

УДК 341.3:621.31

DOI <https://doi.org/10.24144/2307-3322.2025.90.5.19>

МІЖНАРОДНО-ПРАВОВІ СТАНДАРТИ ЗАХИСТУ КРИТИЧНОЇ ЕНЕРГОІНФРАСТРУКТУРИ ПІД ЧАС ЗБРОЙНОГО КОНФЛІКТУ

Качурінер В.Л.,
*кандидат юридичних наук, доцент,
доцент кафедри морського та міжнародного права
Міжнародного гуманітарного університету*

Качурінер В.Л. Міжнародно-правові стандарти захисту критичної енергоінфраструктури під час збройного конфлікту.

Стаття аналізує міжнародно-правові стандарти захисту критичної енергоінфраструктури, зокрема електростанцій, газопроводів та систем електропостачання, під час збройних конфліктів.

Дослідження базується на Женевських конвенціях 1949 року, Додаткових протоколах 1977 року, нормах звичаєвого міжнародного гуманітарного права та міжнародного екологічного права, включаючи Конвенцію ENMOD 1976 року.

Особливий акцент зроблено на принципах розрізнення, пропорційності та військової необхідності, які забороняють атаки на цивільні об'єкти без прямого військового значення.

Розглянуто захист ядерних об'єктів, підкреслюючи їхню вразливість до катастрофічних наслідків, та сучасні виклики, такі як кібератаки на енергосистеми. Практичні приклади, зокрема з конфлікту в Україні 2022–2023 років, ілюструють складнощі застосування правових норм через подвійне призначення інфраструктури та обмежену відповідальність за порушення. Зростання ролі відновлювальних джерел енергії додає нових викликів для захисту.

У статті наголошується на необхідності вдосконалення правових механізмів, зокрема щодо регулювання кібервійни, та посилення міжнародної співпраці для забезпечення безпеки енергоінфраструктури. Захист таких об'єктів є не лише юридичним, а й моральним імперативом, оскільки від нього залежить добробут цивільного населення.

Міжнародна спільнота має адаптувати правові норми до нових технологій і форм війни, щоб ефективно протидіяти загрозам. Надмірна уразливість енергетичних систем, а також відсутність чітких правових рамок для регулювання кібератак і впровадження блокчейн-технологій породжують юридичну невизначеність, що становить загрозу стабільності та безпеці. Отже, існує необхідність у всебічному аналізі міжнародно-правових стандартів захисту енергоінфраструктури, оцінці можливостей блокчейн-технологій та розробці рекомендацій щодо їх інтеграції для підвищення безпеки й ефективності захисту в умовах збройних конфліктів.

Зроблено висновок про важливість розвитку механізмів моніторингу, швидкого реагування та застосування санкцій для захисту критичної інфраструктури. Це сприятиме зменшенню гуманітарних і екологічних наслідків атак, забезпечуючи стабільність у кризових умовах.

Ключові слова: міжнародне гуманітарне право, критична енергоінфраструктура, збройний конфлікт, Женевські конвенції, блокчейн, кібербезпека, смарт-контракт, правове регулювання, екологічне право, кібератаки.

Kachuriner V.L. International legal standards for protecting critical energy infrastructure during armed conflict.

The article examines the international legal standards for protecting critical energy infrastructure, including power plants, gas pipelines, and electricity supply systems, during armed conflicts.

The study is based on the Geneva Conventions of 1949, their Additional Protocols of 1977, customary international humanitarian law, and international environmental law, including the 1976 ENMOD Convention.

Particular emphasis is placed on the principles of distinction, proportionality, and military necessity, which prohibit attacks on civilian objects lacking direct military significance.

The protection of nuclear facilities is addressed, highlighting their vulnerability to catastrophic consequences, alongside contemporary challenges such as cyberattacks on energy systems. Practical examples, particularly from the 2022–2023 conflict in Ukraine, illustrate the complexities of applying legal norms due to the dual-use nature of infrastructure and limited accountability for violations. The increasing role of renewable energy sources introduces additional protection challenges.

The article underscores the need to enhance legal mechanisms, particularly in regulating cyber warfare, and to strengthen international cooperation to ensure the security of energy infrastructure. Protecting such infrastructure is not only a legal but also a moral imperative, as it directly impacts civilian well-being.

