УДК 621.311:355.58 (477)

УДОСКОНАЛЕННЯ ЗАХИСТУ ОБ'ЄКТІВ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

DOI: 10.52363/2518-1777-2026-21-5

Босак П. В.[1]*, ORCID iD 0000-0002-0303-544X
Лаврівський М. З., ORCID iD 0000-0002-8267-1996
Любовецький О. В., ORCID iD 0009-0007-7904-9091
Босак Г. С., ORCID iD 0009-0002-5648-2486
Воробець В. А., ORCID iD 0009-0008-3018-7386
*E-mail: p.bosak@ldubgd.edu.ua

Львівський державний університет безпеки життєдіяльності, Україна

ІНФОРМАЦІЯ ПРО СТАТТЮ

Надійшла до редакції: 10.02.2026
Прийнято: 09.04.2026
Опубліковано: 30.05.2026

КЛЮЧОВІ СЛОВА:

об'єкти критичної інфраструктури, цивільний захист, енергетична безпека, воєнний стан, кіберзагроза, пожежна безпека, стійкість.

АНОТАЦІЯ

У статті розглядається важливе питання забезпечення стійкості та захисту енергетичної інфраструктури України в умовах воєнного стану, особливо в умовах повномасштабної військової агресії з боку країни-агресора. Енергетичний сектор визначений як основна ціль ворожих атак, спрямованих на дестабілізацію національної економіки, оборонного потенціалу та соціального забезпечення. У дослідженні надано комплексний аналіз стану безпеки енергетичної системи України, підкреслюючи багатовимірний характер сучасних загроз. До них належать пряме фізичне руйнування за допомогою ракетних і дронових ударів, виникнення масштабних пожеж на маслонаповненому обладнанні, масштабні кібератаки на системи управління та гібридні методи дестабілізації. Методологія дослідження передбачає комплексний підхід, що поєднує статистичний аналіз динаміки атак, порівняльний аналіз типів загроз та концептуальне моделювання. Автори проаналізували статистичні дані про втрати інфраструктури за період 2022-2025 років. Дослідження виявляє зміну тактики агресора: від націлювання на теплові електростанції у 2022 році до зосередження уваги на мережах розподілу та передачі електроенергії у 2024-2025 роках. Зазначається, що прямі втрати енергетичного сектору досягли критичного рівня, який оцінюється в мільярди доларів, що вимагає негайних стратегічних контрзаходів у сфері цивільного захисту. Ключовим теоретичним внеском статті є розробка та наукове обґрунтування ієрархічної трирівневої моделі управління безпекою, заснованої на принципі «світлофорної індикації». Ця модель дозволяє застосовувати диференційовані протоколи реагування залежно від рівня загрози для оптимізації роботи підрозділів ДСНС України. «Зелений рівень» (нормальний режим) відповідає стану гомеостазу системи, коли загрози відсутні або знаходяться в прийнятних межах, і фокусується на моніторингу. «Жовтий рівень» (режим готовності) ініціюється після отримання перевіреної інформації про потенційну ескалацію (наприклад, кіберзагрози, метеорологічні аномалії або військові маневри). «Червоний рівень» (кризовий режим) вводиться після інциденту для локалізації збитків, ліквідації пожеж, запобігання системному колапсу та забезпечення виживання життєво важливих функцій. У статті аргументовано, що для забезпечення довгострокової стійкості необхідний перехід від вразливої централізованої архітектури радянської епохи до гнучкої децентралізованої мережі. Пропонований комплекс заходів включає будівництво підземних сховищ енергоресурсів, облаштування сучасних систем автоматичного пожежогасіння, розгортання автономних систем електропостачання (мікромереж) та конвергенцію фізичного захисту (інженерні бар'єри, протидронові сітки) з інтегрованою кіберзахистом інформаційних систем. Впровадження цих заходів має на меті мінімізувати час реагування на надзвичайні ситуації та зберегти системи життєзабезпечення цивільного населення під час військових дій.

Постановка проблеми. Критична інфраструктура є основою життєдіяльності будь-якої держави, забезпечуючи стабільне функціонування економіки, оборони, громадської безпеки та інших життєво важливих сфер. В умовах воєнного стану, коли Україна стикається з масштабною агресією, захист цих об’єктів набуває особливого значення. Оскільки противник використовує як фізичні, так і кібернетичні методи атак, необхідно розробити комплексні заходи для підвищення стійкості інфраструктури до загроз. Знищення чи пошкодження об’єктів енергетики, транспорту, зв’язку, водопостачання, фінансової та оборонної систем може спричинити масштабну дестабілізацію, що супроводжується виникненням складних пожеж і техногенних аварій та вимагає негайного впровадження ефективних стратегій захисту [1].

