Національний університет цивільного захисту України
Національна академія Національної гвардії України
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького
Національна академія внутрішніх справ
Навчально-науковий інститут права та правоохоронної діяльності
Львівського державного університету внутрішніх справ
Одеський державний університет внутрішніх справ
Черкаська медична академія

Навчально-науковий інститут цивільного захисту
Кафедра управління у сфері цивільного захисту

Організаційно-управлінське та економіко-правове забезпечення діяльності Єдиної державної системи цивільного захисту (ЄДСЦЗ)

Матеріали
X Всеукраїнської науково-практичної конференції

31 жовтня 2025 року

Черкаси

УДК 365.13:658
О 64

Рекомендовано до друку вченою радою
навчально-наукового інституту цивільного захисту
Національного університету цивільного захисту України
(протокол № 2 від 24 жовтня 2025 року)

Дозволяється публікація матеріалів збірника у відкритому
доступі комісією з питань роботи із службовою інформацією
у Національному університеті цивільного захисту України
(протокол № 5 від 20 жовтня 2025 року)

О 64 **Організаційно-управлінське** та економіко-правове забезпечення діяльності Єдиної державної системи цивільного захисту (ЄДСЦЗ): Матеріали X Всеукр. наук.-практ. конф., м. Черкаси НУЦЗ України – К : 7БЦ, 2025. – 351 с.
ISBN 978-617-549-322-9

У публікаціях досліджуються: організаційно-управлінські засади функціонування ЄДСЦЗ; нормативно-правове регулювання діяльності ЄДСЦЗ; соціальне-економічне забезпечення діяльності ЄДСЦЗ; особливості організації та реалізації заходів цивільного захисту в умовах воєнного стану; соціальна реабілітація та медичне забезпечення в умовах воєнного стану; організаційно-правові основи антитерористичної безпеки держави; інноваційні технології та інформаційне забезпечення діяльності ЄДСЦЗ; організаційно-правові засади забезпечення безпеки та стійкості об’єктів критичної інфраструктури України в умовах ведення воєнних дій; міжнародне співробітництво та інтеграційні процеси у сфері цивільного захисту.

УДК 365.13:658

ISBN 978-617-549-322-9

Організаційно-правові засади захисту КІ України адаптовані до умов війни, з акцентом на кібербезпеку та швидке відновлення. Вони забезпечують стійкість через централізовану координацію, міжнародну співпрацю та сучасні технології, але потребують додаткових ресурсів і кадрів для повної реалізації. Система є основою для протидії сучасним загрозам і відновлення інфраструктури після війни.

СПИСОК ЛІТЕРАТУРИ

1. Аналіз закону від Мінрегіону (серпень 2025) Посилання: mviskarada.gov.ua/news/item/4533-zakon-4321ix-tse-pro-rozvytok-z-urakhuvanniam-interesiv-kozhnoho-meshkantsia.

2. NATO CCDCOE: Ukraine's Critical Infrastructure Protection (2024) Посилання: ccdcoe.org/news/2024/ukraines-critical-infrastructure-protection-lessons-learned/ Опис: Аналіз співпраці з НАТО, обмін розвідданими для захисту КІ.

3. OSCE: Protection of Critical Infrastructure in Ukraine (2025) Посилання: osce.org/files/f/documents/8/9/562345.pdf.

АНАЛІЗ ОРГАНІЗАЦІЙНО-ПРАВОВИХ ЗАСАД ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ФУНКЦІОНУВАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Аліна ПОМАЗА-ПОНОМАРЕНКО, д-р. держ. упр., старший дослідник,
Національний університет цивільного захисту України
Дмитро ТАРАДУДА, канд. техн.наук, доц.,
Львівський державний університет безпеки життєдіяльності

Забезпечення безпеки та стійкості об'єктів критичної інфраструктури є одним із ключових завдань національної безпеки України, особливо в умовах повномасштабної воєнної агресії. Пошкодження чи виведення з ладу енергетичних, транспортних, водопровідних, медичних та інформаційних систем має не лише економічні, але й соціально-політичні наслідки, що підсилюють руйнівний ефект воєнних дій. Тому розробка та впровадження дієвих організаційно-правових механізмів захисту об'єктів критичної інфраструктури (далі – КІ) є пріоритетом державної політики.