The international community must adapt legal norms to new technologies and forms of warfare to effectively counter threats. The excessive vulnerability of energy systems, coupled with the lack of clear legal frameworks for regulating cyberattacks and implementing blockchain technologies, creates legal uncertainty that threatens stability and security. Consequently, there is a need for a comprehensive analysis of international legal standards for protecting energy infrastructure, an assessment of the potential of blockchain technologies, and the development of recommendations for their integration to enhance security and effectiveness of protection in the context of armed conflicts.

The article concludes by emphasizing the importance of developing monitoring mechanisms, rapid response systems, and sanctions to safeguard critical infrastructure, thereby mitigating humanitarian and environmental consequences of attacks and ensuring stability in crisis conditions.

Key words: international humanitarian law, critical energy infrastructure, armed conflict, Geneva Conventions, blockchain, cybersecurity, smart contract, legal regulation, environmental law, cyberattacks.

Постановка проблеми. Критична енергоінфраструктура, включаючи електростанції, газопроводи та системи електропостачання, є життєво важливою для функціонування суспільства, але під час збройних конфліктів стає вразливою до фізичних і кібератак, що призводять до гуманітарних, економічних та екологічних криз.

Міжнародне гуманітарне право, зокрема Женевські конвенції 1949 року та Додаткові протоколи 1977 року, встановлює стандарти захисту таких об'єктів, однак їхнє застосування ускладнене через подвійне призначення інфраструктури, недостатнє регулювання кібервійни та обмежену відповідальність за порушення. В умовах глобалізації та цифровізації особливого значення набуває захист енергосистем від кібератак, які можуть паралізувати інфраструктуру без фізичного втручання.

Технологія блокчейн пропонує інноваційні рішення для забезпечення кібербезпеки, прозорості та стійкості енергомереж, але її інтеграція в критичну інфраструктуру залишається недостатньо дослідженою та нестандартизованою. В Україні, де атаки на енергосистему в 2022–2023 роках виявили вразливість інфраструктури, проблема захисту набуває особливої актуальності. Надмірна вразливість енергосистем і відсутність чітких правових механізмів для регулювання кібератак та використання блокчейну створюють юридичну невизначеність, що загрожує стабільності та безпеці.

Таким чином, виникає потреба в комплексному аналізі міжнародно-правових стандартів захисту енергоінфраструктури, оцінці потенціалу блокчейн-технологій та розробці пропозицій для їх інтеграції, що сприятиме підвищенню безпеки та ефективності захисту в умовах збройних конфліктів.

Мета дослідження – аналіз міжнародно-правових стандартів захисту критичної енергоінфраструктури під час збройних конфліктів, оцінка сучасних викликів, зокрема кібератак, та визначення потенціалу блокчейн-технологій для забезпечення безпеки енергосистем, з розробкою пропозицій щодо їх правового регулювання та практичного впровадження.

Стан опрацювання проблематики. Проблематика захисту критичної енергоінфраструктури під час збройних конфліктів є предметом активного дослідження в міжнародному гуманітарному праві та кібербезпеці. Основною правовою базою є Женевські конвенції 1949 року, Додаткові протоколи 1977 року, Конвенція ENMOD 1976 року та норми звичаєвого права, досліджені Міжнародним комітетом Червоного Хреста.

Вчені, такі як Jean-Marie Henckaerts, Louise Doswald-Beck, Michael N. Schmitt, аналізували принципи захисту цивільних об'єктів і кібервійни, наголошуючи на необхідності адаптації права до цифрових загроз. У контексті блокчейну дослідження таких авторів, як Primavera De Filippi,

Aaron Wright та проекти компаній Enel і RWE, підкреслюють потенціал технології для підвищення безпеки енергосистем. В Україні вчені, зокрема О. Завитій, О. Задорожній, В. Кравченко, досліджували захист інфраструктури в умовах конфлікту, але інтеграція блокчейну залишається малодослідженою.

Недостатня стандартизація блокчейн-рішень і прогалини в правовому регулюванні кібератак вказують на потребу подальшого вивчення для забезпечення ефективного захисту енергосистем.

