УДК 342.9
DOI https://doi.org/10.32837/pyuv.v2i4(29).431

С. С. Теленик
orcid.org/0000-0002-1328-7595
кандидат юридичних наук

СИСТЕМА СУБ'ЄКТІВ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Загальна постановка проблеми. Національна безпека становить собою багатокомпонентну систему, в якій органічно пов'язані між собою як чисельні суб'єкти її забезпечення, так і об'єкти, ефективне і безперебійне функціонування яких визначає загалом потенціал країни, її спроможність реалізовувати власну політику в умовах постійної ескалації загроз. Одними із таких об'єктів виступають об'єкти критичної інфраструктури (ОКІ). Адже сталість функціонування таких об'єктів напряму залежить від ефективної діяльності суб'єктів їхнього захисту, взаємної узгодженості та своєчасної координації їхніх дій, а загалом – функціонування ефективної системи управління. У такому контексті виникає нагальна як теоретична, так і практична потреба у розробленні наукових засад системного підходу щодо адміністративно-правового регулювання діяльності усіх суб'єктів, покликаних забезпечувати захист об'єктів критичної інфраструктури.

Аналіз публікацій. Різні аспекти питання, що досліджується, тою чи іншою мірою розглядалися автором статті у контексті завдань і повноважень Служби безпеки України [1], приватного сектору (О.П. Єрменчук) [2], суб'єктів природних монополій у сфері електричної енергії України (Г.В. Берлач) [3], механізму ідентифікації та трансформації «знань» суб'єкта критичної інфраструктури (Ю.І. Косенко, П.С. Носов) [4], формування системи інформаційної та кібербезпекової політики [5] тощо.

Також окремо відзначимо, що під час розгляду і дослідження національної безпеки автори, визначаючи безпеку як стан, виділяють параметри, що її характеризують: *стійкість, стабільність*, *живучість системи*. Під **стійкістю** розуміється здатність системи нормально функціонувати під час впливів, під **стабільністю** – сукупність сталостей до тривало діючих впливаючих чинників, а під **живучістю** – здатність систем зберігати функціонування в умовах цілеспрямованого впливу [6; 7; 8; 9]. В.А. Ліпкан взагалі на основі застосування синергетичного підходу запропонував об'єднати ці питання одним науковим терміном «гомеостази» [10; 11; 12; 13; 14; 15]. Проте загалом відмітимо, що саме ці характеристики покладено в основу ефективності системи захисту ОКІ.

Питання щодо ролі суб'єктів захисту критичної інфраструктури з позицій технократичного підходу не залишилися поза увагою і фахівців Національного інституту стратегічних досліджень України (далі НІСД), зокрема Д.С. Бірюкова, Д.В. Дубова, С.І. Кондратова, О.М. Суходолі та інших [16; 17; 18; 19; 20; 21; 22; 23].

Виділення не вирішених раніше частин загальної проблеми. Попри постійне звернення вчених до питання щодо визначення кола суб'єктів захисту критичної інфраструктури, наукова картина світу у цій сфері залишається фрагментарною, оскільки опису піддаються лише окремі елементи системи, а не вся система загалом. Навіть більше, серед фахівців НІСД майже немає юристів, які б із позицій правових наук і системного підходу правового регулювання могли б дослідити як структуру правовідносин у цій сфері, так і механізм адміністративно-правового регулювання. Отже, відбувається певне заміщення системної методології дослідження системного явища технократичними підходами, що певним чином звужує науковий потенціал як самого дослідження, так і рівень та верифікативність отримуваних наукових результатів.

У зв'язку з цим виникає необхідність окремого наукового дослідження зазначеного предмета на засадах інтеграції системного й функціонально-структурного підходів.

Відтак **мета статті** полягає у науковому обґрунтуванні авторської концепції щодо системності суб'єктів захисту об'єктів критичної інфраструктури з позицій наукової методології правових наук.

Досягненню поставленої мети сприяє розв'язання таких **завдань**: 1) концептуалізація сутності поняття «система» в контексті її подальшої екстраполяції на систему суб'єктів досліджуваної галузі; 2) узагальнення наукових позицій інших вчених щодо взаємозв'язку системи суб'єктів захисту ОКІ із реалізацією державної політики захисту критичної інфраструктури, організації координації і взаємодії між цими суб'єктами; 3) формально-юридичний та логіко-догматичний аналіз текстів нормативно-правових актів у сфері національної безпеки, включаючи проект Закону України «Про критичну інфраструктуру та її захист» [24] на предмет визначення суб'єктів цієї категорії; 4) репрезентація авторського бачення системи суб'єктів захисту об'єктів критичної інфраструктури з позицій методології правових наук.

Виклад основного матеріалу дослідження. Поняття системи, яке у своєму основному значенні в лексикографічних джерелах тлумачиться як «порядок, зумовлений правильним, планомірним розташуванням і взаємним зв'язком частин чого-небудь» [25, с. 1126], по праву зайняло одне з центральних місць у методології науки. Навіть більше, загальна теорія систем у процесі свого розвитку поступово формує нову галузь знань під назвою «системологія». [26, с. 11] Принципово важливим є спостереження Ю.П. Сурміна, що представлення досліджуваного об'єкта як деякої системи характеризується: елементним складом; структурою як формою взаємного зв'язку елементів; функціями елементів і цілого; єдністю внутрішнього і зовнішнього середовища системи; законами розвитку системи та її складників [26, с. 8–9]. Універсальність зазначеної формули виявляється в тому, що вона однаково актуальна і для технічних, і для природничих, і для соціальних наук, до яких належить і право.