Основним нормативно-правовим актом, що закладає правові та організаційні засади формування національної системи захисту критичної інфраструктури, є Закон України «Про критичну інфраструктуру» (набув чинності у 2021 р.) [1]. Цей закон визначає поняття «критична інфраструктура», регламентує принципи категоризації об'єктів, встановлює повноваження уповноважених та секторальних органів у сфері захисту КІ та закладає правові підстави для створення реєстру об'єктів критичної інфраструктури. Законодавство України

Паралельно з цим державні інструменти деталізуються в нормативних актах Кабінету Міністрів (наприклад, порядок ведення реєстру об'єктів КІ, порядок взаємодії секторальних органів), а також у Національному плані захисту та забезпечення безпеки і стійкості КІ, затвердженому Кабінетом Міністрів України (Національний план визначає стратегічні цілі, заходи та відповідальних виконавців).

У контексті воєнних дій важливим правовим інструментом є законодавство щодо основ національного спротиву та територіальної оборони, яке встановлює додаткові обов'язки для суб'єктів захисту та взаємодію цивільних і оборонних структур у кризовий період. Закон «Про основи національного спротиву» [1] закладає механізми мобілізації ресурсів та широку кооперацію з громадянським суспільством.

Останніми роками законодавство активно оновлюється: уряд вносить зміни до процедур категоризації, складення секторних переліків та взаємодії органів, що

відображено в низці постанов та змін до підзаконних актів (зокрема, зміни 2024–2025 рр. щодо уточнення повноважень та процедур). Це свідчить про прагнення держави адаптувати регулювання до реалій військового часу.

На практиці національна система захисту КІ будується як багатоступенева мережа співпраці між державними органами, операторами інфраструктури та місцевими органами влади. У рамках чинного законодавства виділяється кілька ключових інституційних елементів системи забезпечення стійкого функціонування КІ, а саме:

1. Уповноважений орган у сфері захисту КІ, який координує формування політики, контролює виконання заходів та взаємодіє з секторальними органами. До речі, уУповноваженим органом визнано Держспецзв'язку, за яким свого часу було закріплено повноваження щодо ведення реєстру об'єктів КІ (сектор кібер- та інфобезпеки).

2. Секторальні органи відповідають за визначення секторних переліків об'єктів, проведення категоризації та реалізацію секторних заходів захисту (наприклад, енергетика, транспорт, охорона здоров'я тощо). Нещодавні зміни підкреслюють обов'язок секторальних органів оперативно подавати оновлені переліки.

3. Оператори критичної інфраструктури – власники/управлінці об'єктів КІ, які зобов'язані впроваджувати заходи безпеки, здійснювати сповіщення та взаємодіяти з компетентними органами.

4. Місцеві органи самоврядування, які відповідають за забезпечення безпеки на територіях та координацію локальної стійкості інфраструктури.

Окремий блок інституційного забезпечення стійкості функціонування об'єктів КІ представлений реєстром таких об'єктів. Він ведеться відповідно до встановленого порядку, має стати джерелом для планування захисних заходів, пріоритезації ресурсів та швидкого прийняття рішень у разі ударів по інфраструктурі. Як відомо, постанови КМУ та дотичні правові акти деталізують процедуру включення об'єктів КІ до реєстру та механізми категоризації.

Щодо особливостей забезпечення безпеки КІ в умовах воєнних дій, то воєнний стан висуває додаткові вимоги до забезпечення стійкості КІ, а саме:

1. Пріоритезація та категоризація. В умовах обмежених ресурсів необхідно чітко визначити критичні об'єкти, які забезпечують життєдіяльність населення (енергетика, водопостачання, медицина, транспорт, телекомунікації тощо). Чинне законодавство України закладає принципи пріоритезації, що мають враховувати операційну важливість об'єкта для національної безпеки [1].