Виклад основного матеріалу. Критична енергоінфраструктура, як-от електростанції, газопроводи, нафтопереробні заводи та системи електропостачання, є основою функціонування суспільства. Під час збройних конфліктів ці об'єкти стають вразливими до атак, що може спричинити катастрофічні гуманітарні, економічні та екологічні наслідки. Міжнародне гуманітарне право встановлює норми захисту таких об'єктів, щоб мінімізувати шкоду цивільному населенню та дотримуватися принципів гуманності. Водночас технологія блокчейн відкриває нові можливості для підвищення безпеки та стійкості енергоінфраструктури, зокрема в умовах конфліктів. Ця стаття аналізує міжнародно-правові стандарти захисту критичної енергоінфраструктури, їх застосування, сучасні виклики та потенціал інтеграції блокчейн-технологій.

Женевські конвенції 1949 року та їхні Додаткові протоколи 1977 року є основою міжнародного гуманітарного права. Вони зобов'язують сторони конфлікту розрізняти цивільні об'єкти та військові цілі (Додатковий протокол I, стаття 48) [1]. Критична енергоінфраструктура, якщо вона не використовується для військових потреб, вважається цивільним об'єктом і підлягає захисту. Атаки дозволені лише на військові об'єкти, які за своєю природою, розташуванням чи використанням роблять внесок у військові дії та чие знищення забезпечує чітку військову перевагу (Додатковий протокол I, стаття 52(2)) [1]. Забороняється атакувати об'єкти, необхідні для виживання цивільного населення, наприклад, системи електропостачання, що забезпечують питну воду чи опалення (Додатковий протокол I, стаття 54) [1].

Принципи пропорційності та військової необхідності відіграють ключову роль. Атака на об'єкт із подвійним призначенням, наприклад електростанцію, що живить лікарні та військові бази, є незаконною, якщо шкода для цивільних буде надмірною порівняно з військовою вигодою (Додатковий протокол I, стаття 51(5)(b)) [1]. Військова необхідність дозволяє атакувати лише об'єкти, потрібні для досягнення законної військової мети, виключаючи інфраструктуру без прямого зв'язку з воєнними діями.

Міжнародне екологічне право доповнює захист енергоінфраструктури. Методи ведення війни, які завдають довгострокової, масштабної та серйозної шкоди природному середовищу, заборонені (Додатковий протокол I, стаття 55) [1]. Наприклад, атака на нафтопереробний завод чи ядерну електростанцію може спричинити екологічну катастрофу. Конвенція про заборону військового чи іншого ворожого використання засобів впливу на природне середовище 1976 року (ENMOD) обмежує дії, що змінюють природне середовище через пошкодження енергоінфраструктури [2].

Особливу увагу приділено ядерним електростанціям через їхній потенціал до катастрофічних наслідків. Міжнародні норми закликають уникати атак на ядерні об'єкти, що використовуються в мирних цілях, особливо якщо це може призвести до вивільнення небезпечних сил і серйозної шкоди цивільним (Резолюція МАГАТЕ GC(53)/DEC/13; Додатковий протокол I, стаття 56) [1, 3]. Звичаєве міжнародне право, за висновками Міжнародного комітету Червоного Хреста, також захищає об'єкти з небезпечними силами, як-от електростанції чи греблі (Правило 42) [4].

Застосування цих норм стикається з викликами. Об'єкти енергоінфраструктури часто мають подвійне призначення, що ускладнює визначення їхнього статусу як законної цілі. Сучасні конфлікти включають кібератаки, які виводять з ладу електромережі без фізичного знищення. Міжнародне гуманітарне право ще недостатньо чітко регулює кібервійну, хоча принципи пропорційності та розрізнення застосовуються й до таких атак [4]. Порушення норм часто залишаються без покарання через складність притягнення до відповідальності. Міжнародний кримінальний суд може розглядати такі дії як воєнні злочини, але його юрисдикція обмежена. Пошкодження енергоінфраструктури спричиняє гуманітарні кризи, як-от відключення електроенергії чи брак опалення, що особливо гостро відчувається в холодні місяці чи густонаселених районах.

Недавні конфлікти, зокрема в Україні, ілюструють вразливість енергоінфраструктури. Атаки на електростанції, підстанції та газопроводи спричинили перебої в електропостачанні, впливаючи на цивільне населення [5]. Систематичні атаки на українську енергосистему в 2022-2023 роках підкреслили потребу в ефективніших правових механізмах. Зростання ролі відновлювальних

джерел енергії, таких як сонячні чи вітрові електростанції, додає нових викликів: їхня розподілена природа ускладнює захист, але зменшує ризик масштабних наслідків від однієї атаки.

