

УДК 351.81

DOI <https://doi.org/10.32850/LB2414-4207.2022.27.08>

## **АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ ПІД ЧАС ВОЄННОГО СТАНУ**

**Кузьменко Юлія Василівна**,  
[orcid.org/0000-0001-8151-1686](https://orcid.org/0000-0001-8151-1686)  
доктор педагогічних наук, доцент,  
професор кафедри адміністративного  
права та адміністративного процесу  
(Херсонський факультет  
Одеського державного університету  
внутрішніх справ,  
м. Херсон, Україна)

**Коропатов Олег Миколайович**,  
[orcid.org/0000-0001-6027-3391](https://orcid.org/0000-0001-6027-3391)  
кандидат юридичних наук, доцент,  
завідувач кафедри адміністративного  
права та адміністративного процесу  
(Херсонський факультет  
Одеського державного університету  
внутрішніх справ,  
м. Херсон, Україна)

**Думанський Роман Вікторович**,  
викладач кафедри адміністративного  
права та адміністративного процесу  
(Херсонський факультет  
Одеського державного університету  
внутрішніх справ,  
м. Херсон, Україна)

У статті розкриваються особливості адміністративно-правового забезпечення захисту об'єктів критичної інфраструктури України в умовах воєнного стану. Авторами статті аналізується національне законодавство щодо особливостей захисту та правового режиму роботи та безпеки критичної інфраструктури в умовах особливого періоду, а воєнний стан належить до таких. Підкреслюється актуальність цього питання як базового у процесі створення продуктивних механізмів у сфері забезпечення інтересів національної безпеки нашої держави. Вказується, що у період ведення військових дій російськими окупаційними військами на території України було внесено зміни до нормативних актів спеціалізованого змісту, які розкривають механізм врегулювання ситуацій у разі пошкодження, ліквідації чи нейтралізації пошкоджень стосовно певних категорій об'єктів критичної інфраструктури. Констатується, що всі ці кроки підкреслюють спрямованість державної політики України на захист, своєчасне реагування на загрози критичній інфраструктурі країни від бойових дій, диверсій, терористичних актів, спричинених військовою агресією, для чого необхідна різногалузева консолідація

ресурсів. Серед основних загроз за серйозністю наслідків для критичної інфраструктури називаються кібератаки, терористичні та диверсійні акти, військові операції. Стверджується, що все це призводить до виникнення аварій на об'єктах підвищеної небезпеки, як наслідок, це може привести до виникнення надзвичайних ситуацій регіонального, державного або світового рівня. Визначається, що на сьогодні гостро стоять проблеми фінансового і матеріально-технічного забезпечення тих об'єктів критичної інфраструктури, які постраждали внаслідок військових дій.

**Ключові слова:** критична інфраструктура, система захисту критичної інфраструктури, об'єкти підвищеної небезпеки, військовий стан, нормативно-правова база.

## ADMINISTRATIVE AND LEGAL ENSURING THE PROTECTION OF CRITICAL INFRASTRUCTURE OBJECTS IN UKRAINE DURING MARITAL STATE

**Kuzmenko Iuliia Vasylivna,**  
orcid.org/0000-0001-8151-1686  
PhD, Assistant Professor,  
Professor at the Department of  
Administrative Law and Administrative  
Procedure  
(Kherson Faculty of Odessa State  
University of Internal Affairs, Kherson,  
Ukraine)

**Koropatov Oleh Mykolayovych,**  
orcid.org/0000-0001-6027-3391  
PhD, Assistant Professor,  
Head of the Department of Administrative  
Law and Administrative Procedure  
(Kherson Faculty of Odessa State  
University of Internal Affairs, Kherson,  
Ukraine)

**Dumanskyi Roman Viktorovich,**  
Lecturer at the Department of  
Administrative Law  
and Administrative Procedure  
(Kherson Faculty of Odesa State  
University of Internal Affairs, Kherson,  
Ukraine)