2. Оперативне управління ризиками. Під час воєнних дій потрібні швидкі процедури прийняття рішень, які дозволяють переорієнтувати ресурси, ввести тимчасові регламенти та мобілізувати персонал. Законодавче визначення можливості повторної категоризації та ініціювання перевірок секторальними органами сприяє гнучкості у відповідь на динамічну ситуацію.

3. Міжвідомча координація. Ефективний захист КІ вимагає скоординованих дій між оборонними структурами, ДСНС, органами місцевої влади й операторами. Чинне законодавство України підкреслює необхідність створення координаційних механізмів та процедур оперативного обміну інформацією.

4. Резервування та диверсифікація ресурсів. Передбачається забезпечення резервних потужностей, альтернативних маршрутів постачання та запасів матеріалів, що дозволяє мінімізувати наслідки руйнувань. Частина заходів належить до компетенції операторів КІ; держава має сприяти плануванню та фінансуванню таких заходів у мирний час.

5. Захист інформаційної та кіберінфраструктури. Ворожі засоби впливу на ІТ-системи можуть паралізувати управління критично важливими послугами; тому інтеграція заходів кібербезпеки у плани захисту КІ є обов'язковою. Хоча питання

кіберзахисту регулюється і окремими актами, взаємодія з секторною політикою КІ є необхідною складовою.

На підставі аналізу пропонується низка практичних заходів щодо вдосконалення організаційно-правових засад щодо забезпечення стійкості функціонування КІ, а саме:

1. Уніфікація й оперативне оновлення підзаконних актів [4]. Необхідно забезпечити механізм швидкого внесення змін до порядків та регламентів у разі зміни обстановки (особливо в період воєнних дій), а також стандартизувати формати взаємодії між секторальними органами. (Реалізація цього заходу можлива через відповідні постанови КМУ та накази уповноваженого органу).

2. Розробка фінансових інструментів із підтримки заходів стійкості функціонування КІ. Держава має передбачити програми субсидування чи часткового відшкодування витрат операторів КІ на відновлення об'єктів КІ, резервування, модернізацію та захисні заходи [2]; а також можливе залучення міжнародної допомоги та кредитних інституцій. У цьому контексті пропонується включити до Національного плану дій окремий розділ фінансування операторів КІ. Реалізацію цього заходу доречно покласти на Кабінет Міністрів України.

3. Посилення міжвідомчої координації та створення оперативних штабів. Для швидкої реагування в бойових умовах необхідні спільні міжвідомчі штаби з чітко визначеними повноваженнями, процедурами обміну інформацією та повноваженнями на переорієнтацію ресурсів.

4. Інтеграція кіберзахисту в стратегію захисту КІ. Забезпечити обов'язковість проведення оцінок кіберризиків операторів КІ, впровадження стандартів і тренінгів, а також налагодження швидких каналів реагування на кіберінциденти. Реалізацію цього заходу доречно покласти на Кабінет Міністрів України.

5. Правова регламентація співпраці з приватним сектором, який володіє значною частиною об'єктів КІ в Україні. Слід активніше розвивати механізми публічно-приватного партнерства, захищені процедури обміну інформацією та стимули для приватних операторів КІ до інвестування у стійкість [3].

6. Запровадження регулярних навчань і перевірок стійкості об'єктів КІ. Секторальні тренування, спільні навчання з місцевими адміністраціями та операторами мають стати обов'язковими, з метою відпрацювання сценаріїв відновлення функціонування критичних послуг.

Отже, правове та організаційне забезпечення (що оформлюється в інституційний механізм) у сфері захисту критичної інфраструктури в Україні має достатньо міцну нормативну основу, закладену Законом України «Про критичну інфраструктуру» та супровідними актами вітчизняного уряду. Проте практичне забезпечення стійкості у воєнних умовах висуває нові вимоги щодо оперативності оновлення процедур, гнучкості категоризації, фінансування та координації між органами публічної влади та операторами критичної інфраструктури. Виконання запропонованих заходів передбачає уніфікацію чинних правових норм, у т.ч. у напрямку підвищення фінансової підтримки операторів КІ, створення оперативних механізмів координації, публічно-приватного партнерства, інтеграції кіберзахисту й активізації співпраці з приватним сектором. Усе це покликано сприяти підвищенню готовності та стійкості функціонування КІ України в умовах сучасних воєнних загроз.