Натепер, завдяки науковим доробкам П.П. Богуцького [27], Б.В. Ганьби [28; 29], Р.Б. Галюка [30], Л.І. Заморської [31], О.В. Зіменка [32], М.С. Кельмана [33], В.А. Ліпкана [34; 35; 36], О.Ф. Скакун [37] та інших, системний підхід міцно закріпився у правовій науці. Разом із тим, якщо йдеться про сферу правового регулювання захисту об'єктів критичної інфраструктури, то доводиться констатувати, що дослідження з опертям на теорію систем є необхідним, проте і зараз лишається вкрай рідким у застосуванні методом.

У цьому зв'язку виникає питання: а що саме створює підґрунтя для розгляду суб'єктів захисту об'єктів критичної інфраструктури як певної системи?

По-перше, досліджувану категорію можна розглядати як окремий сегмент великої й надскладної соціальної системи (ми назвали цю систему – макросистемою [38]), від професіоналізму і ефективної повсякденної діяльності якого залежить національна безпека, сталий розвиток, а за великим рахунком – життєздатність всієї соціальної системи.

По-друге, виділений сегмент зазначеної системи більше, ніж інші, перебуває на перетинанні з системами природних і штучних техногенних об'єктів.

По-третє, суб'єкти захисту критичної інфраструктури являють собою не поодинокі уповноважені інституції та окремих представників суспільства, а широко розгалужене, структуроване утворення, в межах якого мають місце взаємозв'язки, координація діяльності по вертикалі й горизонталі, а також інтеграція з суміжними державними системами: національної безпеки, цивільного захисту, протидії тероризму, фізичного захисту, кібербезпеки [38, с. 265–266].

І якщо увага того чи іншого вченого зосереджена на якомусь окремому елементі даної системи, це не означає, що її не існує загалом. Окрім зазначеного, суб'єктів державної системи захисту ОКІ можна розглядати і як невіддільний складник ще однієї системи, а саме – єдиної загальнодержавної системи захисту критичної інфраструктури, формування якої в Україні відбувається нині відповідно до «Концепції створення державної системи захисту критичної інфраструктури», затвердженої постановою Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р [39]. Своєю чергою остання входить до системи національної, міжнародної (транснаціональної) та глобальної безпеки. У такий спосіб вибудовується логічна модель інтегрованих між собою систем і підсистем, стрижневим компонентом яких виступають суб'єкти діяльності.

Отже, аналіз наукових публікацій вчених-правників та аналітичних матеріалів фахівців НІСД у досліджуваній галузі дозволив встановити, що натепер виділені й більшою чи меншою мірою описані такі суб'єкти, як окремі державні, в тому числі правоохоронні, органи. Що ж до місцевих державних адміністрацій та органів місцевого самоврядування, окремих неурядових організацій, аналітичних, ситуаційних та кризових центрів, приватних підприємств, то їх роль у захисті ОКІ у наукових публікаціях висвітлена недостатньо, отже, в перспективі належить звернутися і до цих питань.

У цілому ж є сенс зазначити, що недооцінка системного підходу в наукових працях із досліджуваної тематики, з одного боку, утворює своєрідні «білі плями» в загальному реєстрі суб'єктів цієї категорії, з іншого – ускладнює створення наукового підґрунтя щодо розроблення механізму взаємодії суб'єктів задля превенції або подолання кризових ситуацій на об'єктах критичної інфраструктури, відновлення їхнього штатного функціонування.

Підтвердженням тому є й тези, що містяться в аналітичній записці НІСД «Проблеми забезпечення взаємодії при реагуванні на інциденти та кризи комплексного характеру на об'єктах критичної інфраструктури» [40]. Зокрема, вказується: «Масштаб і комплексний характер загроз та наслідків криз, пов'язаних з безпекою критичної інфраструктури, необхідність її захисту від усіх видів фізичних та кіберзагроз вимагають якісно нового рівня координації дій, взаємодії та обміну інформацією між численними суб'єктами процесу реагування» [40]

Переконаний, що без чіткого уявлення про систему суб'єктів захисту ОКІ лише з орієнтацією на окремих виконавців створити й запровадити дієвий механізм протидії загрозам і ризикам практично нереально. Тим більше, що останнім

часом все частіше йдеться про комплексний характер прояву останніх. Тому укладачі цитованої аналітичної записки неодноразово підкреслюють, що задовольнити усі вимоги сьогодення у сфері безпеки критичної інфраструктури можливо лише на системній основі. Натомість відбувається «домінування відомчих підходів, під впливом яких уповноважені державні органи проявляють схильність опікуватися лише певним набором загроз та ризиків» [40]. По суті, це є нічим іншим, як проявом відсутності у конкретного суб'єкта бачення себе як елемента певної системи. Подолання подібного становища уможливлюється лише через створення відповідного наукового підґрунтя та реалізації його у практику діяльності уповноважених юридичних та фізичних осіб.