The article reveals the peculiarities of the administrative and legal support for the protection of critical infrastructure objects of Ukraine under martial law. The authors of the article analyze the national legislation regarding the specifics of the protection and legal regime of operation and safety of critical infrastructure in the conditions of a special period, and martial law is one of them. The relevance of this issue is emphasized as a basic one in the process of creating productive mechanisms in the sphere of ensuring the national security interests of our state. It is indicated that during the period of military operations by the Russian occupying forces on the territory of Ukraine, changes were made to the normative acts of specialized content, which reveal the mechanism of settlement

of situations in the event of damage, liquidation or neutralization of damage in relation to certain categories of critical infrastructure objects. It is noted that all these steps emphasize the focus of Ukraine's state policy on protection, timely response to threats to the country's critical infrastructure from hostilities, sabotage, terrorist acts caused by military aggression, for which multi-sectoral consolidation of resources is necessary. Among the main threats, in order of seriousness of consequences, for critical infrastructure are cyber attacks, terrorist and sabotage acts, military operations. It is claimed that all this leads to accidents at high-risk facilities, which, as a result, can lead to regional, national or global emergencies. It is determined that today there are acute problems of financial and logistical support of those critical infrastructure objects that have suffered as a result of military operations.

**Key words:** critical infrastructure, critical infrastructure protection system, high-risk facilities, martial law, legal framework.

**Постановка проблеми та її актуальність.** В умовах повномасштабної війни України з російським агресором набувають усе більшого «обговорення та дій щодо протидії злочинам у різних сферах життя» [4, с. 12], в тому числі й військових правопорушень. Нарощення рівня небезпеки для функціонування критичної інфраструктури вимагає правового регулювання з метою забезпечення їх правового визнання, охорони, протидії злочинним проявам, знищенню чи часткового пошкодження, збоїв сталого функціонування цих об'єктів, визначення юридичної відповідальності за такий вид правопорушень. Цілком логічно, що під час бомбардувань знищення, часткове пошкодження чи збій у роботі об'єктів критичної інфраструктури напряму впливає на рівень національної безпеки кожної держави. Під час воєнного стану ці фактори лише посилюються. З 24 лютого 2022 р. відповідно до Закону України «Про правовий статус воєнного стану» в Україні введено режим воєнного стану, а за Указом Президента України від 12 серпня 2022 року № № 573/2022 «Про продовження строку дії воєнного стану в Україні» його строк дії з 23 серпня 2022 р. подовжено на 90 діб.

**Аналіз останніх досліджень і публікацій.** Питання безпеки окремих елементів критичної інфраструктури знайшли своє відображення в науковому доробку вітчизняних учених, таких як: Д. Бірюков, Д. Бобра, О. Верголяс, В. Заплатинський, С. Кондратов, В. Лойко І. Урядникова, С. Іванюта, О. Суходолі, С. Теленик, В. Храпкіна, А. Чорноус та ін.

**Мета статті** – розкрити особливості адміністративно-правового забезпечення захисту об'єктів критичної інфраструктури України під час воєнного стану.

**Виклад основного матеріалу.** Аналіз національного законодавства щодо особливостей захисту та правового режиму роботи та безпеки критичної інфраструктури в умовах особливого періоду, а воєнний стан належить до таких, показав, що на сьогодні ці питання врегульовано такими законами України: «Про критичну інфраструктуру», «Про внесення змін до деяких законодавчих актів України щодо засад державної регіональної політики та політики відновлення регіонів і територій», «Про правовий режим воєнного стану», «Про функціонування єдиної транспортної системи України в особливий період», «Про оборону України», «Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України», «Про державну таємницю», «Про місцеве самоврядування в Україні», «Про місцеві державні адміністрації», «Про основні засади забезпечення кібербезпеки України», «Про національну безпеку України».

