Наталія ФЕДОСЕНКО,
кандидат юридичних наук, доцент, доцент кафедри права гуманітарно-правового факультета Національного аерокосмічного університету «Харківський авіаційний інститут», Харків, Україна,
ORCID: https://orcid.org/0000-0002-6615-3937
e-mail: n.fedosenko@khai.edu

DOI: https://doi.org/10.32620/pls.2025.67.28

ДОГОВІРНІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ПОСТАЧАННЯ ПОСЛУГ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ПРИВАТНО-ПРАВОВИЙ АСПЕКТ

Анотація: *у тезах досліджуються договірно-правові механізми забезпечення безперервності та надійності функціонування об'єктів критичної інфраструктури в умовах дестабілізуючих чинників, зокрема воєнних дій, техногенних загроз і кіберінцидентів. Акцентовано увагу на особливостях регулювання цивільно-правових зобов'язань суб'єктів, що надають послуги у сферах енергетики, зв'язку, водопостачання та інших стратегічно важливих галузях. Проаналізовано зміст договірних положень щодо відповідальності, форс-мажорних обставин, страхового захисту та гарантій належного виконання зобов'язань. З урахуванням порівняльного аналізу європейської договірної практики сформульовано пропозиції щодо підвищення ефективності та стійкості приватно-правових інструментів у контексті захисту критичної інфраструктури.*

Ключові слова: *договір, правочин, цивільне правовідношення, договірне зобов'язання, критична інфраструктура, зобов'язання, форс-мажор, відповідальність, стійкість, страхування*

У світлі глобальних і локальних викликів, пов'язаних із забезпеченням належного функціонування та захисту критичної інфраструктури, Україна постала перед комплексним завданням інтеграції ефективних і гнучких правових механізмів, які мають бути адаптовані не лише до умов повномасштабної війни та супутніх військових загроз, а й до зростаючої інтенсивності кіберзлочинності, дестабілізації у сфері енергетики, транспорту, зв'язку та інших інфраструктурно значущих галузей. Це вимагає перегляду існуючих нормативно-правових підходів і формування системи договірного регулювання, здатної забезпечити правову визначеність, гнучкість реагування на надзвичайні обставини, а також стійкість до економічної нестабільності як на національному, так і на регіональному рівнях. Одним із таких механізмів є цивільно-правовий договір, що має потенціал не лише регламентувати зобов'язальні правовідносини, але й виступати як запобіжник кризових ситуацій [1].

Правовий інструментарій договору в сучасних умовах постає не лише як традиційний механізм упорядкування цивільних правовідносин, але й як стратегічний засіб забезпечення ефективної координації між приватними та публічними суб'єктами у сфері функціонування критичної інфраструктури. Його гнучкість дозволяє адаптувати умови співпраці до конкретних потреб та викликів, зберігаючи при цьому належний рівень правової передбачуваності, необхідної для досягнення стабільності та довіри сторін. Особливої ваги це набуває у високоризикових галузях, таких як енергетика, телекомунікації та цифрові технології, де навіть тимчасові перебої у наданні послуг можуть спричинити ланцюгові наслідки, що зачіпають як безпеку держави, так і основоположні права громадян. У цьому контексті договір виконує не лише регулятивну, а й превентивну функцію, сприяючи формуванню правової основи для запобігання кризовим явищам та забезпечення безперервності надання життєво необхідних послуг.

В умовах цифровізації окремі аспекти захисту інфраструктури реалізуються через договори про обслуговування інформаційних систем, включаючи положення про кіберзахист, обмеження відповідальності та стандарти безпеки [2]. Наразі в Україні відбувається інституціалізація системи захисту критичної інфраструктури, що знаходить своє відображення у проєкті Закону України "Про критичну інфраструктуру" [3]. Прийняття цього закону покликане створити єдині підходи до

визначення об'єктів критичної інфраструктури та організації їх захисту.

У сфері енергетики та комунікацій дедалі більшого поширення набувають договори в межах публічно-приватного партнерства, що є гнучким засобом балансування приватного інтересу з публічними цілями. Такі договори дозволяють приватним партнерам брати участь у модернізації об'єктів інфраструктури, водночас держава забезпечує контроль та нормативну підтримку. Аналіз чинного законодавства та судової практики дозволяє виокремити специфічні особливості укладення договорів у сферах із підвищеним ризиком, зокрема в енергетиці та транспорті [4].

Зважаючи на активну фазу євроінтеграційних процесів та стратегічну мету України щодо гармонізації національного законодавства з правом Європейського Союзу, особливо у сфері цифрової безпеки, перед державою постає нагальна потреба у комплексній імплементації положень Директиви (ЄС) 2022/2555 (NIS2) про заходи для забезпечення високого спільного рівня кібербезпеки в усьому Союзі. Ця директива, яка замінила попередню NIS-директиву, значно розширює перелік суб'єктів, на яких поширюється її дія, включаючи не лише операторів критичної інфраструктури, але й постачальників цифрових послуг, енергетичні, транспортні, медичні, банківські, водопостачальні та інші стратегічні сектори. Для України це означає необхідність створення ефективної нормативної, інституційної та технічної бази для виявлення, запобігання і реагування на кіберзагрози на рівні, сумірному з європейськими стандартами. Особливу увагу необхідно приділити розробці механізмів державного нагляду, впровадженню обов'язкових вимог до управління ризиками для операторів суттєвих послуг, а також встановленню відповідальності за недотримання нових норм. В умовах війни, коли Україна щоденно стикається з гібридними атаками на об'єкти критичної інфраструктури, інтеграція принципів NIS2 набуває не лише правового, але й стратегічного значення для забезпечення кіберстійкості, суверенітету та стійкого функціонування держави. [5]. Враховуючи рекомендації Європейської комісії щодо безпеки мереж 5G, договірна практика має бути орієнтована на відповідність вимогам кіберзахисту [6].