Згідно з нормами юридичної техніки у текстах законів України визначенню суб'єктів діяльності відводиться окрема стаття, в якій міститься вичерпний перелік таких суб'єктів. У разі необхідності під час подальшого опису в інших статтях відповідного закону надаються їхні повноваження й межі компетенції. Тож натепер переліки суб'єктів сфери забезпечення безпеки представлені у низці законів України, якими здійснюється відповідне правове регулювання. Зокрема, йдеться про такі нормативні акти, як Кодекс цивільного захисту України [41], «Про національну безпеку України» [42], «Про основні засади забезпечення кібербезпеки України» [43], «Про боротьбу з тероризмом» [44], «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» [45], «Про правовий режим надзвичайного стану» [46], «Про правовий режим воєнного стану» [47] та інші.

Оскільки Закон України «Про критичну інфраструктуру та її захист» нині існує лише у формі проекту [24], варто розглянути, як представлена в ньому система суб'єктів порівняно із суміжними ключовими законами, зокрема Законом України «Про національну безпеку України» від 21 червня 2018 р. [42] і Законом України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. [43]. Останній є важливим з огляду на те, що в ньому міститься тлумачення понять *«критично важливі об'єкти інфраструктури»* (об'єкти критичної інфраструктури), *«об'єкт критичної інформаційної інфраструктури»* та закріплені відповідні норми, пов'язані із забезпеченням кібернетичної безпеки таких об'єктів. Найбільш наочно представити результати аналізу є сенс у вигляді таблиці.

Отже, за результатами порівняння унаочнюється, що у переліку суб'єктів повний збіг спостерігається лише щодо Служби безпеки України, розвідувальних органів України та Збройних Сил України. Решта позицій відрізняється. З одного боку, це можна пояснити відмінностями в об'єктах правового регулювання, з іншого – недостатньою взаємною концептуальною узгодженістю законодавчих актів у сфері національної безпеки, непродуманістю та відсутністю стратегічного бачення ролі законодавства в регулюванні правовідносин.

Є підстави стверджувати, що проект Закону України «Про критичну інфраструктуру та її захист» під час визначення суб'єктів має більшу схожість із Законом України «Про основні засади забезпечення кібербезпеки України» (6 збігів), аніж із Законом «Про національну безпеку України» (2 збіги).

У проекті Закону України «Про критичну інфраструктуру та її захист» з'являються принципово нові суб'єкти: *«уповноважений орган у сфері захисту критичної інфраструктури України»* і *«оператори критичної інфраструктури незалежно від форм власності»*. Під останнім укладачі розуміють «державний орган, підприємство, установу, організацію, юридичну та/або фізичну особу, якому / якій на правах власності, оренди або на інших законних підставах належать об'єкти критичної інфраструктури та який / яка відповідає за їх поточне функціонування» [24]. Що ж до пропозиції увести до кола суб'єктів окремий уповноважений орган, то насамперед необхідно визначитися із доцільністю чи недоцільністю такого кроку, науково обґрунтувати кожну з його функцій, запропонованих в проекті Закону України.

Наразі можна констатувати, що в українському безпековому законодавстві з'являється спроба легалізувати ті категорії суб'єктів, які до цього часу в законах не фігурували.

Інновацією є додавання до такого суб'єкта, як Збройні Сили України, «інших військових формувань, утворених відповідно до Законів України». З одного боку, приховування за абстрагованою вказівкою назв конкретних суб'єктів не переобтяжує Закон, не потребуватиме внесення змін у разі змін найменування підрозділів, з іншого – створює необхідність додаткового тлумачення, кого саме мав на увазі законодавець. Тож подібна позиція апріорі виглядає дискусійною.

Звертає на себе увагу і той факт, що в усіх розглянутих документах у переліку суб'єктів відсутні Президент України, Рада національної безпеки і оборони (РНБО), Кабінет Міністрів України. У чинних законах на них покладені функції управління, в тому числі координації діяльності, контролю, кадрових призначень вищого керівництва Міністерства оборони тощо. Подібна практика свідчить, що домінує тенденція відносити до суб'єктів діяльності безпосередніх виконавців, відокремлюючи від них суб'єктів управління. Іноді подібне призводить до певних суперечностей.

Таблиця 1

Порівняльний аналіз системи суб'єктів забезпечення безпеки й захисту об'єктів критичної інфраструктури у законодавстві України

Суб'єкт	Проект Закону України «Про критичну інфраструктуру та її захист»	Закон України «Про національну безпеку України»	Закон України «Про основні засади забезпечення кібербезпеки України»
Уповноважений орган у сфері захисту критичної інфраструктури України	+		
Міністерства та інші центральні органи виконавчої влади	+	Міністерство оборони України, МВС України,	+
Національний банк України			+
Служба безпеки України	+	+	+
Правоохоронні та розвідувальні органи	+	Розвідувальні органи України	+ Контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності
Збройні Сили України, інші військові формування, утворені відповідно до Законів України	+	Збройні Сили України, Державна спеціальна служба транспорту	+
Місцеві державні адміністрації	+		+
Органи місцевого самоврядування	+		+
Оператори критичної інфраструктури незалежно від форми власності	+		
Підприємства, установи та організації незалежно від форми власності, які проводять діяльність, пов'язану із забезпеченням безпеки об'єктів критичної інфраструктури, в тому числі суб'єкти охоронної діяльності.	+		Підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури
Громадські організації, об'єднання та організації роботодавців.	+		
Сектор безпеки і оборони України (складається з чотирьох взаємопов'язаних складників: сили безпеки; сили оборони; оборонно-промисловий комплекс; громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки)		+	
Управління державної охорони		+	
Державна служба спеціального зв'язку та захисту інформації		+	
Центральний орган виконавчої влади, що забезпечує формування та реалізує державну військово-промислову політику		+	
Суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.			+