У Законі України «Про критичну інфраструктуру» визначено: «безпека критичної інфраструктури – стан захищеності критичної інфраструктури, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність

і стійкість критичної інфраструктури» [9]. Аналіз змісту цього Закону дає підстави стверджувати, що в ньому регламентовано основні засади утворення системи захисту об'єктів критичної інфраструктури та забезпечення ефективності її функціонування, в тому числі й період військового стану. Зокрема, окреслено: завдання державної політики у цій сфері; рівні управління такою національною системою; категорії критичності об'єктів критичної інфраструктури; реєстр об'єктів критичної інфраструктури; паспортизація об'єктів критичної інфраструктури; суб'єкти національної системи захисту критичної інфраструктури; режими функціонування національної системи захисту критичної інфраструктури; уповноважений орган у сфері захисту критичної інфраструктури України; функціональні органи у сфері захисту критичної інфраструктури; секторальні органи у сфері захисту критичної інфраструктури; місцеві органи виконавчої влади (військово-цивільні адміністрації у разі утворення) у сфері захисту критичної інфраструктури; завдання, права та обов'язки операторів критичної інфраструктури; моніторинг рівня безпеки об'єктів критичної інфраструктури; взаємодія національної системи захисту критичної інфраструктури з іншими системами захисту у сфері національної безпеки; державно-приватне партнерство у сфері захисту критичної інфраструктури; парламентський контроль у сфері захисту критичної інфраструктури; громадський нагляд у сфері захисту критичної інфраструктури; відповідальність за порушення законодавства у сфері захисту критичної інфраструктури; міжнародне співробітництво у сфері захисту критичної інфраструктури.

Із введенням військового стану були внесені зміни до нормативних актів спеціалізованого змісту, які розкривають механізм врегулювання ситуації стосовно певних категорій об'єктів критичної інфраструктури. Зокрема, відбулася редакція таких документів, як:

– Постанова КМУ «Деякі питання об'єктів критичної інфраструктури», де було окреслено «Порядок формування переліку об'єктів критичної інформаційної інфраструктури», «Порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування» [2];

– Постанова КМУ «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», що доповнено Переліком базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури [6];

– Постанова КМУ «Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури», де представлено Акт оцінки стану захищеності об'єкта критичної інфраструктури [8];

– розпорядження КМУ «Про схвалення Концепції створення державної системи захисту критичної інфраструктури» зумовило актуалізацію стратегічного підходу до «питання захисту систем, об'єктів і ресурсів, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки» [10];

– Постанова КМУ «Деякі питання ідентифікації об'єктів підвищеної небезпеки», де представлено Порядок ідентифікації об'єктів підвищеної небезпеки та ведення їх обліку, а також започатковано роботу над Державним електронним реєстром об'єктів підвищеної небезпеки [1];

– Постанова Правління НБУ «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України», де надано перелік об'єктів критичної інфраструктури в банківській системі [7];

- Постанова КМУ «Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України», набирає своєї чинності та відповідно регулює механізм утворення центрального органу виконавчої влади зі спеціальним статусом [11];

- Постанова КМУ «Деякі питання проведення зовнішнього аудиту діяльності уповноваженого органу у сфері захисту критичної інфраструктури України», яким регламентує складення Рахунковою палатою звіту про зовнішній аудит діяльності уповноваженого органу у сфері захисту критичної інфраструктури України [3] та ін.

Такі правові орієнтири щодо захисту та підвищення стійкості критичної інфраструктури є гранично необхідними в розрізі актуальності загроз воєнних дій.

Усі ці кроки підкреслюють спрямованість державної політики на захист, своєчасне реагування на загрози, нейтралізацію пошкоджень чи знищення об'єктів критичної інфраструктури, для цього потрібна різногалузева консолідація ресурсів. Відповідно до чинного законодавства уповноваженими органами державної влади, що відповідальні за сектор (підсектор) критичної інфраструктури, є: Міністерство енергетики – паливно-енергетичний сектор, Міністерство цифрової трансформації – інформаційний сектор, Міністерство розвитку громад і територій України – системи життєзабезпечення, Міністерство економіки – харчова промисловість та агропромисловий комплекс, Міністерство охорони здоров'я – охорона здоров'я, Національна комісія з цінних паперів та фондових ринків – ринки капіталу та організовані товарні ринки, Міністерство інфраструктури – транспорт і пошта, Міністерство з питань стратегічних галузей промисловості – галузі промисловості, Міністерство внутрішніх справ – цивільний захист населення та територій, Міністерство фінансів – фінансовий сектор. Також захист критичної інфраструктури у військовий період покладено й на такі органи виконавчої влади, як: НПУ, МЧС, СБУ, Нацгвардія, ЗСУ, військові адміністрації, Державна служба спеціального зв'язку та захисту інформації, Державна інспекція ядерного регулювання України.

