УДК 351.86
DOI HTTPS://DOI.ORG/10.32782/2524-0374/2021-11/15

# ОСОБЛИВОСТІ СТАНОВЛЕННЯ ПРАВОВИХ ЗАСАД ІСНУВАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ В СИСТЕМІ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ

# PECULIARITIES OF FORMATION OF LEGAL FRAMEWORK OF EXISTENCE OF CRITICAL INFRASTRUCTURE FACILITIES OF UKRAINE IN THE SYSTEM OF THE MINISTRY OF DEFENSE OF UKRAINE

**Ганкевич К.Б., т.в.о. директора**
*Департаменту юридичного забезпечення*
*Міністерство оборони України*

**Левчук В.Д., заслужений юрист України,**
**старший науковий співробітник науково-дослідного відділу**
**проблем військового законодавства Центру воєнно – стратегічних досліджень**
*Національний університет оборони України імені Івана Черняховського*

**Корольов С.С., к.і.н., доцент,**
**начальник кафедри загальновійськових дисциплін**
*Військовий юридичний інститут Національного юридичного університету імені Ярослава Мудрого*

У статті досліджено адміністративно-правові засади існування, функціонування та захисту критичної інфраструктури України з урахуванням впливу передбачуваних загроз у цій системі на стан національної безпеки і оборони держави. У цьому аспекті зазначається, що забезпечення захисту та стабільного функціонування об'єктів критично важливої інфраструктури є важливим та пріоритетним завданням державної політики у сфері національної безпеки і оборони України та її складовим елементом. Наголошено, що особливе місце в аналізованій проблематиці належить питанню формування насправді дієвого правового механізму функціонування даної системи відповідно до сучасних реалій, в яких сьогодні існує Україна, і в яких має забезпечуватися безпека її громадян, суспільства і державних інституцій. Розглянуто сучасний стан правового регулювання критичної інфраструктури як складової частини системи забезпечення національної безпеки на прикладі країн ЄС і США та визначено основні інструменти міжнародного регулювання цієї сфери, пов'язані із захистом об'єктів критичної інфраструктури та секторів, що мають критичне значення. Проаналізовано також чинне законодавство України та напрями національної державної політики у сфері захисту критичної інфраструктури. Зазначається, що в системі національного законодавства питання щодо захисту об'єктів, які згідно міжнародної практики віднесені до сектору критичної інфраструктури, регламентуються низкою нормативно-правових актів, що мають переважно відомчий характер. До кінця не визначеними у правовому полі залишаються й питання щодо вичерпного переліку таких об'єктів, заходів із забезпечення антитерористичної захищеності та оцінки стану систем безпеки критичної інфраструктури в результаті незаконного втручання у функціонування відповідного об'єкта. Акцентується на питанні щодо захисту об'єктів критичної інфраструктури з точки зору інформаційної складової, що має особливе значення в контексті ведення бойових дій на сході України, підтримання державної інформаційної політики на тимчасово окупованих територіях України щодо захисту об'єктів критичної інфраструктури. Зроблено висновок, що в Україні неналежним чином приділяється увага визначенню, захисту та підтриманню об'єктів критичної інфраструктури, що потребує створення необхідного набору правових засобів, які дадуть змогу подолати прогалини правового регулювання у цій сфері.

**Ключові слова:** національна безпека України, нормативне забезпечення, критична інфраструктура, захист критичної інфраструктури, об'єкти критичної інфраструктури, інформаційна безпека.

The article examines the administrative and legal basis for the existence, functioning and protection of critical infrastructure of Ukraine, taking into account the impact of perceived threats in this system on the state of national security and defense. In this aspect, it is noted that ensuring the protection and stable functioning of critical infrastructure is an important and priority task of state policy in the field of national security and defense of Ukraine and its constituent element. It is emphasized that a special place in the analyzed issues belongs to the formation of a truly effective legal mechanism for the functioning of this system in accordance with modern realities in which Ukraine exists today, and in which the security of its citizens, society and state institutions must be ensured. The current state of legal regulation of critical infrastructure as part of the national security system on the example of the EU and the US and identifies the main tools of international regulation in this area, related to the protection of critical infrastructure and critical sectors. The current legislation of Ukraine and the directions of the national state policy in the field of critical infrastructure protection are also analyzed. It is noted that in the system of national legislation, the issues of protection of objects, which according to international practice are classified as critical infrastructure, are regulated by a number of regulations, which are mainly departmental in nature. The issues of an exhaustive list of such facilities, measures to ensure anti-terrorist protection and assessment of the security systems of critical infrastructure as a result of illegal interference in the operation of the facility remain unclear in the legal field. Emphasis is placed on the protection of critical infrastructure from the point of view of the information component, which is especially important in the context of hostilities in eastern Ukraine, maintaining state information policy in the temporarily occupied territories of Ukraine to protect critical infrastructure. It is concluded that Ukraine pays inadequate attention to the identification, protection and maintenance of critical infrastructure, which requires the creation of the necessary set of legal means to overcome the gaps in legal regulation in this area.

