяки цим та іншим науковим дослідженням, результати яких висвітлено у статтях, монографіях, аналітичних матеріалах, натепер склалося достатньо повне уявлення про «необхідність формування єдиної державної політики у сфері захисту критично важливих об'єктів та інфраструк-

тури в Україні» [1, с. 2], про імплементацію в Україні кращих світових практик в галузі захисту критичної інфраструктури, щодо забезпечення стійкості, адекватної сучасним викликам і загрозам [2], про забезпечення координації дій, взаємодії та обміну інформацією при створенні державної системи захисту критичної інфраструктури [3] тощо.

Виділення не вирішених раніше частин загальної проблеми. Попри значний науковий доробок у сфері захисту критичної інфраструктури питання щодо принципів формування ДСЗКІ розглядалися фрагментарно, без належного глибинного обґрунтування. Подібна ситуація потребує систематизації підходів з метою чіткого визначення зазначених принципів. Отже, **метою** статті є встановлення й аргументоване представлення принципів формування ДСЗКІ. Досягнення мети уможливиться через розв'язання таких **завдань**: 1. Узагальнення існуючих наукових поглядів на поняття «принцип», зокрема в контексті ДСЗКІ. 2. Обґрунтування диференціації принципів формування і принципів функціонування ДСЗКІ. 3. Аналіз концептуальних принципів створення ДСЗКІ, закріплених на рівні нормативно-правових актів. 4. Представлення авторської концепції підходів до принципів формування ДСЗКІ.

Виклад основного матеріалу дослідження. Ключове поняття теми – «принцип» – є широко застосовуваним в науці та практиці. Відповідно до лексикографічних джерел воно тлумачиться як: «1. Основне вихідне положення якої-небудь наукової системи, теорії, ідеологічного напрямку і т.ін.; засада; // основний закон якої-небудь точної науки. 2. Особливість, покладена в основу створення

або здійснення чого-небудь, спосіб створення або здійснення чогось; // Правило, покладене в основу діяльності якої-небудь організації, товариства і т. ін.» [4, с. 714]. Виходячи з наведеного, можна стверджувати, що в контексті дослідження ДСЗКІ актуальними є обидва процитовані значення. Спочатку принципи узагальнюються на рівні теоретичної моделі. Потім при реалізації прикладного аспекту застосовуються в якості своєрідних векторів спрямування діяльності. Надзвичайно важливим є розрізнення у другому з представлених значень етапів створення і здійснення. Відштовхуючись від цього, цілком логічним є розподіл принципів досліджуваної сфери на принципи формування й принципи функціонування ДСЗКІ. Аби такий розподіл не здався штучно вигаданим, варто навести аналогію зі сферою архітектури й будівництва, де абсолютно чітко розмежовуються правила будівництва і правила експлуатації будинків.

Аналіз текстів наукових публікацій виявив принаймні дві показові тенденції. По-перше, автори не загострюють уваги на тому, що кожен з аспектів діяльності може мати свої принципи. Так, принципи державної політики у сфері ЗКІ далеко не завжди співпадають з принципами забезпечення безпеки та стійкості критичної інфраструктури. Принципи формування ДСЗКІ не обов'язково збігаються з принципами функціонування даної системи. Усе це треба конкретизувати. По-друге, сам перелік принципів, що наводиться у наукових працях та аналітичних матеріалах, має доволі широкий діапазон і не є уніфікованим. Для підтвердження останньої тези був проведений контент-аналіз текстів найбільш вагомих наукових публікацій за період понад п'ять років. В результаті виявлено суттєві розбіжності у баченні принципів, що є значущими для забезпечення діяльності у досліджуваній галузі.

Наприклад, у монографії О. П. Єрменчука згадуються такі принципи, як: співпраця з громадянським суспільством [5, с. 146], здійснення державно-приватного партнерства

у сфері захисту критичної інфраструктури [5, с. 147], індикативні керівні принципи для підготовки планів [5, с. 79], принципи побудови системи захисту критичної інфраструктури [5, с. 6, 16].