Блокчейн-технології можуть значно посилити захист енергоінфраструктури, особливо в умовах збройних конфліктів. Блокчейн, як розподілена база даних, забезпечує прозорість, незмінність і безпеку даних, що дозволяє захищати критичні системи від кібератак [6]. Наприклад, блокчейн може використовуватися для управління доступом до енергосистем, відстеження транзакцій енергії в децентралізованих мережах або забезпечення цілісності даних про стан інфраструктури. У контексті конфліктів це може запобігти несанкціонованим втручанням у системи управління електромережами. Дослідження показують, що блокчейн підвищує стійкість до кіберзагроз, хоча виклики, такі як низька масштабованість і високі енергетичні витрати, обмежують його широке впровадження [6]. Понад 40 європейських енергетичних компаній, зокрема Enel і RWE, уже тестують блокчейн для оптимізації торгівлі енергоресурсами та управління мережами [7].

Інтеграція блокчейну в енергетичну інфраструктуру вимагає адаптації регуляторних рамок. Наприклад, смарт-контракти можуть автоматизувати управління енергопостачанням у децентралізованих системах, що особливо важливо для відновлювальних джерел енергії, але потребують правового визнання [8]. В Україні пілотні проекти з використання блокчейну в земельному кадастрі та електронних торгах свідчать про потенціал технології, який може бути розширений на енергетику. Міжнародна співпраця, зокрема через ініціативи, подібні до Європейської інфраструктури блокчейн-сервісів (EBSI), може сприяти стандартизації та впровадженню таких рішень [9].

О. Завитій зауважує, що завдяки технології блокчейн потоки електроенергії можуть бути надійно захищені від зовнішнього втручання, що забезпечує можливість сертифікації електроенергії та перевірки реальних показників її генерації й споживання. Як децентралізована система, побудована на принципах розподіленої бази даних, блокчейн дозволяє створити єдиний архів для зберігання всіх даних про рахунки за електроенергію. Це дає споживачам змогу краще контролювати свої договори на постачання електроенергії, відкриваючи широкі можливості для розробки смарт-контрактів, а також отримувати точну інформацію про фактичне споживання. Усі записи в блокчейн-реєстрі залишаються відкритими й доступними. Водночас слід зазначити, що через невизначеність правового статусу криптоіндустрії Національна енергетична корпорація стикається з обмеженнями у впровадженні проектів із використанням смарт-контрактів через відсутність відповідної правової бази [10, с. 248-249].

Для ефективного захисту енергоінфраструктури необхідне посилення міжнародного співробітництва. Держави повинні розробити механізми швидкого реагування на порушення, включаючи санкції та судові переслідування. Міжнародні організації, такі як ООН чи МАГАТЕ, можуть відігравати ключову роль у моніторингу та координації зусиль із захисту критичних об'єктів. Розвиток технологій, зокрема систем кіберзахисту на основі блокчейну, вимагає створення нових правових стандартів, які б ураховували специфіку цифрових загроз.

Міжнародно-правові стандарти, включно з Женевськими конвенціями, Додатковими протоколами, звичаєвим правом та екологічними угодами, створюють основу для захисту критичної енергоінфраструктури. Інтеграція блокчейн-технологій може посилити ці механізми, забезпечуючи стійкість до кібератак і прозорість управління. Такої ж думки дотримується В.С. Назаров: «використання блокчейн-технологій... може посилити довіру зі сторони інвесторів, спростити процес фінансових операцій, розширити доступ до капіталу та покращити управління. Ці чинники, у сукупності, можуть стати джерелом підвищення інвестиційної активності у галузі, позитивно сприяючи її зростанню та розвитку» [11, с. 232]. Проте практична реалізація цих норм і технологій потребує чіткішого регулювання кібервійни, посилення міжнародного моніторингу та співпраці держав. Захист енергоінфраструктури є не лише юридичним, а й моральним обов'язком, адже від нього залежить добробут мільйонів людей. Міжнародна спільнота має вдосконалювати правові та технологічні механізми, адаптуючи їх до сучасних реалій війни.