До прикладу, Президент України в Законі України «Про національну безпеку України» згадується 58 разів, в Законі «Про основні засади забезпечення кібербезпеки в Україні» – 6 разів, у запропонованому проекті Закону – жодного разу. Якщо враховувати, що відповідно до ст. 106 Конституції України Президент України «забезпечує державну незалежність, національну безпеку і правонаступництво держави» [48] (а як вже зазначалося, захист критичної інфраструктури в системному баченні має розглядатися як невіддільний складник системи національної безпеки), то відсутність у зазначеному проекті Президента України ставить під сумнів конституційність самої концепції документа.

Так само можна кваліфікувати як порушення системності безпекового законодавства відсутність у проекті Закону, що розглядається, жодної згадки про РНБО. І це на тлі того, що у ст. 3 Закону України «Про Раду національної безпеки і оборони України» серед її функцій конкретно передбачається «координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України» [49].

Повертаючись до тенденції, за якої законодавець наділяє суб'єктністю лише безпосередніх виконавців тих чи інших функцій, передбачених відповідним законом, продемонструємо ще одне протиріччя.

Так, інтерпретуючи поняття ***«державна система захисту критичної інфраструктури»,*** укладачі проекту Закону «Про критичну інфраструктуру та її захист» тлумачать його як «систему суб'єктів із забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури» [24]. Далі у ч. 1 ст. 13 проекту «Формування та реалізація державної політики у сфері захисту критичної інфраструктури» на Кабінет Міністрів України покладається забезпечення цього напряму політики. При цьому вказаний орган відсутній у переліку суб'єктів, що представлений у ст. 14 зазначеного проекту. У такому разі слід розглядати державну систему захисту критичної інфраструктури дещо інакше, можливо, включаючи до їх кола і Кабінет Міністрів. Принагідно зазначимо, що поняття державної системи захисту критичної інфраструктури не мусить обмежуватися лише суб'єктами, оскільки характеризується комплексним характером і за своїм значенням має суттєво ширший діапазон, який охоплює й інші складники, зокрема, організаційні й технічні заходи, способи забезпечення захисту та інші.

Оскільки доктринальний підхід припускає більш широке бачення, що може відрізнятися від традиційного, представимо власну науково обґрунтовану позицію на систему суб'єктів захисту ОКІ. Авторська класифікація найліпшим чином передається у формі таблиці.

Оскільки майже усі критерії, крім останнього, корелюються із проектом Закону України «Про критичну інфраструктуру та її захист», є сенс прокоментувати авторське бачення розподілу суб'єктів захисту ОКІ за функціональним призначенням.

До **суб'єктів безпосереднього забезпечення захисту ОКІ** пропонуємо відносити такі підсистеми, як:

– управлінсько-координаційна підсистема – охоплює керівників, топ-менеджерів ОКІ, які здійснюють управлінські функції, в тому числі щодо забезпечення стійкого й безперебійного функціонування об'єктів, їхнього захисту; відповідають за паспортизацію об'єктів, сприяють складанню й веденню Національного переліку об'єктів критичної інфраструктури; організують взаємодію з іншими суб'єктами в рамках системи критичної інфраструктури; в межах своїх повноважень скеровують діяльність підлеглих у разі виникнення кризових ситуацій;

– техніко-функціональна підсистема – включає в себе операторів критичної інфраструктури незалежно від форми власності, персонал, що за своїми обов'язками відповідає за функціонування об'єктів у штатному режимі; провадить превентивні заходи щодо запобігання реалізації загроз; перебуває в режимі готовності до виникнення кризових ситуацій; орієнтований на взаємодію з іншими суб'єктами захисту ОКІ; забезпечує режим відновлення штатного функціонування;

– фінансова й матеріально-ресурсна підсистема – представлена суб'єктами (організаціями, установами, їх окремими підрозділами), на яких покладається обов'язок економічного, фінансового забезпечення, постачання необхідних матеріалів, приладів, знаряддя, в тому числі протипожежного, закупівлі необхідних програмних інформаційних продуктів тощо;

– моніторингово-аналітична підсистема – охоплює суб'єктів, на яких покладається обов'язок спостереження за діяльністю технічних та інформаційно-комунікаційних систем на об'єктах, здійснення аналізу щодо можливих загроз і ризиків, підготовки пропозицій керівництву щодо протидії негативним факторам впливу;

– охоронно-превентивна підсистема – має широкий спектр суб'єктів від правоохоронних, розвідувальних, контррозвідувальних органів, окремих суб'єктів оперативно-розшукової діяльності до суб'єктів охоронної діяльності, на яких покладаються обов'язки від підтримання перепускного режиму на ОКІ, фізичного захисту об'єктів до підтримання режиму секретності на об'єктах, а також захисту від несанкціонованих втручань