Д. С. Бірюков віддає перевагу принципам: планування безпеки [1, с. 6], залишковому принципу [1, с. 4], принципу групування [1, с. 22], принципам ідентифікації критичної інфраструктури [1, с. 25], європейським принципам [1, с. 68].

Авторський колектив англomовної монографії «Developing The Critical Infrastructure Protection System in Ukraine» за загальною редакцією О. М. Суходолі [2] виділяє основні принципи формування політики захисту критичної інфраструктури, до яких включено: принципи координованості, методологічної єдності [2, с. 28], державно-приватного партнерства [2, с. 29], конфіденційності [2, с. 30], міжнародної співпраці [2, с. 30], принципи економічних відносин та їх змін [2, с. 36], загальні принципи захисту критичної інфраструктури [2, с. 44], принципи державної політики у сфері захисту критичної інфраструктури [2, с. 46], фундаментальні принципи роботи [2, с. 58], принципи взаємодії та співробітництва державних органів, приватного бізнесу, суспільства та держави [2, с. 58, 181], принципи функціонування державної системи [2, с. 91], широко визнані принципи процесу планування [2, с. 121], узгоджені принципи управління для різних етапів кризи [2, с. 125], принципи антикризового управління [2, с. 130], правові, організаційні, фінансово-економічні принципи [2, с. 161], принципи законодавства ЄС [2, с. 161].

По суті перелічені принципи являють собою творчий розвиток, доповнення того, що зазначалося в «Зеленій книзі з питань захисту критичної інфраструктури в Україні» [6], виданій у 2012-ому році. Там також виділяються принципи: координованості, єдності методологічних засад, державно-приватного партнерства, забезпечення конфіденційності, міжнародного співробітництва.

Разом з тим, наведені приклади наочно демонструють, що домінуючі натепер концепції не передбачають диференціації принципів формування і принципів функціонування ДСЗКІ. Вважаю, що така позиція має бути виправлена, адже між цими групами принципів існують суттєві розбіжності. Результати порівняльного аналізу найбільш доцільно представити у формі таблиці 1.

Тож наведені дані достатньо переконливо аргументують необхідність розрізнення принципів формування і принципів функціонування ДСЗКІ. Ситуація ускладнюється тим, що держава нині водночас здійснює захист критичної інфраструктури і формує відповідну політику, розбудовує ДСЗКІ. Це певною мірою спричиняє наявність такої групи принципів, які умовно можна назвати інтегративно-універсальні. Тобто це такі принципи, які є актуальними для обох виділених груп.

Зокрема, названа категорія представлена у «Концепції створення державної системи захисту критичної інфраструктури», затвердженій розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р [7]. Наразі серед закріплених в акті принципів є:

– *взаємодія суб'єктів державної системи захисту критичної інфраструктури*. Реалізація даного принципу є вкрай важливою, проте цьому має передувати визначення й законодавче закріплення кола суб'єктів ДСЗКІ із чітким розподілом їхніх повноважень. Внаслідок відсутності спеціального профільного Закону України виникають певні складнощі, пов'язані із окремими нормативними положеннями, що інколи призводять до дублювання функцій тих чи інших суб'єктів. З іншого боку, не виключено, що окремі не передбачувані ситуації можуть взагалі не охоплюватися функціями жодного суб'єкту. Як слушно зазначено в аналітичній доповіді Національного інституту стратегічних досліджень «Про забезпечення координації дій, взаємодії та обміну інформацією при створенні державної системи захисту критичної інфраструктури», «наявні механізми та процедури взаємодії за умов, коли окреме міністерство (відомство) має забезпечувати реагування на «свій» набір загроз та небезпек і несе відповідальність за функціонування «своїєї» системи безпеки (кризового реагування), не дозволяють досягти рівня координації дій, взаємодії та обміну

Таблиця 1

Порівняльний аналіз принципів формування і принципів функціонування державної системи захисту критичної інфраструктури