По-перше, існує фізична загроза – прямі ракетні атаки або атаки безпілотників на енергетичні об’єкти, які у 90% випадків призводять до горіння трансформаторної оливи та руйнування систем пожежогасіння [2]. По-друге, стратегічні та системні ризики: підрив довіри громадськості до спроможності держави забезпечувати основні функції, загрозу енергетичної безпеки та, зрештою, негативний вплив на економіку та життя людей. По-третє, під загрозу ставиться системна адаптивність: необхідно не лише відремонтувати пошкоджені об’єкти, але й підвищити їхню стійкість до нових загроз [3]. Таким чином, проблема виникає в неадекватності існуючих заходів захисту енергетичної інфраструктури України в умовах воєнного стану, враховуючи масштаб, характер та динаміку загрози роботи критично важливих енергетичних систем. Існуючі механізми фізичного захисту, координація дій між державними та приватними структурами, а також технологічна та інституційна стійкість не завжди достатні для задоволення потреб воєнного часу. Наприклад, було виявлено, що трирівнева концепція захисту енергетичних об’єктів реалізована лише частково, а алгоритми взаємодії операторів об'єктів з пожежно-рятувальними підрозділами не враховують тактику «подвійних ударів» агресора.

Питання захисту об’єктів критичної інфраструктури та їх нормативно-правового регулювання стали важливими через посилення загроз ззовні, зокрема природних і техногенних катастроф, терористичних актів, військових конфліктів та кібератак, на які піддаються ці об’єкти. Україна не є винятком серед інших країн, тому наявність таких загроз робить дослідження у сфері захисту критичної інфраструктури особливо актуальним. Ці об’єкти є важливими для стабільного функціонування суспільства та держави в цілому. Від 24 лютого 2022 року, коли країна-агресор розпочала повномасштабне вторгнення в Україну і продовжує намагатися знищити об’єкти критичної інфраструктури, питання їх захисту стали ще більш важливими [4].

У сучасних збройних конфліктах об’єкти критичної інфраструктури, які забезпечують життєво важливі послуги для цивільного населення, систематично піддаються атакам, випадковим пошкодженням та неправомірному використанню агресором (рис. 1). Такі дії провокують значні перебої у функціонуванні цих систем, що має серйозні та багатовимірні наслідки. Від негайних криз, як-от масове переміщення населення, кризи з продовольством та енергопостачанням, до довготривалих наслідків, таких як нестача засобів до існування та поширення інфекційних захворювань, наслідки таких руйнувань виходять далеко за межі однієї держави [5, 6].

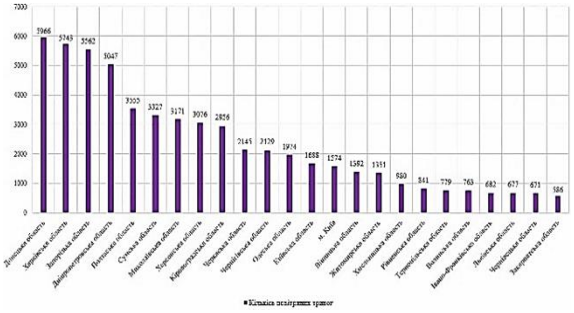

Рисунок 1 – Статистика повітряних тривог в Україні від 24 лютого 2022 року (*станом на 1 січня 2026 року*) [7]

Військова інтервенція завдає шкоди цивільному населенню як безпосередньо, через поранення та загибелі від збройного насилля, так і опосередковано, наприклад, у результаті руйнування або недоступності базових послуг. До таких послуг належать системи електропостачання, охорони здоров'я, водопостачання, обробки та розподілу продуктів харчування, каналізаційної інфраструктури, а також освіти. Безперебійне функціонування цих систем є життєво необхідним для забезпечення базових потреб цивільного населення.