в роботу систем і механізмів через інформаційно-комунікаційні канали та кіберпростір, включаючи хакерські атаки. Ця підсистема водночас виступає як складник державної системи фізичного захисту з питань захищеності та охорони ядерних установок, ядерних матеріалів, запобігання диверсіям, крадіжкам або будь-якому іншому неправомірному вилученню радіоактивних матеріалів; єдиної державної системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків; національної системи кібербезпеки;

– кризово-ситуативна підсистема – інтегрується із єдиною державною системою цивільного захисту, передбачає залучення до заходів з реагування на кризову ситуацію Державної служби з надзвичайних ситуацій, окремих підрозділів Міністерства оборони України, МВС України, Державної служби спеціального зв'язку та захисту інформації України, Державної спеціальної служби транспорту та інших.

Авторська концепція системи суб'єктів захисту об'єктів критичної інфраструктури не обмежується традиційними підходами, а передбачає виділення ще й такої категорії, як **суб'єкти опосередкованого забезпечення захисту ОКІ**. До неї пропонується віднести такі підсистеми, як:

концептуально-наукова підсистема – включає в себе наукові та науково-дослідні установи, аналітичні організації, авторські колективи, окремих вчених, які створюють фундаментальне й прикладне підґрунтя для формування державної політики у сфері захисту критичної інфраструктури, реалізації відповідних державних Стратегій, сприяють оптимізації діяльності суб'єктів безпосереднього захисту ОКІ;

нормативно-правнича підсистема – охоплює суб'єктів, на яких покладаються обов'язки підготовки, правової експертизи, узгодження, ухвалення нормативно-правових актів, які регулюють питання захисту ОКІ. Сюди можна віднести Верховну Раду України, Департаменти правового забезпечення / юридичні відділи Центральних органів виконавчої влади, задіяні в захисті ОКІ, місцевих органів виконавчої влади, операторів критичної інфраструктури;

кадрова підсистема – включає в себе об'єднання та організації роботодавців, відповідні

Таблиця 2

Класифікація системи суб'єктів захисту об'єктів критичної інфраструктури

Критерій класифікації	Підсистеми суб'єктів захисту в межах системи
За сферами, галузями і секторами об'єктів критичної інфраструктури	Суб'єкти захисту об'єктів критичної інфраструктури – у сфері життєзабезпечення населення; – у галузі; – енергетики; – хімічної промисловості; – транспорту; – оборонно-промислового комплексу; – інформаційно-комунікаційних технологій; – в банківському і фінансовому секторах та ін.
За рівнями управління	Суб'єкти управління загальнодержавного рівня; Суб'єкти управління регіонального та галузевого рівня; Суб'єкти управління місцевого рівня; Суб'єкти управління об'єктового рівня
За категоризацією критичності об'єктів	Суб'єкти захисту критично важливих об'єктів (1 категорія критичності); Суб'єкти захисту життєво важливих об'єктів (II категорія критичності) Суб'єкти захисту важливих об'єктів (III категорія критичності) Суб'єкти захисту об'єктів, безпосередній захист яких є відповідальністю оператора (IV категорія критичності)
За формою власності об'єктів критичної інфраструктури	Суб'єкти захисту ОКІ державної власності; Суб'єкти захисту ОКІ колективної форми власності
За розподілом по видах осіб	Суб'єкти захисту, що є юридичними особами Колективні суб'єкти, що не є юридичними особами (наприклад, громадські організації) Суб'єкти захисту – фізичні особи
За режимом забезпечення захисту	Суб'єкти забезпечення штатного режиму діяльності Суб'єкти забезпечення режиму готовності та запобігання реалізації загроз Суб'єкти реагування на виникнення кризової ситуації Суб'єкти забезпечення режиму відновлення штатного функціонування
За функціональним призначенням	Суб'єкти безпосереднього забезпечення захисту ОКІ Суб'єкти опосередкованого забезпечення захисту ОКІ

підрозділи підприємств, на яких покладається обов'язок підбору й відбору персоналу ОКІ, виявлення благонадійності чи неблагонадійності працівника, кадрового супроводження при зміні ним посади або звільненні, його атестації тощо. До цієї підсистеми також можна віднести окремі підрозділи Служби безпеки України, які відповідно до Закону України «Про державну таємницю» [50] здійснюють спеціальні перевірки для надання особі допуску до державної таємниці, контролюють дотримання режиму секретності працівниками, які мають такі допуски;

– освітньо-кваліфікаційна підсистема – представлена закладами професійної, фахової передвищої, вищої, післядипломної освіти, на базі яких здійснюється підготовка, перепідготовка, підвищення кваліфікації працівників ОКІ. Ще одним напрямом у діяльності цієї підсистеми виступає просвітництво серед населення щодо правомірної поведінки відносно об'єктів критичної інфраструктури, наслідків порушення законів у цій сфері та юридичної відповідальності за вчинене;

– підсистема охорони здоров'я працівників ОКІ – включає в себе спеціалізовані медичні заклади, що задіяні у перевірці кандидатів на роботу на ОКІ, з отриманням даних щодо відсутності в такої особи наркотичної, алкоголічної та інших видів залежності, психічних захворювань, проведення психологічного тестування, а також медичного обслуговування діючого персоналу ОКІ;