СПИСОК ЛІТЕРАТУРИ

1. Законодавство // Офіційний веб-сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws.

2. Помаза-Пономаренко А. Л. Збитки, нанесені бойовими діями об'єктам критичної інфраструктури в україні: механізми оцінювання та відновлення // Успіхи і досягнення в науці. 2025. Вип. 1 (1). С. 601 – 61.

3. Помаза-Пономаренко А. Л., Тарадуда Д. В. Забезпечення стійкості системи державного регулювання об'єктів підвищеної небезпеки // Державне управління:

удосконалення та розвиток. 2024. № 4. URL: https://www.nayka.com.ua/index.php/dy/article/view/3461.

4. Помаза-Пономаренко А. Л., Тарадуда Д. В. Перспективи розвитку публічного адміністрування як критичної інфраструктури // Матеріали XI Міжнародної науково-практичної он-лайн конференції «Стан та перспективи розвитку адміністративного права України» (24.10.2024, м. Одеса). С. 131 – 133.

5. Помаза-Пономаренко А. Л., Тарадуда Д. В. Управлінські підходи до попередження надзвичайних ситуацій на об’єктах критичної інфраструктури та підвищеної небезпеки // Державне управління: удосконалення та розвиток. 2025. № 1. URL: https://www.nayka.com.ua/index.php/dy/article/view/5502/5557.

ІНСТИТУЦІЙНА СПРОМОЖНІСТЬ РЕАЛІЗАЦІЇ ППП-ПРОЄКТІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Марина ПОРОКА, аспірант,
Національний університет цивільного захисту України
НК – Світлана ДОМБРОВСЬКА, д-р. держ. упр., проф.,
Національний університет цивільного захисту України

Масштабні руйнування критичної інфраструктури України внаслідок російської агресії актуалізують питання пошуку ефективних механізмів її відновлення та забезпечення стійкості [1]. Публічно-приватне партнерство (ППП) розглядається як один із ключових інструментів залучення приватних інвестицій та експертизи до процесів відбудови [2]. Однак успішність реалізації ППП-проєктів у сфері критичної інфраструктури безпосередньо залежить від спроможності інституційного середовища, яке формують органи публічної влади, спеціалізовані агенції та координаційні структури. В умовах воєнного стану та постійних трансформацій системи публічного управління питання діагностики інституційної спроможності набуває особливого значення для забезпечення ефективності використання обмежених ресурсів та створення передумов для масштабного залучення приватного сектору до відновлення стратегічно важливих об'єктів.

Інституційна архітектура публічно-приватного партнерства в Україні характеризується фрагментарністю повноважень та відсутністю єдиного координаційного центру [3]. На центральному рівні функції розподілені між Міністерством економіки України, Міністерством розвитку громад, територій та інфраструктури, галузевими міністерствами та Фондом державного майна. Відсутність спеціалізованого агентства з ППП, яке б концентрувало експертизу, методологічну підтримку та координацію проєктів, призводить до дублювання функцій, неузгодженості дій та зниження ефективності підготовки і реалізації проєктів. На місцевому рівні органи самоврядування часто не мають достатніх кадрових та фінансових ресурсів для якісної підготовки ППП-проєктів, що особливо критично для об'єктів критичної інфраструктури комунального підпорядкування.

Виявлена фрагментація інституційної системи безпосередньо впливає на управлінську спроможність реалізації ППП-проєктів. Ця спроможність проявляється через кілька ключових аспектів. По-перше, кадрова складова демонструє дефіцит фахівців з досвідом структурування складних інфраструктурних проєктів, фінансового моделювання та управління контрактами ППП. По-друге, методологічне забезпечення є недостатнім – відсутні адаптовані до умов воєнного стану методики оцінки доцільності ППП для об'єктів критичної інфраструктури, розподілу ризиків та визначення ціни за гроші. По-третє, координаційні механізми між різними рівнями влади та між