Висновки. Міжнародно-правові стандарти, зокрема Женевські конвенції 1949 року, Додаткові протоколи 1977 року, Конвенція ENMOD 1976 року та норми звичаєвого права, створюють міцну основу для захисту критичної енергоінфраструктури під час збройних конфліктів. Ці норми, ґрунтуючись на принципах розрізнення, пропорційності та військової необхідності, забороняють атаки на цивільні об'єкти, включаючи електростанції, газопроводи та системи електропостачання, якщо вони не мають прямого військового значення. Особливий захист надається ядерним об'єктам через їхній потенціал до катастрофічних наслідків. Однак практичне застосування цих

норм ускладнене через подвійне призначення інфраструктури, зростання кібератак і обмежену відповідальність за порушення. Конфлікт в Україні 2022–2023 років продемонстрував вразливість енергосистем і необхідність ефективніших правових механізмів.

Інтеграція блокчейн-технологій відкриває нові можливості для захисту енергоінфраструктури, забезпечуючи прозорість, кібербезпеку та стійкість до атак завдяки децентралізованому управлінню даними й смарт-контрактам. Пілотні проекти в Україні та Європі підтверджують потенціал блокчейну, але його впровадження стримується недостатньою стандартизацією, високими енергетичними витратами та прогалинами в правовому регулюванні. Для підвищення ефективності захисту необхідне чіткіше регулювання кібервійни, стандартизація блокчейн-рішень і посилення міжнародної співпраці через ООН, МАГАТЕ та інші організації. Захист енергоінфраструктури є юридичним і моральним імперативом, що вимагає адаптації правових і технологічних механізмів до сучасних викликів війни, включаючи цифрові загрози та розвиток відновлювальних джерел енергії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Женевські конвенції 1949 року та Додаткові протоколи 1977 року. URL: <https://www.icrc.org/en/doc/war-and-law/treaties-customary-law/geneva-conventions/overview.htm> (дата звернення: 04.08.2025 р.).
2. Конвенція про заборону військового чи іншого ворожого використання засобів впливу на природне середовище 1976 року (ENMOD). URL: <https://www.un.org/disarmament/enmod/> (дата звернення: 04.08.2025 р.).
3. Резолюція МАГАТЕ GC(53)/DEC/13. Доступно за: <https://www.iaea.org/about/governance/general-conference-documents>.
4. Дослідження звичаєвого міжнародного гуманітарного права Міжнародного комітету Червоного Хреста. URL: <https://www.icrc.org/en/doc/resources/documents/publication/pcustom.htm> (дата звернення: 04.08.2025 р.).
5. Енергетична інфраструктура. Який обсяг української генерації захопила Росія. URL: <https://nv.ua/ukraine/events/energetichna-infrastruktura-yakiy-obsyag-ukrajinskoji-generaciji-zahopila-rosiya-galushchenko-50330597.html> (дата звернення: 04.08.2025 р.).
6. Застосування блокчейну у державному секторі. URL: <https://klona.ua/ua/blog/zastosuvannya-blokchejnu-v-derzhavnomu-sektori> (дата звернення: 04.08.2025 р.).
7. Трансформація – 2050: що потрібно енергетичній галузі від діджиталізації. URL: <https://razumkov.org.ua/statti/transformatsiia-2050-shcho-potribno-enerhetychnii-haluzi-vid-didzhytalizatsii> (дата звернення: 04.08.2025 р.).
8. Інтеграція блокчейн-технологій у системи забезпечення кібербезпеки для об'єктів критичної інфраструктури. URL: <https://bulletin-chstu.com.ua/index.php/pts/article/view/1213> (дата звернення: 04.08.2025 р.).
9. Європейської інфраструктури блокчейн-сервісів (EBSI). URL: <https://www.eternitylaw.com/ua/novyny/european-blockchain-services-infrastructure-main-points> (дата звернення: 04.08.2025 р.).
10. Завитій О. Використання смарт-контрактів на енергетичному ринку України. *Економічний аналіз*. 2023. № 2. С. 247–251.
11. Назаров В.С. Застосування технології блокчейн у підвищенні якості і стимулюванні системного зростання у сучасній економіці. *Економіка і регіон*. 2023. № 4 (91). С. 230–235.