Для кращого розуміння й захисту цивільного населення у контексті військової агресії необхідно чітко визначити поняття «*життєво необхідних послуг*». Ці послуги охоплюють комплекс із трьох ключових компонентів: матеріально-технічні засоби (інфраструктура, обладнання тощо), людські ресурси (оператори та обслуговуючий персонал), а також витратні матеріали (наприклад, паливо чи лікарські засоби). Усі елементи, що забезпечують безперебійну роботу системи послуг, називають критично важливими. Попри різноманітність форм негативного впливу на ці послуги, головною причиною їх порушення залишається пошкодження або руйнування об'єктів критичної інфраструктури під час військових дій. Ці ушкодження можуть мати як умисний характер – наприклад, прицільні атаки на об'єкти інфраструктури однією зі сторін конфлікту, так і випадковий, коли важке озброєння із широкою зоною ураження використовується поблизу таких об'єктів. Окрім цього, часто об'єкти критичної інфраструктури використовуються неправомірно у своїх військових стратегіях, блокуючи доступ до базових послуг для цивільного населення з метою посилення тиску на Україну (наприклад військове захоплення Запорізької АЕС).

Енергетична система України зазнала безпрецедентної деградації внаслідок комбінованих ударів (рис. 2). Якщо у 2022 році основний збиток було завдано тепловій генерації (уражено кілька блоків ТЕС), то у 2024-2025 роках вектор атак змістився на об'єкти розподілу та передачі електроенергії. Прямі збитки ТЕС та ТЕЦ оцінюються у 2,5 млрд та 320 млн доларів відповідно, що становить критичну частку від загальних втрат енергосектору (7,4 млрд доларів) [8].

Рисунок 2 – Динаміка інтенсивності атак на критичну інфраструктуру 2022-2025 рр. [9]

Рисунок демонструє чітку тенденцію переходу ворога від ракетного терору до стратегії виснаження за допомогою БпЛА. Видно, що інтенсивність ударів по критичній інфраструктурі у 2025 році (понад 830 атак сумарно) перевищує показники попередніх років.

Додатково слід зазначити, що Міжнародне гуманітарне право забороняє використання голоду як зброї війни. Це пряма заборона нападів на об'єкти, що необхідні для життєзабезпечення цивільного населення. До таких об'єктів належать запаси продуктів харчування, сільськогосподарські угіддя, пасовища з худобою, водозабірні споруди та ін. Заборони також охоплюють енергетичну інфраструктуру, яка суттєво впливає на функціонування інших критично важливих систем. Весь цей комплекс норм спрямований на мінімізацію шкоди для цивільного населення та збереження його основних засобів існування навіть у найскладніших умовах війни.

Аналіз останніх досліджень та публікацій. У вітчизняних та закордонних наукових працях розглядаються різні методи до забезпечення охорони об'єктів критичної інфраструктури.

Українські науковці зосереджують увагу на особливостях захисту важливих

об'єктів, аналіз впливу воєнних загроз на інфраструктуру, а також питання організаційного забезпечення безпеки [10-13]. Західні науковці приділяють значну увагу адаптації об’єктів до гібридних загроз, використанню розумних систем моніторингу та співпраці державного й приватного сектору у сфері безпеки [14].

Аналіз останніх досліджень та публікацій свідчить про те, що наукова думка у сфері захисту об’єктів критичної інфраструктури України трансформувалася від вивчення теоретичних засад безпеки до розробки прикладних механізмів гібридної стійкості. Сучасні дослідження підкреслюють, що характер загроз для об’єктів критичної інфраструктури має комплексний та гібридний вимір, що вимагає оновлення нормативної бази. Наукова праця [15] наголошує на проблемах та перспективах впровадження системного захисту об’єктів критичної інфраструктури в Україні, розглядаючи їх як фундамент національної безпеки. Наукові статті [16-17] аналізують організаційно-нормативні перепони, пропонуючи перехід до превентивного управління ризиками замість реактивного відновлення. Науковці [18], акцентують увагу на важливості підготовки фахових кадрів, здатних оперувати системами захисту в умовах екстремальних навантажень воєнного стану.

Також вчені [19] досліджують зарубіжний досвід, вказуючи на необхідність адаптації кращих практик НАТО щодо будівництва заглиблених (підземних) пунктів керування та енергетичних сховищ. Також науковці [20] проводять інформаційний аналіз систем захисту, обґрунтовуючи доцільність впровадження багаторівневих інженерних споруд (габіонів, антидронових сіток, тощо).

