УДК 351:65.012.8:33
DOI https://doi.org/10.32782/TNU-2663-6468/2023.4/02

***Возненко О.М.***
Національний технічний університет України
«Київський політехнічний інституту імені Ігоря Сікорського»

# ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ЄВРОПЕЙСЬКИЙ І НАЦІОНАЛЬНИЙ ПІДХОДИ

*У статті розглядаються питання формування нормативно-правового регулювання у сфері захисту критичної інфраструктури в ЕС та Україні. Основною метою статті є узагальнення основних підходів до управління об'єктами критичної інфраструктури та їх відображення у європейському та національному правовому полі. Показана еволюція підходів до регулювання забезпечення безпеки критичної інфраструктури: від захисту об'єктів критичної інфраструктури (ОКІ), які визначають найважливіші умови життєдіяльності людини, – до забезпечення стійкості розгалуженої системи ключових інституцій і підприємств, функціонування яких впливає на міжнародну, національну, регіональну безпеку людини, бізнесу, демократичних інститутів і їх взаємодії. Розкрито у хронологічному порядку прийняття в ЄС основних документів за період з 2005 року по теперішній час, визначено основні тенденції та підходи до забезпечення захисту критичної інфраструктури. Проаналізовано принципи створення системи захисту критичної інфраструктури, які вперше були сформульовані в ЄС у 2005 році. Показано, що розширювалися напрями, галузі, сфери діяльності, що були віднесені до критичної інфраструктури; рівні управління (мега-, меза-, макро, мікрорівні), цільові об'єкти впливу та загроз (інформація, техніка, фінанси та банки, кібернетичні системи, системи життєдіяльності людини, засоби масової інформації) і врахування чинників територій (їх розташування, локалізація діяльності, що може впливати на рівні більш високого порядку). Також підкреслювалось значення превентивних заходів забезпечення безпеки ОКІ, а також швидкого реагування на небажані або незаплановані події. Нарешті, створювалась специфічна інфраструктура, яка обслуговувала систему захисту об'єктів критичної інфраструктури. Охарактеризовано віхи урегулювання питань, пов'язаних із створенням системи захисту критичної інфраструктури в Україні. Доведено, що підходи щодо формування національного законодавства в основному гармонізовані з підходами, що міститься в законодавстві Європейського Союзу.*

***Ключові слова:*** *об'єкти критичної інфраструктури, критична інфраструктура, забезпечення безпеки критичної інфраструктури, нормативно-правове регулювання, Європейська програма захисту критичної інфраструктури, принципи захисту критичної інфраструктури.*

**Постановка проблеми.** Об'єкти критичної інфраструктури (ОКІ) та забезпечення їх безпеки традиційно виходили за рамки наднаціонального регулювання та лишалися в царині національного. Однак із зростанням загроз безпеки, які зачіпають інтереси багатьох країн, їх населення, бізнесу, демократичних основ існування, інформації, питання захисту ОКІ було поставлено на наднаціональному рівні. Досить широка практика функціонування критичної інфраструктури у практично всіх регіонах світу доводить, що різного роду загрози діяльності окремому об'єкту критичної інфраструктури, з першого погляду обмеженої територіально або галузево, можуть мати значний вплив на широке коло учасників у різних інфраструктурах, регіонах, країнах. Це вимагає розроблення підходів і програм щодо інтернаціоналізації системи управління протидією усіляким загрозам ОКІ. В умовах воєнного стану в Україні загострилося проблема порушення нормального ритму роботи подібних об'єктів. Отже, особливу увагу доцільно приділити вирішенню проблеми формування правової основи регулювання цих процесів та гармонізувати їх з підходами, прийнятими в ЄС.

**Аналіз досліджень і публікацій.** Проблематиці захисту критичної інфраструктури присвячено чимало наукових праць. Однією з основоположних наукових праць із проблематики забезпечення стійкості критичної інфраструктури є робота Д. Бобро. Вчений систематизує загрози критичній інфраструктурі, визначає критерії її оцінювання [1]. У статті Б. Богдана йдеться про законодавче забезпечення формування системи захисту критичної інфраструктури в Україні [2]. У роботах О. Мельничука, окрім аналізу методологічної

складової моделювання процесів управління критичною інфраструктурою, запропоновано оригінальну модель системи управління критичною інфраструктурою на рівні регіону та схема її впровадження [4]. О. Суходоля та інші співробітники Національного інституту стратегічних досліджень ґрунтовно розглядають питання захисту критичної інфраструктури з точки зору забезпечення національної безпеки країни [3]. У роботі [8] систематизовано наукові підходи до поняття «загроза об'єктам критичної інфраструктури» та розглядаються дії загроз на різних рівнях ієрархії системи управління.