Критерій порівняння	Принципи формування ДСЗКІ	Принципи функціонування ДСЗКІ
Період дії	Етап розбудови ДСЗКІ, обмеженість у часі	Не обмежені у часі
Цілі визначення	Закріплення пріоритетних напрямів діяльності у сфері ДСЗКІ, їх легітимація	Унормування способів діяльності
За способом	Спосіб створення	Спосіб здійснення
Сфера охоплення	Наукова, правотворча, нормотворча, організаційна діяльність	Правозастосовна, організаційно-правова, управлінська діяльність
За характером втілення	Концептуальні	Організаційно-управлінські
Зв'язок з етапами становлення і втілення засад інфраструктурної політики	Ініціювання і формування інфраструктурної політики	Реалізація інфраструктурної політики
Рівень нормативно-правових актів, якими закріплюються принципи	Концепції, схвалені розпорядженням Кабінету Міністрів України	Закони України, Укази Президента України
Розподіл по групах	Загальні і спеціальні (орієнтовані на вузькопрофільний вид діяльності) принципи	Загальні принципи

інформацією, адекватного цілям та завданням захисту національної КІ» [3, с. 5-6].

Бракує й спеціального уповноваженого органу, на який би покладалися обов'язки координації та організації взаємодії усіх суб'єктів. Такий орган повинен мати характер міжінституціонального, надвідомчого. За своєю суттю він виступатиме в якості національного координатора і мусить на пряму підпорядковуватися Кабінету Міністрів України, а по окремих позиціях – Раді національної безпеки і оборони України. В цілому ж специфіка подібної взаємодії полягає в тому, що вона має бути відпрацьована, як в режимі штатних, так і поза штатних ситуацій.

Таким чином, надзвичайна важливість принципу взаємодії суб'єктів ДСЗКІ зумовлює здійснення цілого комплексу додаткових правових, організаційних, управлінських заходів.

– *Підвищення рівня власних спроможностей громадян, суб'єктів господарювання, установ та організацій, уразливих до припинення або погіршення функціонування критичної інфраструктури.* Представлений принцип є інноваційним, оскільки запроваджує нову світоглядну парадигму. Держава не може і не повинна брати на себе абсолютно все. На сучасному етапі слід визначитися, що саме має стати сферою самозабезпечення й самозахисту, а що діє за принципами субсидіарності. Реалізація даного принципу починається із надто складного кроку – зміни системи мислення громадян. Застосовуючи комплекс просвітніх, роз'яснювальних, подекуди рекламних заходів, залучаючи окремих громадян та їхні спільноти до розв'язання проблем забезпечення стійкості КІ, держава у такий спосіб створюватиме підґрунтя для максимального убезпечення від ймовірних загроз. З урахуванням вимог Закону України «Про державну таємницю» є усі можливості залучення даної категорії суб'єктів до проведення громадських експертиз, участі в наглядових радах підприємств, що входять до складу об'єктів КІ. З іншого боку, не слід не-

дооцінювати роль подібної діяльності у профілактиці проявів негативної дії антропогенних чинників.

Підвищення рівня власних спроможностей окремих громадян і суб'єктів водночас потребує й доступного програмного забезпечення, якщо йдеться про безпеку критичної інформаційної інфраструктури. Відтак при формуванні державного бюджету необхідно врахування і таких видатків.

– *Будівництво та експлуатація об'єктів критичної інфраструктури з дотриманням вимог (інженерно-технічних, організаційних, експлуатаційних тощо) стосовно їх стійкого функціонування у різних режимах функціонування критичної інфраструктури.* Даний принцип є одним з ключових, проте й майже найскладнішим у своєму втіленні. Річ в тім, що існує ряд об'єктивних чинників, які значною мірою перешкоджають його дотриманню. Зокрема, до таких чинників можна віднести моральну застарілість, зношеність фонду об'єктів КІ. Більшість з них будувалися за радянських часів, коли діяли абсолютно інші стандарти, а також були кардинально інші уявлення про можливі загрози таким об'єктам. Слід враховувати й те, що економіка Радянського Союзу методологічно ґрунтувалася на взаємній залежності регіонів. Так, необхідні компоненти для функціонування атомних електростанцій, що знаходяться в Україні, вироблялися в Росії. На той час це було виправдано, натепер переросло у фактор національної безпеки. Подібних прикладів можна навести чимало Їх аналіз і систематизація має перспективу для окремого дослідження. Що ж до організаційно-правової складової реалізації зазначеного принципу, то до неї слід віднести: організацію експертизи кількісних та якісних показників стану існуючих об'єктів КІ; укладання Національного переліку об'єктів КІ з опертям на дані аудиту їхньої діяльності (сфера діяльності чи обслуговування, коефіцієнт зношеності, залежність у забезпеченні ресурсами тощо); паспортизацію й категоризацію таких об'єктів, правовий механізм