– інформаційно-комунікаційна підсистема – охоплює працівників відділів зв'язків з громадськістю, ЗМІ, медійні видання, окремих блогерів, які з урахуванням обмежень, передбачених Законом України «Про державну таємницю», інформують населення про діяльність об'єктів, віднесених в установленому порядку до таких, що мають стратегічне значення для економіки й безпеки держави, а також покликані виконувати функцію правового виховання в аспекті правомірної поведінки щодо об'єктів критичної інфраструктури;

– громадсько-наглядова підсистема – включає в себе громадські організації й рухи, які в межах чинного законодавства беруть участь у публічному управлінні критичною інфраструктурою, здійснюють громадський контроль, можуть виступати з пропозиціями щодо оптимізації діяльності ОКІ з позицій захисту суспільних інтересів у контексті національної безпеки держави.

Безперечно, запропонована авторська концепція не є вичерпною та остаточною, проте вона має інноваційний характер і найбільш повно репрезентує систему суб'єктів захисту об'єктів критичної інфраструктури відповідно до сучасних реалій розвитку держави в епоху постійної ескалації і появі нових видів загроз.

Висновки. Ефективність реалізації державної політики у сфері захисту критичної інфраструктури більшою мірою залежить від діяльності суб'єктів захисту відповідних об'єктів. Проведене дослідження довело правильність робочої гіпотези щодо необхідності розгляду цих суб'єктів як складної розгалуженої системи зі своїми підсистемами, що докорінно відрізняються від тих підходів, які існували до цього. Подібна зміна парадигми як у сфері науки, так і в галузі законотворчості дозволить у подальшому відкрити увесь потенціал можливостей задля вирішення завдань, що слугують забезпеченню безпеки людини, суспільства і держави.

Література

1. Теленик С.С. Завдання і повноваження Служби безпеки України як суб'єкта захисту критичної інфраструктури. *Юридичний бюлетень*. 2019. Вип. 7. Ч. 2. С. 155–163.
2. Єрменчук О.П. Приватний сектор як важливий суб'єкт захисту критичної інфраструктури. *Науковий вісник дніпропетровського держ. ун-ту внутр. справ*. 2019. № 1. С. 62–66.
3. Берлач Г.В. Наукові підходи до системи суб'єктів адміністративно-правового регулювання суб'єктів природних монополій у сфері електричної енергії України. *Правова позиція* 2018. № 2 (21). С. 13–18.
4. Косенко Ю.І., Носов П.С. Механізму ідентифікації та трансформації «знань» суб'єкта критичної інфраструктури. *Інформаційні технології в освіті, науці та виробництві*. 2013. Вип. 3 (4). С. 99–104.
5. Соснін О.В. Проблеми державного управління системою національних інформаційних ресурсів з наукового потенціалу в Україні : [моногр.]. Київ : Ін-т держави і права ім. В.М. Корецького НАН України, 2003. 572 с.
6. Костенко Г.Ф. Теоретичні аспекти стратегії національної безпеки : навчальний посібник. Київ : ЗАТ Видавничий дім «ДЕМІД», 2002. 144 с.
7. Нижник Н.Р., Ситник Г.П., Білоус В.Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : навчальний посібник для вищих навчальних закладів / Українська Академія держ. управління при Президентові України; Академія держ. податкової служби України. Київ : Преса України, 2000. С. 19–40.
8. Данільян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: структура та напрямки реалізації: Навчальний посібник. Харків : Фоліо, 2002. 285 с.
9. Ліпкан В.А. Управління системою національної безпеки України / Володимир Анатолійович Ліпкан. Київ : КНТ, 2006. 68 с.
10. Ліпкан В.А. Національна безпека України у світлі теорії самоорганізації. *Держава і право*. 2002. № 16. С. 142–148.
11. Василькова В.В. Порядок и хаос в развитии социальных систем (Синергетика и теория социальной самоорганизации). Серия мир культуры истории и философии. Санкт-Петербург : Лань, 1999. 480 с.
12. Ліпкан В.А. Безпекознавство : навчальний посібник. Київ, 2003. С. 39–56.
13. Пригожин И. От существующего к возникающему: Время и сложность в физических науках / Пер. с англ. / Под ред., с предисл. И послеслов. Ю.Л. Климонтовича. Изд. 2-е, доп. Москва : Едиториал УРСС, 2002. 288 с.

14. Синергетическая парадигма. Нелинейное мышление в науке и искусстве. Москва : Прогресс-Традиция, 2002. 496 с.

15. Чернавский Д. С. Синергетика и информация. Москва : Наука, 2001. 244 с.

16. Бірюков Д.С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні / Д. С. Бірюков, С. І. Кондратов. Київ : НІСД, 2012. 96 с.

17. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доповідь / за заг. ред. Д. Дубова. Київ : НІМД, 2018. 84 с.

18. Зелена книга з питань захисту критичної інфраструктури в Україні: збірник матеріалів міжнародних експертних нарад. URL: http://old2.niss.gov.ua/articles/2213/.

19. Суходоля О.М. Захист критичної інфраструктури: сучасні виклики та пріоритетні завдання сектору безпеки. *Науковий часопис Академії національної безпеки*. № 1–2 (13–14). 2017. С. 30–80.