Незважаючи на значний пласт наукових праць, що присвячено питанням управління об'єктами критичної інфраструктури та забезпечення їх стійкості до різного роду викликів і загроз, замало робіт (за виключенням [9; 16]) присвячено формуванню правового механізму управління ОКІ в Європейському Союзі та в Україні в їх поступовому та гармонічному взаєморозвиткові.

**Мета статті** – узагальнення основних підходів до управління об'єктами критичної інфраструктури та їх відображення у європейському та національному правовому регулюванні.

**Методи дослідження:** метод аналізу та синтезу застосовувався для систематизації підходів щодо формування системи захисту критичної інфраструктури; метод порівняльного аналізу – для співставлення окремих положень законодавства в ЄС та Україні. Також застосовувався метод абстракції, узагальнення, системний підхід та інші методи і підходи наукового пошуку.

**Виклад основного матеріалу дослідження.** Робота із розроблення системи захисту об'єктів критичної інфраструктури в ЄС почалася на початку тисячоліття. Факторами, які стимулювали її активізацію, були безпрецедентні масштаби нарощування потужностей критичної інфраструктури, а також посилення тероризму, техногенних катастроф, зростання негативних наслідків їх реалізації.

Одним із перших документів в ЄС, які побачили світло в листопаді 2005 року, була Зелена книга з Європейської програми захисту критичної інфраструктури [10]. Її створенню передували численні семінари та обговорення, а також дослідження з питань реагування європейської спільноти на загрози від терористичних атак. У документі було визначено ключові принципи формування Європейської програми захисту критичної інфраструктури, а саме: субсидіарність, компліментарність, конфіденційність, кооперація між стейкхолдерами, пропорційність. Останнє передбачало врахування ступеню ризику, співвідношення між витратами та ефектом від заходів, рівень критичності, рівень досягнутої безпеки та ефективності стратегії пом'якшення негативних впливів [10]. Отже, вже в цьому першому документі зазначено про встановлення вибірковості та пріоритетності при реалізації стратегії та тактики управління критичною інфраструктурою.

У 2006-му році була прийнята Європейська програма захисту критичної інфраструктури (European Programme for Critical Infrastructure Protection), а у 2008 році – директива Ради Європи [13], далі – Директива (2008).

Як визначено у статті 2 Директиви (2008), критична інфраструктура ЄС – це розташований в державах-членах актив, система або їх частина, що має важливе значення для підтримки життєво важливих суспільних функцій, зокрема здоров'я, безпеки, економічного чи соціального благополуччя людей, порушення або знищення яких мали б значний вплив у державі-члені в результаті невиконання або можливості невиконання технічного забезпечення цих функцій.

Як видно з визначення, об'єкти критичної інфраструктури ЄС розглядаються, по-перше, як активи, які належать країні-члени Співтовариства; по-друге, як складова забезпечувального комплексу соціальних, духовних і матеріальних благ, які мають надаватися людині. Водночас, загроза економіці окремої країни і/або співтовариству не знайшла відображення у цьому визначенні від 2008 року. Також не розглянуто ще один важливий аспект – загроза демократії, її цінностям і встановленим правилам «гри».

Стокгольмська програма – «Відкрита та безпечна Європа на благо та захист громадян» (the stockholm.., далі – Стокгольмська програма) продовжує тенденцію щодо вироблення системи заходів в сфері запобігання тероризму, тяжких злочинів, загроз інформаційній безпеці, а також їх виявлення та проведення заходів протидії. Стокгольмська програма передбачала розроблення стратегічного підходу щодо досягнення безпеки на період 2010–2014 рр., що був зосереджений навколо п'яти основних пріоритетів, серед яких був і захист ОКІ [12; 17].

Зауважимо, що у п. 4.2.3 «Мобілізація необхідних технологічних засобів» визначено необхідність розробляти та впроваджувати політику для забезпечення високого рівня мережевої та інформаційної безпеки в усьому Союзі та покращувати заходи, спрямовані на захист, готовність до безпеки та стійкість критичної інфраструктури,

включаючи інформаційні та комунікаційні технології (ІКТ) та інфраструктуру послуг; просувати законодавство, яке забезпечує дуже високий рівень безпеки мережі та дозволяє швидше реагувати в разі кібератак [12]. Тобто, поставлена більш широке завдання, яке включає і заходи боротьби із загрозами інформаційній і кібербезпеці.