їх здійснення; пріоритетність закріплення в нормативних актах індикаторів безпекового середовища даної категорії об'єктів (з урахуванням безпеки людей і довкілля); розробку й затвердження в установленому порядку стандартів нового покоління щодо діяльності об'єктів КІ; запровадження системної моніторингової, статистичної, аналітичної компоненти в управлінні цими об'єктами; гармонізація міжнародних, державних і відомчих нормативних актів щодо усіх аспектів захисту подібних об'єктів; моделювання загроз та уразливостей з подальшим нормативним врегулюванням особливостей діяльності об'єктів КІ, дій персоналу у позаштатних ситуаціях тощо. Отже, для того, щоб вказаний принцип не залишився декларацією, а почав повноцінно діяти, необхідно провести складну, багатопланову роботу. Без неї забезпечення стійкості КІ, а відтак і національної безпеки в цілому практично унеможливується.

– *Обмін інформацією між суб'єктами державної системи захисту критичної інфраструктури*. За своєю суттю вказаний принцип є складовою першого із групи зазначених – принципу взаємодії. Виокремлення його в переліку зумовлено важливістю даного аспекту діяльності. Натепер цей аспект нормативно не врегульований. Відтак на практиці діють вузьковідомчі інтереси, що часом приймає форми нездорової конкуренції. Знову ж таки відчувається відсутність єдиного координаційного центру, який би сприяв розповсюдженню необхідної інформації та здійснював на її підставі подальшу координацію дій. З позицій управлінської діяльності, має бути визначений перелік суб'єктів, в тому числі на рівні окремих штатних посад персоналу, на яких покладається обов'язок з обміну відповідною інформацією по горизонталі й вертикалі. Потребується й винахід балансу між повідомленням інформації іноземним партнерам та дотриманням норм Закону України «Про державну таємницю». То ж і цей принцип має бути покроково відпрацьований і внормований.

– *Здійснення державно-приватного партнерства у сфері захисту критичної інфраструктури*. Зазначений принцип також невід'ємно пов'язаний із принципом взаємодії, підвищення рівня власних спроможностей громадян, суб'єктів господарювання, установ та організацій. Його реалізація на методологічних засадах починається зі зміни методологічної парадигми, за якої лише держава та її органи несуть відповідальність за забезпечення національної безпеки. Сюди ж можна віднести й переорієнтацію на служіння держави потенційних правопорушників, які мають високий рівень професійних компетентностей. До прикладу, в аналітичній доповіді Національного інституту стратегічних досліджень «Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України» розглядається питання щодо трансформації від протиправної діяльності до легального співробітництва з державою так званих «хактивістів» (неологізм, що поєднує «хакерів» та «активістів») [8, с. 64-67]. Відштовхуючись від цього, до кола відповідних суб'єктів на рівні законодавства мають бути віднесені не тільки державні органи, а й оператори КІ, себто організації, підприємства, установи усіх форм власності, що діють у сфері КІ. Також передбачається залучення до окремих видів діяльності громадських організацій, об'єднань роботодавців, експертних співтовариств, профільних фахівців тощо. З позицій права, підлягають унормуванню засади залучення таких суб'єктів до захисту КІ; межі допуску до конфіденційної й таємної інформації відповідно до чинного законодавства; запобіжні заходи щодо проникнення під виглядом «активістів» представників спеціальних служб іноземних держав й здійснення ними шпionажу, підготовки терористичних актів; здійснення контррозвідального, оперативного-розшукового забезпечення діяльності об'єктів КІ. Таким чином, при реалізації розглянутого принципу важливо не тільки перетворити на партнерів держави відповідний приватний сектор, зокрема операторів КІ, а й

не припустити проникнення до цих об'єктів, ознайомлення з конфіденційною інформацією осіб, які можуть нашкодити справі захисту КІ й національній безпеці в цілому.