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

21. Суходоля О.М. Законодавче забезпечення та механізми управління у сфері енергетичної безпеки України. *Стратегічні пріоритети*. 2019. № 2 (50). С. 13–26.

22. Кондратов С.І. Про забезпечення координації дій, взаємодії та обміну інформацією при створенні державної системи захисту критичної інфраструктури. Київ : НІСД. 30 с.

23. Developing Th e Critical Infrastructure Protection System in Ukraine : monograph / [S. Kondratov, D. Bobro, V. Horbulin et al.] ; general editor O. Sukhodolia. Kyiv : NISS, 2017. 184 p.

24. Проект Закону України «Про критичну інфраструктуру та її захист» від 27.06.2019 № 10328. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996.

25. Великий тлумачний словник сучасної української мови / Уклад. і голов. ред. В. Т. Бусел. Київ ; Ірпінь : ВТФ «Перун», 2003. 1440 с.

26. Сурмин Ю.П. Теория систем и системный анализ. Київ : МАУП, 2003. 368 с.

27. Богуцький П.П. Про використання системного підходу в осягненні цілісності системи права. *Право України*. 2015. № 6. С. 157–164.

28. Ганьба Б. Системний підхід та його застосування в дослідженні державно-правових явищ. *Право України*. 2000. № 3. С. 41–44.

29. Ганьба Б. Системний підхід у державно-правових дослідженнях. *Вісник Львівського університету. Серія Юридична*. Львів, 2000. Вип. 35. С. 59–66.

30. Галюк Р.Б. Системний підхід до правових явищ. *Науковий вісник Херсонського державного університету*. Вип. 6-1. Т.1. 2014. С. 16–19.

31. Заморська Л.І. Системний підхід у дослідженнях правової реальності. *Вісник південного регіонального центру Національної академії правових наук України*. 2016. № 7. С. 38–44.

32. Зіменко О.В. Система права та правова система: поняття та особливості співвідношення. *Вісник Запорізького нац. ун-ту*. 2011. № 4. С. 27–34.

33. Кельман М.С. Методологія сучасного правознавства: становлення та основні напрями розвитку : дис. ... д-ра юрид. наук: 12.00.01. Львів : Льв. держ. ун-т внутр. справ, 2013. 445 с.

34. Ліпкан В. А. Системний підхід до побудови еталонної моделі системи забезпечення національної безпеки. *Науковий вісник Національної академії внутрішніх справ України*. 2002. № 2. С. 19–24.

35. Ліпкан В.А. Синергетичний і гомеостатичний підходи до системи національної безпеки. *Науковий вісник Національної академії внутрішніх справ України*. 2003. № 2. С. 104–111.

36. Ліпкан В.А. Міждисциплінарний підхід до формування національної безпекознавства. *Право України*. 2005. № 1. С. 94–99.

37. Скакун О.Ф. Право і правова система у їх співвідношенні. *Правова держава: щорічник наукових праць Ін-ту держави і права ім. В. М. Корецького НАН України*. Київ, 2005. Вип. 16. С. 30–34.

38. Теленик С.С. Служба безпеки України як суб'єкт державної системи захисту критичної інфраструктури. *Право України*. 2019. № 3. С. 260–286.

39. 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.

40. Проблеми забезпечення взаємодії при реагуванні на інциденти та кризи комплексного характеру на об'єктах критичної інфраструктури: Аналіт. записка НІСД від 07.09.2018. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/problemi-zabezpechennya-vzaemodii-pri-reaguvanni-na-incidenti-ta.

41. Кодекс цивільного захисту України від 2 жовтня 2012 р. (редакція від 01.01.2020). *Відомості Верховної Ради України*, 2013, № 34-35, ст. 458.

42. Про національну безпеку України: Закон України від 21 червня 2018 р. Голос України від 07.07.2018. № 122.

43. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2018 р. (редакція від 08.07.2018). *Голос України* від 08.11.2017. № 208.

44. Про боротьбу з тероризмом: Закон України від 26 березня 2003 р. (редакція від 04.11.2018. *Відомості Верховної Ради України*, 2003, № 25, ст. 180.

45. Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання: Закон України від 19 жовтня 2000 р. (Редакція від 28.12.2015). *Відомості Верховної Ради України*, 2001, № 1, ст. 1.

46. Про правовий режим надзвичайного стану: Закон України від 16 березня 2000 р.(редакція від 28.12.2015). *Відомості Верховної Ради України,* 2000, № 23, ст. 176.

47. Про правовий режим воєнного стану: Закон України від 12 травня 2015 р. (редакція від 26.05.2018). *Відомості Верховної Ради України*, 2015, № 28, ст. 250.

48. Конституція України від 28 червня 1996 р. *Відомості Верховної Ради України* від 23.07.1996 р. , № 30, ст. 141.

49. Про Раду національної безпеки і оборони України: Закон України від 5 березня 1998 р. (редакція від 11.01.2019). *Голос України* від 03.04.1998.

50. Про державну таємницю: Закон України від 21 січня 1994 р. (редакція від 12.07.2018). *Відомості Верховної Ради України*, 1994, № 16, ст. 93.

51. Діордіца І.В. Кібербезпекова політика України: стан та пріоритетні напрями реалізації : монографія. Запоріжжя : Видавничий дім «Гельветика», 2018. 548 с.