У п. 7.3 запобігання та захист критичної інфраструктури, внутрішня та зовнішня безпека заявлена пріоритетом антитерористичної діяльності Союзу. Також, що дуже важливо для подальших дій ЄС, окреслено бажання співтовариства співпрацювати з ключовими стратегічними партнерами, серед яких названо Євроюст, Європол, а також Frontex. Основними точками «дотику» визначено обмін інформацією, запобігання радикалізації та вербування [12].

Зауважимо, що програми, подібні до Стокгольмської, є політичним документом і не є обов'язковими для виконання. Однак вони є підставою для подальшого розвитку законодавства та прийняття відповідних рішень.

Протягом 2007–2012 рр. у рамках Програми запобігання, готовності та ліквідації наслідків тероризму та інших ризиків, пов'язаних з безпекою (the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks programme (CIPS), далі Програма) Європейською Комісією профінансовано понад 100 різноманітних проєктів. Передусім Програма була розроблена для захисту громадян і об'єктів критичної інфраструктури від терористичних атак та інших інцидентів порушення безпеки. Програмою передбачались дії щодо сприяння попередженню та підвищення рівня готовності до захисту критичної інфраструктури та вирішення проблем управління кризою. Основною метою реалізації проєктів була підтримка пріоритетів політики ЄС шляхом надання експертних знань і формування наукової основи для кращого розуміння критичних моментів і організації взаємодії на всіх рівнях [14].

В якості інформаційного ресурсу Європейська Комісія розробила інформаційну мережу попередження про критичну інфраструктуру (Critical Infrastructure Warning Information Network, CIWIN), яка працює з середини січня 2013 року. Ця мережа забезпечує багаторівневу систему в Інтернеті для обміну ідеями, дослідженнями та передовою практикою щодо захисту критичної інфраструктури, а також служить сховищем інформації, пов'язаної з цими процесами. Портал CIWIN спрямований на підвищення обізнаності та сприяння захисту критичної інфраструктури в Європі [14].

У 2013 році було оголошено більш широкий порівняно з Програмою 2006 року підхід до захисту критичної інфраструктури, що визначав взаємозалежність між ОКІ, галуззю та державними акторами [15, p. 14]. Як йдеться в документі, новий підхід до EPCIP базується на практичній реалізації діяльності щодо запобігання загроз, готовності до випробувань та адекватного реагування на них [11].

У грудні 2020 року Європейська Комісія, ґрунтуючись на кількох проміжних звітах і широкому обговоренні проблематики під час публічних слухань зацікавлених сторін, опублікувала свою пропозицію замінити Директиву ЕС по критичній інфраструктурі новою, відомою як Директива «Про стійкість об'єктів критичної інфраструктури» (далі – Директива 2022). Ця нова директива була остаточно затверджена у 2022 році та має обов'язковий правовий статус для 27 держав-членів [15].

Як визначено у ст. 2 Директиви 2022, в контексті захисту ОКІ «стійкість» означає здатність запобігти, протистояти, пом'якшити дію, пристосуватися, а також відновити роботу критично важливого об'єкту після інциденту, який порушує або може порушити його діяльність». Тобто, мова йде про передусім про превентивні дії щодо захисту ОКІ, визначення напряму реагування під час лиха, а також розроблення програми дій відновлення нормального функціонування об'єкту. Відзначимо також, що в документі Європейської комісії визначається «стійкість на рівні оператора та системну стійкість» [15]. Такий підхід пов'язує між собою управлінські дії на мікро- та макрорівні.

Отже, загальний еволюційний шлях розвитку європейського правового поля в питаннях захисту критичної інфраструктури означав все ширше розуміння напрямів (галузей, сфер діяльності), рівнів (мега-, меза-, макро-, мікрорівні), цільових систем (інформаційної, технічної, фінансової, кібернетичної, системи життєдіяльності людини, засоби масової інформації) і територій (їх розташування, локалізація діяльності, що може впливати на рівні більш високого порядку), які мають бути охоплені. Також зміщувався акцент у бік превентивних заходів забезпечення безпеки ОКІ, а також швидкого реагування на небажані або незаплановані події. З цією метою створювалась специфічна інфраструктура, яка обслуговувала систему захисту об'єктів критичної інфраструктури.