– *Сприяння міжнародному співробітництву у сфері захисту критичної інфраструктури з урахуванням глобальних та регіональних безпекових процесів.* Суттєве прискорення й значне поширення процесів глобалізації вплинуло на розуміння сутності конструктивного міжнародного співробітництва, зокрема у сфері захисту критичної інфраструктури. Загрози терористичних актів, дистанційного протиправного втручання в роботу систем і механізмів через мережу Інтернет спричинили зростання масштабів можливих наслідків. Відтак, протистояння подібним загрозам і викликам потребує об'єднання зусиль на міждержавному рівні. Поле діяльності у зазначеному напрямі є доволі широким: від визначення пріоритетів для захисту об'єктів КІ, суттєвих у міжнародних масштабах, від можливостей вивчення досвіду провідних країн на рівні нормативно-правового регулювання, консультативної допомоги, адаптації та гармонізації українського законодавства із міжнародними стандартами до проведення спільних заходів. При цьому подібна кооперація заради спільної безпеки має проводитися з урахуванням вимог як національного, так і міжнародного законодавства. На Службу Безпеки України як одного з провідних суб'єктів ДСЗКІ у зазначеному контексті покладається обов'язок визначення меж конфіденційності при обміні інформацією в міжнародних контактах, неприпущення витоку таємної інформації, контррозвідувальна діяльність тощо.

Перспективним є й дослідження, а потім і реалізація дольового фінансування інфраструктурних проектів на засадах субсидіарності. З урахуванням фінансового становища України, проблематичності самостійно здійснити реалізацію усіх планів по забезпеченню стійкості КІ необхідно визначити організаційно-правовий механізм залучення додаткових коштів в якості фінансової

допомоги держав-партнерів України, провідних міжнародних інституцій, кола інвесторів та умов їх участі в інфраструктурних проектах. Потребується також унормування порядку здійснення контролю та звітності за використанням міжнародних інвестицій в ДСЗКІ України.

Отже міжнародне співробітництво у сфері захисту критичної інфраструктури є вимогою часу. Від реалізації даного принципу багато в чому залежить не тільки теперішнє, а й майбутнє держави, стан національної безпеки у ній, а також архітектура глобальної безпеки в цілому.

– *Розроблення та удосконалення законодавства у сфері захисту критичної інфраструктури з урахуванням норм і стандартів НАТО, а також положень річних національних програм під егідою Комісії Україна – НАТО на відповідні роки.* Співробітництво України з Організацією Північноатлантичного Договору (НАТО) було започатковано ще у 1997 р. на рівні Хартії [9], а у 2001 році – на рівні відповідного Указу Президента України [10]. Вкрай важливим є те, що вже тоді було визначено ставлення України до НАТО як до «найбільш ефективної структури колективної безпеки» [10]. Передбачалося, що до сфер консультацій та співробітництва з-поміж інших входить: цивільне планування на випадок надзвичайних ситуацій та катастроф, аспекти безпеки у сфері довкілля, включаючи ядерну безпеку, використання космічного та повітряного простору. Від 2011 року щорічно приймаються Річні національні програми співробітництва Україна – НАТО, що затверджуються указами Президента України. Так, відповідно до такої програми на 2019 р. розроблені пріоритетні завдання та заходи щодо створення системи раннього попередження та реагування на конфлікти (ціль 1.2.6), надійного енергозабезпечення (ціль 1.4.3), створення національної інфраструктури геопросторових даних (ціль 1.4.4), забезпечення екологічної безпеки (ціль 1.5.2), захисту критичної інфраструктури та ефек-

тивного попередження загроз (ціль 1.5.3). Пунктом 77 зазначеного акту передбачено формування Державної системи захисту критичної інфраструктури, пунктом 79 – створення в Україні Національної системи стійкості. Проте, не зважаючи на фундаментальність й надзвичайну актуальність поставлених завдань, які мають виконуватися за участі консультативної місії НАТО, їхня реалізація неможлива у встановлені терміни одного року. Це доволі складний і довготривалий процес. Безумовно, успішність його перебігу залежатиме від ефективності координації зусиль між усіма партнерами.