Війна висуває нові посилені вимоги до здійснення контррозвідувального, контртерористичного і контрдиверсійного захисту таких об'єктів: енергетики та ядерної енергетики; нафтової, газової, харчової промисловості; інформаційних технологій та електронних комунікацій; мережі життєзабезпечення; агропромислового, транспортного комплексу, пошти, системи зв'язку; об'єктів охорони здоров'я; стратегічно важливих сфер народного господарства; банківського сектору та ін.

Серед основних загроз за серйозністю наслідків для критичної інфраструктури слід назвати кібератаки, терористичні та диверсійні акти, військові операції. Усе це призводить до виникнення аварій на об'єктах підвищеної небезпеки, як наслідок, це може привести до виникнення надзвичайних ситуацій регіонального, державного або світового рівня. Наведемо приклади таких ситуацій.

Проведення військових дій на території України збройними силами країни-агресорки не обходить стороною об'єкти ядерної енергетики (Запорізька та Південноукраїнська АЕС), що становить серйозну потенційну загрозу для всього світу.

Негативний вплив на безпеку об'єктів критичної інфраструктури носять ракетно-артилерійські обстріли об'єктів енергетичної галузі України. Зокрема, було нанесено значну шкоду шляхом обстрілів системи енергетики: ГЕС – Дніпровської, Кременчуцької, Київської, Каховської, ТЕС – Київської, Трипільської, Харківської, Старобешівської, Слов'янської, Миронівської, Луганської, Курахівської, Зуївської, Зміївської, Запорізької, Вуглегірської.

Об'єкти інфраструктури із забезпечення життєдіяльності населення, електромережі, об'єкти із генерування та передачі електроенергії, водоканал, тепло- та газомережі,

телефонні лінії та ін. постійно піддаються обстрілам по всій території України. Особливо гостро це стосується Запорізької, Херсонської, Миколаївської областей, окупованих, деокупованих та територій, де проводяться військові дії.

Значна шкода (часткова руйнація чи ліквідація) через ведення військових дій нанесена об'єктам портового господарства, транспортним магістралям, мостам, переправам, об'єктам промисловості, нафтопроводам та сховищам; газопровадам та ін. об'єктам критичної інфраструктури по всій території нашої держави.

Уряд додатково виділяє з резервного фонду держбюджету кошти для фінансової підтримки пошкоджених об'єктів критичної інфраструктури від бойових дій, диверсій, терористичних актів, спричинених військовою агресією Російської Федерації. Наприклад, Постанова КМУ «Про внесення змін до Порядку виконання повноважень Державною казначейською службою в особливому режимі в умовах воєнного стану», Постанова КМУ «Деякі питання здійснення оборонних та публічних закупівель товарів, робіт і послуг в умовах воєнного стану», розпорядження КМУ «Про виділення коштів з резервного фонду державного бюджету для фінансової підтримки комунального підприємства "Облводоканал" Запорізької обласної ради», Постанова КМУ «Деякі питання отримання, розподілу, використання та обліку гуманітарної допомоги для задоволення потреб енергетики в умовах воєнного стану» та ін. Проте така кількість знешкоджених та пошкоджених об'єктів національної мережі критичної інфраструктури України вимагає міжнародного втручання та значних фінансових санкцій. Відповідно, на сьогодні триває робота законодавчої гілки влади щодо врегулювання правового простору у цьому питанні.

Законодавство з питань державної регіональної політики щодо відновлення об'єктів критичної інфраструктури під час військового стану врегульовано законами України: «Про внесення змін до деяких законодавчих актів України щодо засад державної регіональної політики та політики відновлення регіонів і територій», «Про засади внутрішньої і зовнішньої політики», «Про місцеві державні адміністрації», «Про місцеве самоврядування в Україні», «Про регулювання містобудівної діяльності», «Про транскордонне співробітництво», «Про державне прогнозування та розроблення програм економічного і соціального розвитку України», «Про державні цільові програми», «Про Генеральну схему планування території України» та іншими нормативно-правовими документами. Такі кроки державної політики націлені на ефективність та прискорення роботи конкретних об'єктів критичної інфраструктури по всій території нашої країни.