Положення Директиви NIS2 також можуть бути ефективно інкорпоровані у договірні конструкції, що регулюють надання послуг із забезпечення безпеки критичної інфраструктури в Україні. Зокрема, принципи управління кіберризиками, вимоги до звітності про інциденти безпеки, зобов'язання щодо збереження конфіденційності та сталість роботи інформаційних систем можуть бути закріплені як істотні умови договорів між операторами критичної інфраструктури та постачальниками IT-послуг, системного адміністрування, хмарних технологій або програмного забезпечення. Наприклад, в умовах договору про обслуговування дата-центру, що забезпечує безперебійну роботу цифрових сервісів об'єктів енергетичного сектору, можуть бути передбачені положення щодо регулярного аудиту кібербезпеки, зобов'язання про негайне інформування замовника про виявлені вразливості, а також про участь у спільних навчаннях із кіберзахисту. Аналогічно, у договорах з телекомунікаційними провайдерами, що обслуговують об'єкти з підвищеним рівнем ризику, можуть бути деталізовані умови щодо технічної підтримки у режимі 24/7, резервного копіювання даних, відповідальності за невиконання стандартів безпеки. Таким чином, положення NIS2 можуть слугувати не лише орієнтиром для державного регулювання, а й основою для формування сучасної договірної практики, що поєднує гнучкість приватного права з вимогами до високого рівня захищеності, необхідного для стабільного функціонування критичних інфраструктурних об'єктів в умовах зовнішніх загроз [6].

На міжнародному рівні акцент робиться на довгострокову стійкість інфраструктури до природних та техногенних загроз, що також відображається в договірній практиці із залученням страхових механізмів [7]. Це відкриває можливості для трансформації українського підходу до договірного регулювання – із врахуванням глобальних тенденцій, включаючи зобов'язання щодо страхування, перевірки контрагентів на надійність та внесення специфічних застережень force majeure.

Таким чином, договір у сфері захисту критичної інфраструктури постає не лише як формалізований правовий акт, що регламентує взаємні права та обов'язки сторін, а як комплексний інструмент забезпечення довіри між суб'єктами публічного і приватного секторів, засіб правової координації, що дозволяє досягати синергії у забезпеченні безпеки життєво важливих об'єктів. Він відображає не лише юридичну природу відносин, але й слугує проявом інституційної спроможності суспільства до реагування на кризові явища. Ефективність такого договору значною мірою обумовлюється стабільністю та актуальністю нормативно-правової бази, наявністю послідовної судової практики, що забезпечує передбачуваність рішень, а також здатністю суб'єктів до адаптації договірних конструкцій до умов гібридних загроз, зокрема воєнного стану, кіберінцидентів, перебоїв у функціонуванні енергетичних систем та цифрових сервісів.

Не менш важливим чинником є правова культура сторін, їхня готовність до відкритого діалогу, обміну критично важливою інформацією, а також до розроблення механізмів запобігання та мінімізації ризиків, що мають як економічний, так і соціально-безпековий вимір. У цьому контексті договір виконує роль інструменту правової стійкості – здатності правової системи та її суб'єктів витримувати вплив дестабілізуючих чинників, залишаючись ефективними в забезпеченні публічного інтересу та національної безпеки.

Бібліографічні посилання

1. Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV (поточна редакція від 07.05.2022) URL: https://ips.ligazakon.net/document/view/t030435?ed=2021_11_17 (дата звернення 20.04.2025)

2. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 20.04.2025)

3. Про критичну інфраструктуру. Закон України Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення 21.04.2025)

4. Сімутін С.О. Проблеми правового регулювання публічних договорів у сфері енергетики. Юридичний вісник України. 2021. № 9. С. 14–18.

5. Commission Recommendation (EU) 2019/534 of 26 March 2019 on Cybersecurity of 5G networks [Electronic resource]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019H0534

6. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity (NIS2 Directive) [Electronic resource]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

7. OECD. Ensuring the Resilience of Critical Infrastructure to Natural Hazards and Climate Change. – Paris: OECD Publishing, 2021. – DOI: https://doi.org/10.1787/e10f3f5f-en

N. Fedosenko

Contractual mechanisms for ensuring the reliability of the supply of critical infrastructure services: private legal aspect.

Abstract: the paper explores contractual and legal mechanisms aimed at ensuring the continuity and reliability of critical infrastructure operation under destabilizing conditions, including warfare, technological threats, and cyber incidents. Particular attention is paid to the regulation of civil obligations of entities providing services in strategically important sectors such as energy, communications, and water supply. The content of contractual clauses related to liability, force majeure, insurance coverage, and performance guarantees is analyzed. Based on a comparative review of European contractual practices, proposals are formulated to enhance the effectiveness and resilience of private-law instruments in the context of critical infrastructure protection.

Keywords: contract, transaction, civil legal relationship, contractual obligation, critical infrastructure, obligation, force majeure, liability, sustainability, insurance.

Зразок для цитування:

Федосенко Н. Договірні механізми забезпечення надійності постачання послуг критичної інфраструктури: приватно-правовий аспект. Пропілеї права та безпеки, 2025. №6-7. С. 100-102. DOI: https://doi.org/10.32620/pls.2025.67.28.