Фіналізуючи розгляд принципів, представлених у «Концепції створення державної системи захисту критичної інфраструктури», слід зазначити, що кожен з них є вкрай важливим, широкомасштабним. За своєю суттю вони є універсальними, адже не втратять актуальності й на подальших етапах функціонування ДСЗКІ.

Характерно, що вони не дублюють переліку принципів, визначених Європейською Програмою захисту критичної інфраструктури [11]. Останній включає в себе принципи: субсидіарності, взаємної доповнюваності, конфіденційності, співробітництва із зацікав-

леними сторонами, співмірності, посекторного підходу. Більшість перелічених принципів рідко зустрічається у текстах українських нормотворчих документів, проте має широкі перспективи для опанування в діяльності з формування ДСЗКІ.

Авторське бачення наукової проблеми полягає в тому, що по-перше, доцільно розрізняти принципи створення й принципи функціонування ДСЗКІ, а також виділяти групу інтегральних принципів, актуальних для обох груп. По-друге, є сенс вирізняти кластери принципів за сферами. В узагальненому вигляді найкраще представити це в формі таблиці 2.

Представлена класифікація не є вичерпною, проте характеризується системністю й дозволяє за необхідності на практиці створювати певні алгоритми дій та сприяти найбільш ефективній реалізації поетапного розв'язання важливих завдань.

Висновки. Поняття принципів формування державної системи захисту критичної інфраструктури є важливим і для теорії, і для практики. Без його чіткого визначення унеможливується створення дієвого адміністративно-правового регулювання функціонування та розвитку ДСЗКІ. Тож

Таблиця 2

Класифікація принципів формування державної системи захисту критичної інфраструктури

Сфера	Принципи
Концептуалізації та наукового обґрунтування	Об'єктивності, методологічної одноманітності, всебічності, повноти і цілісності, системності, адаптивності, випереджального характеру, прогнозованості, єдності теорії і практики
Легітимації	Верховенства права, примату безпеки, відповідальності, гуманізму, людиноцентризму, збалансованості інтересів суб'єктів, конфіденційності, гармонізації міжнародного й національного законодавства, превентивності
Організації та управління	Доцільного розподілу й розмежування повноважень; прозорості; ефективної взаємодії; безперервності управління; державно-приватного партнерства; плановості, адекватності дій; гнучкості, збалансованості інтересів; міжнародного співробітництва
Фінансування	Необхідної достатності, своєчасності, гарантованості ресурсного забезпечення, оптимізації витрат, бюджетного контролю.

результати проведеного дослідження у подальшому дозволять оптимізувати вирішення ключових питань, що, своєю чергою, підвищенню ефективності як функціону-

вання даної системи в цілому, так і удосконаленню напрямів адміністративно-правового регулювання суспільних відносин у даній сфері зокрема.

Анотація

Формування державної системи захисту критичної інфраструктури (ДСЗКІ) потребує чіткого визначення принципів, за якими відбуватиметься цей процес. Проаналізовано сутність ключового поняття «принцип» в контексті досліджуваної галузі. Обґрунтовано диференціацію принципів формування й принципів функціонування ДСЗКІ. Розглянуто концептуальні принципи на рівні офіційних і доктринальних джерел. Представлено авторську концепцію принципів формування ДСЗКІ.

Ключові слова: національна безпека, критична інфраструктура, захист критичної інфраструктури, державна система захисту критичної інфраструктури, класифікація принципів, принципи формування, принципи функціонування, взаємодія суб'єктів державної системи захисту критичної інфраструктури, об'єкти критичної інфраструктури, міжнародне співробітництво у сфері захисту критичної інфраструктури.