Аналіз літературних джерел показує, що найбільш актуальним завданням сучасної науки є конвергенція фізичного та кібернетичного захисту. Україна демонструє унікальний досвід оперативної адаптації енергосистеми, що стає об’єктом прискіпливого вивчення західними фахівцями. Водночас, в умовах війни треба поєднувати ці методи і вдосконалювати або створювати нові методи та розробляти національні стратегії, що беруть до уваги специфіку реалій війни.

Формулювання мети статті (постановка завдання). Метою цієї статті є аналіз сучасного стану захисту об’єктів енергетичної інфраструктури України в умовах воєнного стану (зокрема в розрізі пожежної безпеки та цивільного захисту) та розробка ефективних заходів її удосконалення.

Методи досліджень. У процесі підготовки наукової статті використано комплексний методологічний апарат, що відповідає сучасним вимогам до досліджень у сфері цивільного захисту. Застосовано метод системного аналізу для оцінки поточного стану енергетичної та пожежної безпеки; статистичний метод для обробки та візуалізації емпіричних даних щодо інтенсивності атак (за період 2022-2025 рр.); концептуальне моделювання для розробки ієрархічної трирівневої моделі управління безпекою, а також метод структурно-функціонального аналізу для доведення необхідності превентивної взаємодії операторів інфраструктури з підрозділами ДСНС України. Отримані результати аргументовано за допомогою дедуктивного методу, де від загальної статистики уражень виведено конкретні вимоги до протоколів безпеки.

Завдання дослідження – оцінити та проаналізувати забезпечення безпеки та стійкості об’єктів енергетичної інфраструктури та визначити ефективні заходи щодо їх удосконаленням.

Виклад основного матеріалу. В умовах збройного конфлікту критична інфраструктура стає однією з головних цілей атак, оскільки її руйнування може суттєво послабити економічний та оборонний потенціал держави, спричинити гуманітарну кризу та погіршити моральний стан населення.

Основними загрозами для критичної інфраструктури в умовах воєнних дій є: фізичні атаки, зокрема ракетні удари, авіаційні бомбардування, артилерійські

обстріли стратегічних об'єктів; кібернетичні загрози, які включають атаки на урядові установи, фінансовий сектор, телекомунікаційні компанії, підприємства енергетики та транспорту; гібридні методи дестабілізації, до яких належать інформаційні операції, диверсійні дії, економічні санкції, а також використання агентів впливу для поширення паніки та хаосу серед населення.

Однією з найсерйозніших загроз для критичної інфраструктури є ракетні удари та авіаційні бомбардування, які можуть знищити енергетичні об'єкти, транспортні вузли, комунікаційні центри, військові бази та промислові підприємства. Наприклад, атаки на електростанції можуть спричинити масштабні перебої в електропостачанні, що негативно вплине на роботу лікарень, підприємств харчової промисловості, систем водопостачання та опалення, тощо.

При оцінці втрат у галузі електроенергії використовувались прямі та непрямі засоби для обчислення витрат на втрачені та пошкоджені об'єкти. Вартість пошкоджених суб'єктів визначається на основі первинного транспортування основних активів, вартість ремонту, вартість відновлення, тощо.

Основні дані про втрати енергії, надані Міністерство розвитку громад, територій та інфраструктури України та Міністерством енергетики України. Особистий підхід, який використовується для оцінки втрат у надані відповідно до інформації з відкритих джерел, власників та лідерів бізнесу, центральних організацій управління. Збір даних про втрату енергетичних об'єктів здійснювався обома загальними джерелами через ризик високого розповсюдження інформації детального пошкодження важливої інфраструктури внаслідок військової агресії рф.

Поточна оцінка дуже складна через відсутність детальної інформації. З жовтня 2022 року по лютий 2023 року військові рф здійснювали наймасованіші ракетні атаки на об'єкти, що забезпечують виробництво, передачу та розповсюдження електроенергії (рис. 3).