В умовах військового стану в Україні, коли порушено або загалом припинено нормальне

функціонування багатьох об'єктів критичної інфраструктури, а також відбувається загроза інформаційно-комунікативній сфері, слід проаналізувати національне законодавство в напряму розроблення стратегії забезпечення стійкості ОКІ.

Зауважимо, що нормативно-правове регулювання сфери управління об'єктами критичної в Україні відбувалось в унісон з аналогічними процесами в ЄС лише з невеликим лагом запізнення. Більшість з визначень, які були затверджені у відповідних актах, гармонізовані з визначеннями в програмах і документах Європейської комісії.

Зокрема, у Законі України «Про критичну інфраструктуру» захист критичної інфраструктури розуміється досить широко як «… 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» [5, стаття 1]. Тобто, загалом наведене визначення охоплює широке коло діяльності із формування системи забезпечення захисту критичної інфраструктури.

Зауважимо, що в Концепції створення державної системи захисту критичної інфраструктури, яка була прийнята у 2017 році, створення нормативно-правової бази з питань організації діяльності у сфері захисту критичної інфраструктури названа одним із трьох основних напрямів роботи державних органів і суб'єктів господарювання. Двома іншими напрямами окреслено створення організаційно-інституційної структури та визначення повноважень, завдань та відповідальності суб'єктів державної системи захисту критичної інфраструктури [6].

Постановою Кабінету Міністрів України визначено основні функції та завдання Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України (далі – Постанова) [7]. Зауважимо, однак, що тимчасово Постанова не діє, а обов'язки з виконання зазначених функцій перекладено на Державну службу спеціального зв'язку та захисту інформації України. Водночас, завдання цієї інституції виписано досить повно та масштабно. Серед основних завдань окреслено: проведення оцінки захищеності об'єктів критичної інфраструктури та оцінки загроз у секторальній та функціональній площинах; створення та управління базами даних; розроблення нормативно-технічної бази з питань забезпечення безпеки об'єктів критичної інфраструктури, встановлення обов'язкових вимог із забезпечення безпеки об'єктів критичної інфраструктури, їх захищеності на всіх етапах життєвого циклу, у тому числі під час створення, прийняття в експлуатацію, модернізації; забезпечення взаємодії національної системи захисту критичної інфраструктури з відповідними міжнародними системами, насамперед європейськими та євроатлантичними; розроблення відповідних державних цільових програм і їх реалізація (п. 3 Положення). Водночас зауважимо, що виконання таких завдань потребує значного фінансування та великого штату кваліфікованих, обізнаних працівників. Із закінченням воєнного стану в Україні на перший план постане завдання створення системи превенції загрозам ОКІ та підготовки кваліфікованого персоналу в державних і приватних структурах.

**Висновки.** Отже, можна дійти до висновків, що захист критичної інфраструктури має найвищий пріоритет серед завдань, які постають перед будь-якою країною та її органами управління, однак є особливо важливим в умовах військових дій або їх загрози. Нормативно-правова основа щодо управління процесами забезпечення безпеки критичної інфраструктури в Україні в основному створена. В умовах воєнного стану найбільш актуальним завданням стає формування та наповнення бази даних щодо загроз ОКІ та управлінських, технічних, фінансових, інформаційно-аналітичних рішеннях, які стануть у нагоді при систематизації дій щодо управління ОКІ.

**Список літератури:**

1. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. *Стратегічні пріоритети.* Серія : Економіка. 2015. № 4. С. 83–93.

2. Богдан Б. В. Актуальні питання нормативно-правового регулювання захисту критичної інфраструктури в умовах воєнного стану в Україні. *Проблеми сучасних трансформацій.* Серія : право, публічне управління та адміністрування. 2022. № 6. URL: https://doi.org/10.54929/2786-5746-2022-6-01-09 (дата звернення 12.07.2023).

3. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. / за ред. О. М. Суходолі. Київ : НІСД, 2020. 28 с.

4. Мельничук О. Управління критичною інфраструктурою: модель та її впровадження. *Актуальні проблеми державного управління.* 2020. 1 (81). С. 64–74.

5. Про критичну інфраструктуру. Закон України від 16 листопада 2021 року № 1882-IX, Редакція від 05.12.2022. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text, стаття 1 (дата звернення 08.07.2023).