Для зміцнення системи захисту критичної інфраструктури необхідно також прописати у законодавстві «можливість застосування за порушення (як умисне, так і неумисне) вимог безпеки стосовно об'єктів критичної інфраструктури, а також знехтування законними вимогами суб'єктів-контролерів заходів державного примусу (залежно від обставин – дисциплінарного, адміністративного і кримінального характеру) стосовно відповідальних посадовців як фізичних осіб. У відношенні ж юридичних осіб слід розглянути можливість реалізації системи фінансових санкцій або ж певних обмежень у профільній господарській діяльності (оскільки її ведення в умовах недостатньої захищеності об'єкта критичної інфраструктури може призвести до тяжких наслідків і становити пряму загрозу національній безпеці)» [5, с. 71–72].

**Висновки.** Стан захищеності об'єктів критичної інфраструктури є складником національної безпеки країни. На сьогодні гостро стоять проблеми фінансового і матеріально-технічного забезпечення тих об'єктів критичної інфраструктури, що постраждали внаслідок військових дій. У короткий час було доопрацьовано нормативно-правове поле щодо створення ефективних умов функціонування та відбудови

критичної інфраструктури в умовах військового стану. Це питання базує у процесі створення продуктивних механізмів у сфері забезпечення інтересів національної безпеки нашої держави. Отже, подальшого наукового вивчення потребують проблеми пошуку можливості адаптації світового досвіду щодо системи захисту та підвищення стійкості критичної інфраструктури крізь призму військових загроз.

#### Список використаних джерел:

1. Деякі питання ідентифікації об'єктів підвищеної небезпеки : Постанова КМУ від 13 вересня 2022 р. № 1030. Дата оновлення: 16.09.2022. URL: <https://zakon.rada.gov.ua/laws/show/1030-2022-%D0%BF#Text> (дата звернення: 20.10.2022).
2. Деякі питання об'єктів критичної інфраструктури : Постанова КМУ від 9 жовтня 2020 р. № 1109. Дата оновлення: 07.09.2022. URL: <https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text> (дата звернення: 21.10.2022).
3. Деякі питання проведення зовнішнього аудиту діяльності уповноваженого органу у сфері захисту критичної інфраструктури України : Постанова КМУ від 10 червня 2022 р. № 675. Дата оновлення: 15.06.2022. URL: <https://zakon.rada.gov.ua/laws/show/675-2022-%D0%BF#Text> (дата звернення: 12.10.2022).
4. Кузьменко Ю.В. Правове поле у сфері протидії рейдерству. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки»*. 2018. Вип. 4. Т. 2. С. 12–16.
5. Кузьменко Ю.В., Бондар В.В. Захист об'єктів критичної інфраструктури: адміністративно-правове забезпечення. *Юридичний бюлетень*. 2021. Вип. 21. С. 67–72.
6. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова КМУ від 19 червня 2019 р. № 518. Дата оновлення: 7.09.2022. URL: <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text> (дата звернення: 11.10.2022).
7. Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України : Постанова Правління НБУ від 12 серпня 2022 № 178. Дата оновлення: 20.08.2022. URL: <https://zakon.rada.gov.ua/laws/show/v0178500-22#Text> (дата звернення: 13.10.2022).
8. Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури : Постанова КМУ від 22 липня 2022 р. № 821. Дата оновлення: 22.07.2022. URL: <https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#Text> (дата звернення: 15.10.2022).
9. Про критичну інфраструктуру : Закон України від 16 листопада 2021 року № 1882-ІХ. Дата оновлення: 15.06.2022. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (дата звернення: 13.08.2022).
10. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : розпорядження КМУ від 6 грудня 2017 р. № 1009-р. Дата оновлення: 6.12.2017. URL: <https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text> (дата звернення: 10.10.2022).
11. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України : Постанова КМУ від 12 липня 2022 р. № 787. Набуває чинності. URL: <https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text> (дата звернення: 17.10.2022).