Аннотация

Формирование государственной системы защиты критической инфраструктуры (ГСЗКИ) требует четкого определения принципов, по которым будет осуществляться этот процесс. Проанализирована сущность ключевого понятия «принцип» в контексте исследуемой отрасли. Обоснована дифференциация принципов формирования и принципов функционирования ГСЗКИ. Рассмотрены концептуальные принципы на уровне официальных и доктринальных источников. Представлена авторская концепция принципов формирования ГСЗКИ.

Ключевые слова: национальная безопасность, критическая инфраструктура, защита критической инфраструктуры, государственная система защиты критической инфраструктуры, классификация принципов, принципы формирования, принципы функционирования, взаимодействие субъектов государственной системы защиты критической инфраструктуры, объекты критической инфраструктуры, международное сотрудничество в сфере защиты критической инфраструктуры.

Telenyk S.S. Principles of formation of the state system of the critical infrastructure protection

Summary

The formation of a state system of the critical infrastructure protection requires a clear definition of the principles by which this process will be carried out. The author of the article examines the key concept "principle" in the context of the semantic field of the critical infrastructure. Analysis of doctrinal sources showed that there is no unified vision of the list of principles in the area under study. Each scientist offers a different set of principles. The author's position consists in a clear delineation of the principles of the formation of the system and the principles of the functioning of the system. The comparison of categories argues the need for such a distinction. He states the discrepancy between the principles presented in the doctrinal and normative sources. The article contains a detailed analysis of the principles enshrined in the "Concept for the creation of a state system of the critical infrastructure protection", approved by the order of the Cabinet of Ministers of Ukraine. The author proposes his own classification, which based on priority areas.

In particular, he highlights the scope of conceptualization and scientific justification, legitimation, organization and management, and financing. Each group includes a specific set of principles. The scientist believes that the use of this classification will further find its application in the theory and practice of the critical infrastructure protecting.

Key words: national security, critical infrastructure, the critical infrastructure protection, state system of the critical infrastructure protection, classification of principles, principles of formation, principles of functioning, interaction of subjects of the state system of the critical infrastructure protection, critical infrastructure facilities, international cooperation in the field of the critical infrastructure protection.

Список використаних джерел:

1. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. К.: НІСД, 2012. 96 с.
2. Developing The Critical Infrastructure Protection System in Ukraine : monograph / [S. Kondratov, D. Bobro, V. Horbulin et al.] ; general editor O. Sukhodolia. Kyiv : NISS, 2017. 184 p.
3. Кондратов С. І. Про забезпечення координації дій, взаємодії та обміну інформацією при створенні державної системи захисту критичної інфраструктури. К.: НІСД. 30 с.
4. Новий тлумачний словник української мови у чотирьох томах / Уклад. В. Яременко, О. Сліпущко. Т. 3. О-Р. К.: Аконт. 1998. 927 с.
5. Єрменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України. Дніпро: ДДУВС, 2018. 177 с.
6. Зелена книга з питань захисту критичної інфраструктури в Україні: збірник матеріалів міжнародних експертних нарад [Електронний ресурс] // <http://old2.niss.gov.ua/articles/2213/>
7. Концепція створення державної системи захисту критичної інфраструктури: затверджено розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р. Урядовий кур'єр від 10.01.2018. № 5.
8. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доповідь / за заг. ред. Д. Дубова. К. : НІСД, 2018. 84 с.
9. Хартія про особливе партнерство між Україною та Організацією Північно-Атлантичного договору від 09.07.1997 // Голос України, 11 липня 1997 р. № 127 (1627).
10. Державна програма співробітництва України з Організацією Північноатлантичного Договору (НАТО) на 2001-2004 роки: затверджена Указом Президента України від 27 січня 2001 р. // Офіційний вісник України від 16.02.2001, № 5, стор. 11, ст. 175.
11. Commission of the European Communities. Communication from the commission on a European Programme for Critical Infrastructure Protection / Brussels, 12.12.2006.