6. Про схвалення Концепції створення державної системи захисту критичної інфраструктури. Розпорядження Кабінету Міністрів України від 06.12.2017 р. № 1009-р. URL: http://zakon0.rada.gov.ua/laws/show/1009-2017-%D1%80 (дата звернення 11.07.2023).

7. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України. Постанова Кабінету Міністрів від 12 липня 2022 р. № 787. URL: https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#n13 (дата звернення 07.07.2023).

8. Яременко О. І., Страхніцький Я. О. Теоретико-методичні основи забезпечення системи захисту критичної інфраструктури держави. *Державне управління: удосконалення та розвиток.* 2022. № 1. URL: http://www.dy.nayka.com.ua/?op=1&z=2610 (дата звернення: 09.07.2023). DOI: 10.32702/2307-2156-2022.1.38.

9. Christer Pursiainen & Eero Kytömaa. From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure.* 2023. #8:sup1. Pp. 85–101, DOI: 10.1080/23789689.2022.2128562.

10. Commission of the European Communities. Green Paper on a European programme for critical infrastructure protection. 2005. URL: https://op.europa.eu/en/publication-detail/-/publication/4e3f9be0-ce1c-4f5c-9fdc-07bdd441fb88/language-en]/ (дата звернення: 19.07.2023).

11. Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure. Brussels, 28.8.2013. SWD(2013) 318 final Conclusions of the European Council of 10/11 December 2009 on «The Stockholm Programme – An open and secure Europe serving and protecting citizens (2010–2014)»; 17024/09 (дата звернення: 18.07.2023).

12. Conclusions of the European Council of 10/11 December 2009 on «The Stockholm Programme – An open and secure Europe serving and protecting citizens (2010–2014)»; 17024/09 (дата звернення: 12.07.2023).

13. 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. *Official Journal of the European Union.* L345/75. (дата звернення: 22.07.2023).

14. Critical infrastructure. URL: https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en (дата звернення: 03.07.2023).

15. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557 (дата звернення: 03.07.2023).

16. Interdependency: A bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other.' Steven M. Rinaldi, James P. Peerenboom, Terrence K. Kelly, Identifying, Understanding and Analysing Critical Infrastructure Interdependencies, *IEEE Control Systems Magazine.* December 2001. P. 14.

17. The Stockholm Programme – An open and secure Europe serving and protecting citizens. Document 52010XG0504(01). Official Journal of the European Union. 2010/C 115/01. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2010.115.01.0001.01.ENG&toc=OJ%3AC%3A2010%3A115%3ATOC (дата звернення: 03.07.2023).

**Voznenko O.M. ENSURING THE SECURITY OF CRITICAL INFRASTRUCTURE: EUROPEAN AND NATIONAL APPROACHES**

*The article discusses the issues of formation of legal regulation in the sphere of critical infrastructure protection in the EU and Ukraine. The main aim of the article is to generalize the main approaches to management of critical infrastructure objects and their reflection in the European and national legal field. The evolution of approaches to regulating the security of critical infrastructure is shown: from protection of critical infrastructure objects (OCI), which determine the most important conditions of human life, to ensuring the stability of an extensive system of key institutions and enterprises, the functioning of which affects international, national, regional security of man, business, democratic institutions and their interaction. The chronological order of adoption in the EU of the main documents for the period from 2005 to the present is disclosed, the main trends and approaches to ensuring the protection of critical infrastructure are determined. The principles of creating a critical infrastructure protection system, which were first formulated in the EU in 2005, are analyzed. It is shown that the directions, industries, spheres of activity that were classified as critical infrastructure were expanded; levels of management (mega-, mesa-, macro, micro levels), target objects of influence and threats (information, technology, finance and banks, cybernetic systems, human life systems, media) and taking into account factors of territories (their location, localization of activities that can affect at higher levels). The importance of preventive measures to ensure the safety of OCIs, as well as rapid response*

*to unwanted or unplanned events, was also emphasized. Finally, a specific infrastructure was created that served the system of protection of critical infrastructure objects. The milestones of settlement of issues related to the creation of a system of protection of critical infrastructure in Ukraine are characterized. It is proved that approaches to the formation of national legislation are mainly harmonized with the approaches contained in the legislation of the European Union.*

***Key words:*** *critical infrastructure objects, critical infrastructure, critical infrastructure security, legal regulation, European Program for the Protection of Critical Infrastructure, principles of critical infrastructure protection.*