52. Ліпкан В.А. Правові засади розвитку інформаційного суспільства в Україні : [монографія] / В.А. Ліпкан, І.М. Сопілко, В.О. Кір'ян / за заг. ред. В.А. Ліпкана. Київ : ФОП О.С. Ліпкан, 2015. 664 с.

53. Сопілко І.М. Органи державної влади як суб'єкти правовідносин щодо отримання інформації.

Малий і середній бізнес (право, держава, економіка). 2009. № 3–4. С. 144–145.

54. Топчій О.В. Адміністративно-правове забезпечення інформаційної безпеки неповнолітніх в Україні: сучасний стан і тенденції реалізації : монографія. Ужгород, 2019. 512 с.

55. Топчій О.В. Компетенції центрального органу виконавчої влади у сфері освіти та науки щодо забезпечення інформаційної безпеки неповнолітніх. *Право і суспільство.* № 4. Дніпро, 2018. С. 141–147.

56. Топчій О.В. Суб'єкти забезпечення інформаційної безпеки неповнолітніх у парадигмі адміністративного права. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія «Юридичні науки»*. № 6. Том 29 (68). Київ, 2018. С. 94–99.

Анотація

Теленик С. С. **Система суб'єктів захисту об'єктів критичної інфраструктури.** – Стаття.

Питання щодо системи суб'єктів захисту об'єктів критичної інфраструктури має не тільки власно наукове, а й суттєве прикладне значення. Особливо воно актуалізується на етапі обговорення проекту Закону України «Про критичну інфраструктуру та її захист». Автор статті насамперед звертається до методології науки, до концепції системи та системології. Це наочно демонструє, що суб'єкти захисту критичної інфраструктури мають усі ознаки системності. Дослідник демонструє взаємозв'язок цієї системи з системою національної, міжнародної та глобальної безпеки. У той же час аналіз наукових джерел свідчить про те, що правові експерти вважають за краще вивчати окремі фрагменти цієї системи, а не її цілісний стан. Це призводить до того, що на практиці координація та взаємодія партнерів є складною. Порівняльний аналіз законопроекту з ключовими законами України у сфері безпеки показує, що ці документи в ряді позицій не узгоджуються між собою. У зв'язку з цим автор представляє власну класифікацію, в якій предмети розподіляються за такими критеріями, як: сфера, галузь та сектор об'єктів; рівні управління; категорії критичності об'єктів; форма власності на об'єкти; режим захисту; функціональне призначення. Нововведення полягає в тому, що в системі предметів за функціональною ознакою розрізняють дві підсистеми. Перша з них об'єднує структури, які безпосередньо захищають критичну інфраструктуру. Друга – охоплює ті сутності, які опосередковано забезпечують захист таких об'єктів. Кожна з підсистем містить власні категорії сутностей, автор яких визначає юридичні характеристики у статті. Дослідник формулює висновок, що лише системний підхід до розуміння суб'єктів критичної інфраструктури на практиці ефективно виконуватиме завдання забезпечення національної безпеки.

Ключові слова: національна безпека України, критична інфраструктура, захист критичної інфраструктури, об'єкти критичної інфраструктури, система суб'єктів захисту критичної інфраструктури, координація і взаємодія суб'єктів захисту критичної інфраструктури; системологія, системи і підсистеми в праві, підсистема безпосереднього забезпечення захисту критичної інфраструктури, підсистема опосередкованого забезпечення захисту критичної інфраструктури.

Summary

Telenyk S. S. **Critical infrastructure protection subject system.** – Article.

The question of the subjects system of protection of critical infrastructure has not only scientific, but also significant applied value. This issue becomes even more relevant when there is a discussion of the draft Law of Ukraine "On critical infrastructure and its protection". The author of the article primarily refers to the methodology of science, to the concept of system and systemology. It clearly demonstrates that the subjects of critical infrastructure protection have all the signs of systemicity. The researcher demonstrates the relationship of this system with the system of national, international and global security. At the same time, an analysis of scientific sources indicates that legal experts prefer to study individual fragments of this system rather than its integral state. This leads to the fact that in practice the coordination and interaction of partners is complicated. A comparative analysis of the draft Law with the key laws of Ukraine in the field of security shows that these documents are not consistent with each other in a number of positions. In this regard, the author presents his own classification, in which subjects are distributed according to criteria such as: sphere, industry, and sector of objects; management levels; criticality categories of objects; ownership form of objects; protection mode; functional purpose. The innovation consists in the fact that in the system of subjects according to a functional attribute two subsystems are distinguished. The first of them brings together entities that directly protect critical infrastructure. The second subsystem covers those entities that indirectly provide protection for such objects. Each of the subsystems contains its own categories of entities whose author defines the legal characteristics in the article. The researcher formulates the conclusion that only a systematic approach to understanding the subjects of critical infrastructure protection will in practice effectively carry out tasks to ensure national security.

Key words: national security of Ukraine, critical infrastructure, protection of critical infrastructure, critical infrastructure objects, system of critical infrastructure protection entities, coordination and interaction of critical infrastructure protection entities, systemology, systems and subsystems in law, subsystem for direct protection of critical infrastructure, subsystem of indirect protection of critical infrastructure.