**Богдана БОГДАН,**
кандидат юридичних наук, доцент,
професор кафедри публічного та міжнародного права
навчально-наукового інституту «Юридичний інститут
Київського національного економічного університету
імені Вадима Гетьмана», уповноважений з антикорупційної
діяльності Київського національного економічного
університету імені Вадима Гетьмана, Київ, Україна
ORCID: https://orcid.org/0000-0002-0422-7021
e-mail: bvbogdan@ukr.net

**DOI: https://doi.org/10.32620/pls.2025.67.06**

# НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

***Анотація:*** *Критична інформаційна інфраструктура тривалий час перебуває у фокусі уваги держави в цілому, оскільки особливо протягом введеного воєнного стану на території України є об'єктом, якому ворожими силами завдається суттєва шкода. Державні інституції мають сприяти забезпеченню належного захисту критичної інформаційної інфраструктури через сукупність організаційних, нормативно-правових, інженерно-технічних та інших заходів з метою забезпечення безпеки об'єктів критичної інформаційної інфраструктури. Наразі не передбачено вичерпного переліку заходів, за допомогою яких має забезпечуватись захист критичної інформаційної інфраструктури. Метою цього дослідження є аналіз стану нормативно-правових засад, на підставі яких в державі унормовується правове забезпечення заходів захисту критичної інформаційної інфраструктури.*

***Ключові слова:*** *захист, критична інфраструктура, безпека, інформація, кібербезпека, воєнний стан*

Критична інформаційна інфраструктура неодноразово була предметом досліджень вітчизняних науковців як самостійний предмет, так і в межах досліджень критичної інфраструктури в цілому. В різні темпоральні періоди окремі аспекти кібербезпеки досліджували О. В. Грищенко, Д. О. Грищенко, К. Е. Чукалов [1], О. П. Єрменчук [2], А. В. Омельченко [3]. Тож, є підстави констатувати систематичну увагу з боку науковців до проблематики, що стосується критичної інформаційної інфраструктури.

Зміст терміну «критична інформаційна інфраструктура» визначався як «сукупність об'єктів критичної інформаційної інфраструктури» у пункті 2 Порядку формування об'єктів критичної інформаційної інфраструктури, затвердженого Постановою Кабінету Міністрів України від 09.10.2020 № 943 [4]. Проте зміст пункту 2 зазначеного Порядку було змінено Постановою Кабінету Міністрів України від 28.03.2025 № 447 [5] на бланкетну норму, яка відсилає до дефініційних норм законів України «Про електронні комунікації», «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України» та «Про критичну інфраструктуру».

В той же час лише в Законі України «Про основні засади забезпечення кібербезпеки України» міститься визначення терміну «критична інформаційна інфраструктура» [6], яке дублює зміст визначення, що містилось у Порядку формування об'єктів критичної інформаційної інфраструктури. При цьому пункт 19 частини 1 статті 1 зазначеного Закону визначає зміст терміну «об'єкт критичної інформаційної інфраструктури», під яким розуміється «інформаційна, електронна, комунікаційна, інформативно-комунікаційна або технологічна система, яка необхідна для стійкого та безперервного функціонування об'єкта критичної інфраструктури, істотно впливає на безперервність та стійкість процесу надання життєво важливих функцій та/або послуг та відсутній альтернативний об'єкт (спосіб) їх надання» [6]. На підставі вищенаведеного визначення можна дійти висновку, що критична інформаційна інфраструктура включає в себе сукупність систем (інформаційну, електронну, комунікаційну, інформаційно-комунікаційну або технологічну), які забезпечують функціонування об'єкта критичної інфраструктури в цілому або впливають на безперервність та стійкість надання життєво важливих функцій та/або послуг таким об'єктом критичної інфраструктури.

Життєво важливі функції та/або послуги визначені статтею 1 Закону України «Про критичну інфраструктуру»: це - функції та/або послуги, реалізація яких забезпечується органами державної влади, органами місцевого самоврядування, установами, суб'єктами господарювання та організаціями будь-якої форми власності, збої,

переривання та порушення надання яких призводять до швидких негативних наслідків для національної безпеки [7]. З аналізу наведеного визначення вбачаються підстави констатувати про причинно-наслідковий зв'язок між порушенням безперебійного (безперервного) функціонування перелічених суб'єктів щодо надання життєво важливих функцій та/або послуг і негативними наслідками, які кваліфікуються як загрози національній безпеці України, адже за визначенням статті 1 Закону України «Про національну безпеку України» до них належать «явища, тенденції та чинники, що унеможливлюють чи ускладнюють реалізацію національних інтересів та збереження національних цінностей України» [8].