**Key words:** national security of Ukraine, normative security, critical infrastructure, protection of critical infrastructure, information of critical infrastructure, information security.

**Постановка проблеми.** Забезпечення захисту та стабільного функціонування об'єктів критично важливої інфраструктури є важливим та пріоритетним завданням державної політики у сфері національної безпеки й оборони України та її складовим елементом. Збройний конфлікт на сході нашої держави, зростання кількості злочинів, що вчиняються в кібернетичному просторі, загострення загальної криміногенної обстановки у сформованих умовах становлять значний ризик для країни та суттєво підвищують уразливість важливих об'єктів інфраструктури, вихід із ладу чи знищення яких може призвести до згубних наслідків у сфері оборони, економіки та безпеки нації, унеможливити нормальне функціонування суспільства у цілому. Саме тому постає нагальна потреба у створенні

комплексної системи захисту критичної інфраструктури від загроз будь-якого типу, розробленні ефективного алгоритму відновлення важливих функцій відповідного об'єкту в разі настання негативних наслідків, подальшому розвитку організаційних, правових, технологічних та інших інструментів охорони критичної інфраструктури й режимів функціонування системи захисту залежно від рівня передбачуваних загроз та ризиків. Особливе місце в цьому аспекті належить питанню формування насправді дієвого правового механізму функціонування названої системи відповідно до сучасних реалій, в яких сьогодні існує Україна, і в яких має забезпечуватися безпека її громадян, суспільства і державних інституцій.

**Аналіз останніх досліджень і публікацій.** Варто зазначити, що дослідженню теоретичних питань, пов'язаних із захистом критичної інфраструктури, в різний час приділяли увагу у своїх працях вчені-правознавці, зокрема О. Андрійко, Д. Бєлов, Д. Бірюков, О. Бондаренко, М. Віхляєв, В. Гаращук, О. Глушкевич, Є. Додін, В. Доненко, О. Дубинський, Н. Коваленко, Т. Коломоєць, В. Колпаков, С. Кондратов, М. Корнієнко, О. Кохановська, І. Крегул, В. Куріло, М. Кучерявенко, В. Ліпкан, М. Лошицький, І. Манжул, А. Монаєнко, В. Настюк, О. Орлюк, В. Павловський, Ю. Піддубний, П. Рабінович, В. Сіренко, О. Світличний, О. Скрипнюк, О. Тильчик, Ю. Шемшученко та інші дослідники.

**Постановка завдання.** Мета статті – дослідження теоретико-концептуальних засад існування та захисту критичної інфраструктури України з метою забезпечення її ефективного адміністративно-правового регулювання, з урахуванням передбачуваних загроз та ризиків в сучасних умовах.

**Виклад основного матеріалу.** Починаючи з 90-х років минулого століття, поняття «критична інфраструктура» перестає бути чутками та починає вживатися у нормативно-правових актах національного законодавства і правових актах міжнародного рівня. І хоча значення чи перелік таких об'єктів у кожній державі дещо відрізняється один від одного, його стратегічне та військове значення складно переоцінити.

Одна з перших країн, де з'явилося таке поняття – США. Так, відповідно до законодавства США критична інфраструктура тлумачиться як «системи та об'єкти, фізичні чи віртуальні, настільки життєво важливі для держави, що недієздатність або знищення таких систем або об'єктів підриває національну безпеку, економіку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з перерахованого вище». Основними об'єктами, які зазвичай вважаються складовими критичної інфраструктури, є такі: енергетичні та транспортні магістральні мережі, нафто- й газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення (водо- й теплопостачання) мегаполісів, утилізації відходів, служби екстреної допомоги населенню та служби реагування на надзвичайні ситуації, високотехнологічні підприємства і підприємства військово промислового комплексу, а також центральні органи влади [1]. Пізніше до цих сфер були додатково включені такі сектори: критичного виробництва, надзвичайних сервісів, базової оборонної індустрії, дамб, хімічний, комерційного устаткування, урядового устаткування, продовольства та сільського господарства, охорони здоров'я, інформаційних технологій та ядерних реакторів, матеріалів та сміття [2]. Крім того, законодавство США включає до складових об'єктів критичної інфраструктури навіть національні символи та пам'ятки культурної спадщини.