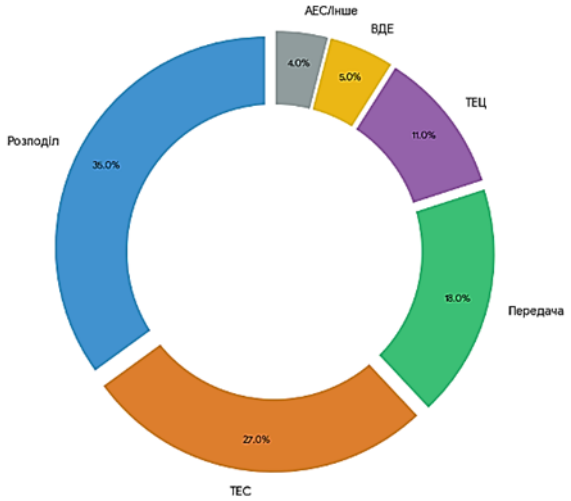

Рисунок 3 – Прямі інфраструктурні збитки об'єктам електроенергетики

Значні збитки припадають на великі об'єкти генерації електрики. В результаті одного з масованих обстрілів під час опалювально-зимового періоду 2022-2023 років, за словами Прем'єр-міністра України, було пошкоджено 9 блоків теплових електростанцій, причому щонайменше один з них був повністю знищений в наслідок прямого влучення. Загалом, оцінюються поточні прямі збитки теплової електрогенерації на рівні 2,5 млрд доларів для ТЕС та 320 млн доларів для ТЕЦ.

Окремою загрозою, яка прямо корелює з фізичними атаками, є критичне пожежне навантаження. Знищення трансформаторів супроводжується витоком 100 тис. т горючої рідини, що створює екстремальні умови для роботи пожежно-рятувальних підрозділів.

Дороги, мости, залізничні вузли та порти є ключовими елементами транспортної інфраструктури, які забезпечують логістичні операції, військові перевезення та гуманітарні місії. Їх руйнування значно ускладнює пересування військових сил, постачання продовольства, медикаментів та пального.

Наприклад, воєнний злочин та потенційно акт екоциду рф – підрив Каховської ГЕС у 2023 році спричинив масштабну екологічну та гуманітарну

катастрофу, підтоплення населених пунктів і загибель людей [21].

Окрім фізичних нападів, критична інфраструктура зазнає кібернетичних загроз. Ці атаки здатні вивести з ладу державні реєстри, фінансові системи, мережі енергопостачання та телекомунікаційні вузли. Злом інформаційних баз державних установ може спричинити витік конфіденційних відомостей, що послаблює обороноздатність держави.

Наприклад, у 2017 році кібератака вразила українські державні структури, банки та аеропорти, паралізувавши їхню діяльність. Атаки на системи керування енергомережами можуть спричинити аварійні вимкнення електроенергії. Так, у 2015 році хакерська атака на українські енергокомпанії залишила без світла понад 200 тисяч осіб. Гібридна війна поєднує фізичні та кібернетичні атаки з інформаційними маніпуляціями, економічним тиском та використанням агентів впливу.

З 2014 року на сході України розпочалася антитерористична операція, яка в 2022 році переросла у повномасштабну війну. Внаслідок цього частина областей опинилася під окупацією. Деякі території вдалося звільнити, проте значна частина залишається під контролем агресора. Водночас щоденні обстріли охоплюють всю країну, використовуючи різні види озброєння: ракети, безпілотники, авіабомби, балістичні ракети тощо. Це спричиняє не лише матеріальні, екологічні та фінансові втрати, а й головну трагедію війни – загибель мирного населення, навіть у віддалених від фронту містах. Обстріли завдають ударів по житлових будинках, школах, лікарнях, підприємствах та критично важливих об’єктах інфраструктури.

У 2022 році ворог здійснив численні обстріли критичної інфраструктури та енергетичних об’єктів України, що призвело до масштабних пожеж, руйнувань і серйозних проблем в енергосистемі країни. Крім того, з 10 жовтня 2022 року почалися регулярні удари по об’єктам енергетики із застосуванням крилатих ракет (Х-101, «Калібр»), що спричинило масове відключення світла та ускладнення в роботі критичної інфраструктури. За весь 2022 рік було зафіксовано 11 масованих ракетних атак на енергосистему, в ході яких було випущено понад 1400 ракет різних типів.

Загалом у 2022 році було знищено або пошкоджено понад 700 життєво важливих споруд, серед яких аеропорти, мости, нафтобази, трансформаторні підстанції та електростанції та ін. Найбільше руйнувань відзначили такі області, як Дніпропетровська, Львівська, Вінницька, Запорізька, Івано-Франківська, Київська та Харківська. Унаслідок цих обстрілів енергосистема втратила значну частину потужностей. Мета цих атак – виведення з ладу енергетичної системи і психологічний хаос населення України, що послаблює обороноздатність України та її волю до захисту. На рис. 4 зображено обстріли енергетичної інфраструктури України у 2022 році.