Серед заходів, які спрямовані на захист інформації та в своїй сукупності визначаються як «кіберзахист» відповідно до статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» [6], вирізняються такі види:

1) організаційні заходи захисту інформації – заходи, які повинні здійснювати посадові особи в процесі створення та експлуатації системи для забезпечення захисту інформації (наприклад, обмеження доступу до приміщень, де створюється та обробляється інформація; зберігання носіїв інформації; заходи з відбору персоналу);

2) правові заходи захисту інформації – полягають у створенні, розробці нормативно-правового забезпечення (сукупності нормативно-правових актів), яким закріплюються права і свободи, регулюється порядок захисту інформації, передбачається кваліфікація правопорушень у сфері інформаційної безпеки та види юридичної відповідальності за їх вчинення);

3) заходи інженерно-технічного захисту інформації - сукупність спеціальних технічних засобів та їх використання для захисту інформації;

4) заходи криптографічного захисту інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо (частина 1 статті 1 Закону України «Про захист інформації в інформаційно-комунікаційних системах» [9]);

5) заходи технічного захисту інформації – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації (частина 1 статті 1 Закону України «Про захист інформації в інформаційно-комунікаційних системах» [9]).

Підсумовуючи викладене вище, слід зауважити, що наразі нормативно-правове забезпечення захисту критичної інформаційної інфраструктури перебуває в стані системного оновлення та внесення змін, які обґрунтовані як внутрішніми факторами, так і зовнішніми загрозами.

**Бібліографічні посилання**

1. Грищенко О. В., Грищенко Д. О., Чукалов К. Е. Кібербезпека критичної інформаційної інфраструктури. Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України: матеріали Науково-практичної конференції (Львів, 22 грудня 2023) / упорядник: Т. В. Магеровська. – Львів : ЛьвДУВС, 2024. С. 43-45. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/6900/1/22_12_2023.pdf#page=43 (дата звернення: 10.05.2025).

2. Єрменчук О. П. Стан нормативно-правового регулювання захисту об'єктів критичної інфраструктури в кіберсфері як складник забезпечення національної безпеки. Правові новели. 2019. № 7. С. 95-101. URL: http://legalnovels.in.ua/journal/7_2019/7_2019.pdf#page=95 (дата звернення: 10.05.2025).

3. А. В. Омельченко. Організаційно-правові засади забезпечення кібербезпеки України. Київський часопис права. № 3. 2022. С. 140-145. DOI: https://doi.org/10.32782/klj/2021.3.22 (дата звернення: 10.05.2025).

4. Деякі питання об'єктів критичної інформаційної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#n16 (дата звернення: 10.05.2025).

5. Про внесення змін щодо кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури до деяких постанов Кабінету Міністрів України : Постанова Кабінету Міністрів України від 28.03.2025 № 447. URL: https://zakon.rada.gov.ua/laws/show/447-2025-%D0%BF#n40 (дата звернення: 10.05.2025).

6. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#n3 (дата звернення: 11.05.2025).

7. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 11.05.2025).

8. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#n7 (дата звернення: 11.05.2025).

9. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#n61 (дата звернення: 11.05.2025).

**B.Bogdan**

Regulatory and legal principles of protection of critical information infrastructure.

**Abstract:** Critical information infrastructure for a

long time is in the focus of attention of the state as a whole, since especially during the imposed martial law on the territory of Ukraine it is an object to which significant damage is caused by enemy forces. State institutions should contribute to ensuring the proper protection of critical information infrastructure through a set of organizational, regulatory, engineering and other measures to ensure the security of critical information infrastructure facilities. Currently, there is no comprehensive list of measures that should protect critical information infrastructure. The purpose of this study is to analyze the legal and regulatory framework, on the basis of which the state is to ensure the protection of critical information infrastructure.

**Keywords:** protection, critical infrastructure, security, information, cybersecurity, martial law

**Зразок для цитування:**

Богдан Б. Нормативно-правові засади захисту критичної інформаційної інфраструктури. Пропілеї права та безпеки, 2025. №6-7. С. 35-37. DOI: https://doi.org/10.32620/pls.2025.67.06.