Також в останні п'ять років такі організації, як ЄС та НАТО, одним із пріоритетних завдань вважають безпеку країн-членів, причому першочергово – саме об'єкти критичної інфраструктури. Так, на рівні ЄС термін «критична інфраструктура» визначається у двох ключових документах. Перший – «Зелена книга» за Програмою захисту критичної інфраструктури, опублікована у 2005 р. Європейською комісією [3]. Друга – директива Ради ЄС 114 від 8 грудня 2008 р. щодо визначення і позначення європейських критичних інфраструктур і оцінювання необхідності підвищення їх захисту. Директива визначає критичну інфраструктуру як актив, систему чи її частину, що має місце в країнах-членах ЄС, вплив яких у разі відмови, інциденту або зловмисного втручання буде поширюватися як на країну, де такий об'єкт розташований, так і на хоча б одну іншу країну-член ЄС. Згідно з цією директивою, критичність інфраструктури визначається при перевищенні порогових значень впливів на відповідні сектори інфраструктури та її об'єкти. Директива залишає відповідальність за захист критичної інфраструктури національним органам влади [4].

Щодо України, то наша держава лише починає свій шлях до уніфікації розгалуженого і максимального розмитого законодавства щодо об'єктів критичної інфраструктури. Так, нещодавно (16 листопада 2021 р.) Верховна Рада України прийняла Закон України «Про критичну інфраструктуру» [5], який визначає правові та організаційні засади створення та функціонування критичної інфраструктури. Визначено, що критична інфраструктура – це сукупність об'єктів критичної інфраструктури; а об'єкти критичної інфраструктури – це об'єкти інфраструктури, системи, їхні частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам. У законодавстві України важливі з точки зору військового забезпечення та стратегічного планування дефініції понять «безпека» та «захист критичної інфраструктури» відсутні. Натомість, новоприйнятий Закон України «Про критичну інфраструктуру» містить ці поняття.

Так, вказаним законом поняттям «безпека критичної інфраструктури» пропонується називати стан захищеності критичної інфраструктури, за якого забезпечується функціональність, безперервність роботи, цілісність і стійкість об'єктів критичної інфраструктури, а поняттям «захист критичної інфраструктури» – всі види діяльності, що виконуються перед або під час створення, функціонування, відновлення і реорганізації об'єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації.

Своєю чергою, вказані дефініції майже не розкривають фактичний склад речей, тобто лише поверхнево окреслюють такі явища, як безпека та захист критичної інфраструктури. Що стосується питання вичерпного переліку об'єктів критичної інфраструктури, то він в Україні і зовсім відсутній. Натомість новоприйнятий закон передбачає створення відповідного реєстру (стаття 11) «для цілей узгодження дій суб'єктів національної системи захисту критичної інфраструктури формується Реєстр об'єктів критичної інфраструктури».

Одна з причин такої прогалини – це відсутність єдиного підходу до того, який об'єкт має входити до системи критичної інфраструктури, а який не має такого вирішального захисту в обороні держави. Ще однією можливою причиною вбачається недосконалість правового регулювання в аспекті великої кількості нормативно-правових актів в секторі безпеки та оборони держави, що нівелює будь-який порядок та передбачуваність в нормативній базі держави [6].

Якщо ж проаналізувати державну політику у сфері захисту критичної інфраструктури, то слід виділити перелічені нижче напрями:

– забезпечення безперебійного та стійкого функціонування об'єктів критичної інфраструктури, запобігання

проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури, підвищення рівня їх захисту, безпеки та стійкості до загроз будь-якого типу, зокрема, терористичних актів;

– гарантування безпеки в процесі розроблення та реалізації основних проєктів у області інфраструктури для транспортування нафти, нафтопродуктів, газу й інших стратегічних сировинних матеріалів.

