Сергій БЄЛАЙ,
доктор наук з державного управління, професор
начальник центру організації та координації наукової та інноваційної діяльності
Національної академії Національної гвардії України
м. Харків, Україна
ORCID: https://orcid.org/0000-0002-0841-9522
e-mail: belwz3@ukr.net

Іван ЛАВРОВ,
ад'юнкт докторантури та ад'юнктури
Національної академії Національної гвардії України
м. Харків, Україна
ORCID: https://orcid.org/0009-0005-0706-3711
e-mail: johnapleased417@gmail.com

DOI: https://doi.org/10.32620/pls.2025.8.46

ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ЗАСАДИ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація: *У роботі обґрунтовано правові та організаційні засади кібербезпеки об'єктів критичної інфраструктури в умовах збройної агресії та кібервійни. Показано логіку інтеграції дефінітивного та інституційного каркасу з уніфікованими процедурами планування, реагування, відновлення та регулярною оцінкою результативності. Наголошено на ролі міжвідомчої сумісності, стандартизованої комунікації, документування й підзвітності. Сформульовано механізм координації із контррозвідувальним компонентом, що зменшує регуляторну невизначеність, прискорює погодження рішень і переводить взаємодію від ситуативних домовленостей до вимірюваного управлінського процесу. Практичне значення полягає у створенні підґрунтя для стандартизації планово-управлінських документів та оптимізації процедур забезпечення безперервного надання суспільно важливих послуг.*

Ключові слова: *критична інфраструктура, кібербезпека, сектор безпеки і оборони.*

Під час повномасштабної агресії РФ кібератаки системно спрямовуються на державні інформаційні ресурси та об'єкти критичної інфраструктури (ОКІ), що висуває на перший план питання правової керованості захисту й швидкого відновлення функцій, які є суспільно значущими. Наукові джерела фіксують зростання масштабів і комплексності загроз, а також необхідність посилення спроможностей сектору безпеки і оборони та органів виконавчої влади діяти на випередження, особливо в умовах кібервійни [1]. Саме в цьому контексті Стратегія кібербезпеки України визначає кібербезпеку одним із пріоритетів національної безпеки та окреслює засади державної політики, релевантні для захисту ОКІ [2].

У цих умовах постає потреба у цілісній адміністративно-правовій рамці кіберзахисту ОКІ, що поєднує дефінітивний та інституційний каркас із процедурними механізмами керованості: чітке визначення статусу об'єктів і відповідальних суб'єктів, прозорі правила взаємодії та комунікації, стандартизовані процеси планування, реагування й відновлення, а також повторювані цикли оцінювання результативності. Така рамка забезпечує узгоджені рішення органів влади й операторів, зменшує регуляторну невизначеність і переводить політику кібербезпеки з декларативної площини у практику управлінського виконання та контролю.

Нормативне ядро становить Закон України «Про критичну інфраструктуру», який визначає понятійний апарат, визначає коло суб'єктів, принципи публічної політики у сфері критичної інфраструктури та розмежовує повноваження між органами державної влади, операторами та іншими учасниками [3].

Процедуризація державної політики реалізується через Положення про організаційно-технічну модель кіберзахисту [4]. Документ інституалізує взаємодію учасників системи кіберзахисту, уніфікує ролі, канали обміну та кризові процедури, що критично важливо для ОКІ у воєнний час. У поєднанні з науковими

напрацюваннями це забезпечує передбачуваність поведінки суб'єктів і підвищує ефективність міжвідомчої координації [4].

Уніфікацію вимог до суб'єктів забезпечують «Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури», які встановлюють організаційно-методологічні, технічні й технологічні умови захисту, а також базові підходи до оцінювання ризиків, документування, повідомлення про інциденти та відновлення [5].

Ключовим інструментом управління якістю є періодичні огляди стану кіберзахисту критичної інформаційної інфраструктури та державних інформаційних ресурсів, що забезпечують замкнений цикл «оцінка — коригувальні дії — повторна оцінка» [6]. Їх практична доцільність, зокрема для стратегічних секторів, спеціально акцентована в наукових публікаціях [1].

Важливим елементом адміністративно-правової архітектури є контррозвідувальний компонент: спеціально уповноважений орган безпеки виконує превентивні, виявлювальні та координаційні функції у протидії загрозам ОКІ, включно з деструктивним інформаційним впливом. Водночас на оператора покладаються передбачувані обов'язки повідомлення, взаємодії та виконання секторальних процедур [1]. Така конфігурація спрямована на зменшення операційних розривів під час інцидентів і забезпечення узгодженого реагування на багатофакторні події.

У підсумку синхронізація законодавчого визначення статусу ОКІ, організаційно-технічної моделі, уніфікованих (і секторально деталізованих) вимог і циклічних оглядів створює доказову модель публічного управління кіберзахистом. Правила перетворюються на стандартизовані процедури, а міжвідомча взаємодія – на відтворюваний управлінський цикл. Така модель, посилена контррозвідувальною складовою, мінімізує вразливості критично важливих процесів і забезпечує безперервне надання суспільно важливих послуг навіть за умов ескалації загроз

Бібліографічні посилання

1. Мануілов Я.С. Забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах кібервійни. Інформація і право. 2023. № 1. С. 154-167.

2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 22.10.2025).

3. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX : станом на 21 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 21.10.2025).

4. Про затвердження Положення про організаційно-технічну модель кіберзахисту : Постанова Каб. Міністрів України від 29.12.2021 № 1426 : станом на 26 груд. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-п#Text (дата звернення: 22.10.2025).

5. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Каб. Міністрів України від 19.06.2019 № 518 : станом на 7 верес. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text (дата звернення: 22.10.2025).

6. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом : Постанова Каб. Міністрів України від 11.11.2020 № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-п#Text (дата звернення: 22.10.2025).

S. Belay, I. Lavrov

Legal and organizational foundations of cybersecurity for critical infrastructure facilities.

Abstract: The paper substantiates the legal and organizational foundations of cybersecurity for critical infrastructure facilities under conditions of armed aggression and cyber warfare. It demonstrates the integration of a definitional and institutional framework with standardised procedures for planning, response, recovery, and regular performance evaluation. Emphasis is placed on interagency interoperability, standardised communication, documentation, and accountability. A coordination mechanism incorporating a counterintelligence component is proposed, which reduces regulatory uncertainty, accelerates decision alignment, and shifts cooperation from ad hoc arrangements to a measurable management process. The practical contribution lies in providing a basis for the standardisation of planning-and-management documents and the optimisation of procedures ensuring the uninterrupted delivery of essential public services.

Keywords: critical infrastructure, cybersecurity, security and defence sector.

Зразок для цитування:

Бєлай С., Лавров І. Правові та організаційні засади кібербезпеки об'єктів критичної інфраструктури. Пропілеї права та безпеки, 2025. №8. С. 192-193. DOI: https://doi.org/10.32620/pls.2025.8.46.