Останній напрям було підтверджено заявою, зробленою за результатами саміту країн НАТО (п. 522 ), що відбувся 20–21 травня 2012 р. у м. Чикаго (США). Відповідно до Стратегії національної безпеки, пріоритетами забезпечення безпеки критичної інфраструктури є:

– комплексне вдосконалення правової основи захисту критичної інфраструктури, створення системи державного управління її безпекою;

– посилення охорони об'єктів критичної інфраструктури, зокрема енергетичної і транспортної;

– налагодження співробітництва між суб'єктами захисту критичної інфраструктури, розвиток державно-приватного партнерства у сфері запобігання надзвичайним ситуаціям та реагування на них;

– розробка та запровадження механізмів обміну інформацією між державними органами, приватним сектором і населенням стосовно загроз критичній інфраструктурі та захисту чутливої інформації у цій сфері, тощо [7].

З метою забезпечення комплексного вдосконалення правової основи захисту критичної інфраструктури та створення системи державного управління її безпекою Рада національної безпеки і оборони України 29 грудня 2016 р. на своєму засіданні розглянула стан реалізації пріоритетних напрямів державної політики національної безпеки України щодо забезпечення безпеки критичної інфраструктури, визначених Стратегією національної безпеки України [8].

Проте стає очевидним, що ці положення сьогодні є застарілими, оскільки майже не мають економічної складової та новітньої кіберінформаційної безпеки. Що стосується економічної безпеки в контексті критичної інфраструктури, то особливу роль захисту критичної інфраструктури відзначають також експерти Світового банку. Вони наголошують на тому, що хоча й слід здійснювати якісне проєктування й будування будь-якої інфраструктури, але виокремлення категорії критичних об'єктів інфраструктури дасть змогу урядам приділяти останнім особливу увагу, зменшуючи тим самим наслідки, спричинені природними лихами й техногенними аваріями. Саме тому у вказаному питанні обов'язково має бути проаналізований та імплементований міжнародний досвід [9]. Також слід відзначити, що у системі національного законодавства питання щодо захисту об'єктів, які згідно з міжнародною практикою віднесені до сектору критичної інфраструктури, регламентуються низкою нормативно-правових актів, що мають переважно відомчий характер.

Щодо антитерористичної захищеності об'єктів критичної інфраструктури треба зазначити, що в рамках державної системи фізичного захисту за результатами оцінки вразливості формуються документи, що певною мірою відповідають паспорту потенційно небезпечного об'єкта, але є значно ширшими з точки зору оцінки загроз [10]. До кінця не визначеними у правовому полі залишаються й питання щодо заходів із забезпечення антитерористичної захищеності та оцінки стану систем безпеки критичної інфраструктури в результаті незаконного втручання у функціонування відповідного об'єкта.

Як показує сьогодення, основою забезпечення захищеності й безпеки критичної інфраструктури є вирішення низки питань, з-поміж яких основними є такі: координація і взаємодія органів державної влади та обмін інформацією про загрози; організація державно-приватного партнерства у сфері безпеки; використання ризик-орієнтованого підходу при попередженні загроз критичній інфраструктурі.

І врешті, найбільш актуальним стає питання захисту об'єктів критичної інфраструктури з точки зору інформаційної складової. Уперше поняття «інформаційної безпеки» в Україні було визначено в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 9 січня 2007 р. № 537-V [11]. У 2018 р. набрав чинності Закон України «Про основні засади забезпечення кібербезпеки України», яким було запроваджено термін об'єкта критичної інфраструктури, встановлено повноваження для формування переліку об'єктів критичної інфраструктури, задекларовано спеціальний режим для операторів критичної інфраструктури. Чинний Закон визначає, що до об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації, які провадять діяльність та надають послуги в галузі енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах [12]. Проте у згаданому нормативно-правовому акті так і не були встановлені критерії, згідно з якими ті чи інші об'єкти можуть бути ідентифіковані як об'єкти критичної інфраструктури.

Згідно з даними програми щодо Постійного структурного співробітництва з питань безпеки і оборони PESCO, було визначено два основних стратегічних шляхи, а саме:

– створення загальної мережної платформи для обміну інформацією щодо кіберзагроз об'єктам критичної інфраструктури між державами;

– створення єдиної розгалуженої системи центрів реагування та протидії загрозам об'єктам критичної інфраструктури в кіберпросторі – системи колективного реагування на такі кіберінциденти.

Приєднання до цих проєктів означає необхідність створення відповідної системи кібербезпеки в державі з урахуванням вимог Європейської комісії стосовно кіберзахисту об'єктів критичної інфраструктури та доведення її можливостей виконувати всі завдання з кіберзахисту на відповідному рівні, у зв'язку з чим виникає питання щодо потенційних можливостей країни стосовно досягнення та підтримки необхідного рівня забезпечення та спроможностей в сфері кіберзахисту [13].

Сьогодні наша держава має величезну прогалину у здійсненні інформаційної безпеки, особливо в контексті ведення бойових дій на сході України, підтримання державної інформаційної політики на тимчасово окупованих територіях України щодо захисту об'єктів критичної інфраструктури. Навіть більше, незважаючи на велику кількість нормативних актів у сфері безпеки і оборони, загалом не здійснено комплексної оцінки ризиків знищення чи ушкодження об'єктів критичної інфраструктури.

Водночас слід зазначити, що збитки від кібернетичних атак на об'єкти критичної інфраструктури можуть вимірюватися не лише фінансовими втратами, а й впливом на економіку держави, безпеку життєдіяльності громадян та загальну суспільно-політичну ситуацію в країні загалом. Кіберзлочинці прагнуть захопити максимальний контроль над інфраструктурою, атакуючи системи IT-управління шляхом зараження робочих станцій шкідливим програмним забезпеченням, яке використовується для знищення, копіювання, блокування, модифікації інформації в критичній інфраструктурі, або нейтралізації засобів захисту зазначеної інформації. Очевидно, що наша держава не зможе ефективно реагувати на загрози та виклики щодо захисту інформаційного простору без створення відповідної системи кібербезпеки критичної інфраструктури та необхідного набору правових засобів, що дозволять подолати прогалини правового регулювання у цій сфері.

**Висновки.** Таким чином, слід визнати, що в Україні неналежним чином приділяється увага визначенню,

захисту та підтриманню об'єктів критичної інфраструктури. За цих обставин основним недоліком нормативного забезпечення захисту об'єктів критичної інфраструктури є відсутність вичерпного переліку таких об'єктів, відсутність ефективного й дієвого порядку їх паспортизації та категоризації, що значно ускладнює діяльність Збройних Сил України, особливо в районі проведення операції Об'єднаних сил.

**ЛІТЕРАТУРА**


1. Крижний А.В. Еволюція поглядів та особливості інженерного забезпечення підготовки і ведення територіальної оборони України. / А.В. Крижний та ін. *Труди університету:* зб. наук. праць. Київ : НУОУ, 2011. № 6(105). С. 198–203.
2. National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience.
3. Green Paper on a European Programme for Critical Infrastructure Protection: European Commission, 2006. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/ PDF/?uri=CELEX:52006DC0786&from=EN.
4. 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. (2008). *European Council. Official Journal of the European Union,* L 345, 75–80. URL: https://publications.europa.eu/en/publication-detail/-/publication/ ba51b03f-66f4-4807-bf7d-c66244414b10.
5. Прийнято Закон «Про критичну інфраструктуру». *Інформаційне управління Апарату Верховної Ради України.* Опубліковано 16 листопада 2021 р. URL: https://www.rada.gov.ua/news/Novyny/216426.html.
6. Устименко О.В. Ретроспективний аналіз стану аеродромної мережі Повітряних Сил Збройних Сил України. *Наука і техніка Повітряних Сил Збройних Сил України.* Харків : ХУПС, 2013. Вип. № 3(12). С. 32–34.
7. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 р. «Про Стратегію національної безпеки України» : Указ Президента України. *База даних «Законодавство України».* URL: http://zakon2.rada.gov.ua/laws/show/287/2015/paran7#n7
8. Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури : Рішення Ради Національної безпеки і оборони України від 29 грудня 2016 р. *База даних «Законодавство України».* URL: https://zakon.rada.gov.ua/laws/show/n0014525-16#Text
9. Захист критичної інфраструктури : проблеми та перспективи впровадження в Україні / Д.С. Бірюков, С.І. Кондратов. Київ : НІСД, 2012. 96 с.
10. Про затвердження Порядку функціонування державної системи фізичного захисту : Постанова Кабінету Міністрів України від 21 грудня 2011 р. № 1337. URL: *База даних «Законодавство України».* http://zakon0.rada.gov.ua/laws/show/1337-2011-%D0%BF
11. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 9 січня 2007 р. № 537-V. *Відомості Верховної Ради України* (ВВР). 2007. № 12. Ст. 102.
12. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403.
13. Бірюков Д.С., Кондратов С.І. Актуальні питання захисту критично важливої для життєдіяльності держави інфраструктури. *Стратегічні пріоритети.* Київ : НІСД. 2012. Вип. № 3(24). С. 107–113.