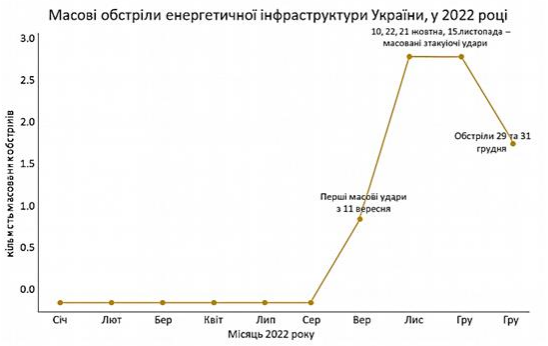

Рисунок 4 – Обстріли енергетичної інфраструктури України у 2022 році

У 2023 році рф продовжувала масовані обстріли критичної інфраструктури, зокрема енергетичних об’єктів України, завдаючи багатьох руйнувань та масштабних втрат енергосистеми. За підрахунками, у перші місяці 2023 року за період з жовтня 2022-го до лютого 2023 року було понад 220 ударів по 110 об’єктах критичної та цивільної інфраструктури.

У лютому 2023 року відбулися численні масовані ракетні атаки, зокрема 67 запусків крилатих ракет по об’єктам

критичної інфраструктури, що спричинило одночасні масштабні відключення світу вперше в історії. Також окупаційні війська рф почали застосовувати комбінаційні атаки, а саме додатково застосовуючи балістичні ракети, ракети Х-22, Х-47 «Кинджал», а також ударні БПЛА типу Shahed-136/131.

Особливо потужні атаки були наприкінці 2023 року. У листопаді станції «Зміївська» та «Трипільська» теплоелектростанції (ТЕС) «Центренерго» знову були знищені російськими ударами, що призвело до повної зупинки генерації в Харківській та Київській області. Внаслідок цього «Укренерго» було вимушено запровадити аварійні та погодні графіки відключення електропостачання по всій країні. Застосовувалась велика кількість ракет і безліч дронів, які одночасно атакували відновлені після попередніх ударів по об'єктах електроенергії. За підсумками 2023 року прямі збитки енергетичного сектору України сягнули понад 16 млрд доларів. Найбільше постраждали об'єкти генерації електроенергії (8,5 млрд), магістральні лінії передачі (2,1 млрд) та нафтогазової інфраструктури (3,3 млрд). Загальні втрати включають також втрачений дохід від роботи енергетичних компаній, оцінений у понад 39 млрд доларів.

Отже, 2023 рік (рис. 5) характеризувався продовженням інтенсивних і системних атак на критичну інфраструктуру та енергетичні об'єкти, що викликало масштабні руйнування, складності з електропостачанням в Україні та величезні економічні втрати.

Рисунок 5 – Обстріли енергетичної інфраструктури України у 2023 році

У 2024 році обстріли критичної інфраструктури і енергетичних об'єктів України залишилися системними та надзвичайно інтенсивними. З 21 березня 2024 року агресор почав нові масовані удари по енергетичних об'єктах, які тривали протягом року. Серед пошкоджених об'єктів були підземне газове сховище, а також численні теплові електростанції (ТЕС) і гідроелектростанції (ГЕС) у різних регіонах України.

Протягом 2024 року було понад 1100 запусків ракет, зокрема 17 днів інтенсивних обстрілів із понад 80 ракетами за добу. Ворог активно застосовував ракети різного типу, зокрема з комплексів С-300, а також ударні безпілотники. Через ці дії понад 40% генеруючих потужностей енергосистеми було пошкоджено чи знищено.

Наприкінці 2024 року, агресор завдав масованого комбінованого ракетно-дронового удару по паливно-енергетичному сектору із застосуванням ракет різних типів та ударних безпілотників, що спричинило значні пошкодження та масштабні відключення електропостачання у багатьох випадках (рис. 6). Обстріли призвели до масштабних пожеж, руйнувань інфраструктури, відключень електрики, перебоїв із комунальними послугами та роботи транспорту. Зусилля українських сил ППО дозволили збивати значну частину ракети, але значні втрати в енергетиці та критичній інфраструктурі мали місце. Були пошкоджені об'єкти у Львівській, Київській, Харківській, Дніпропетровській, Запорізькій, Вінницькій та інших областях.

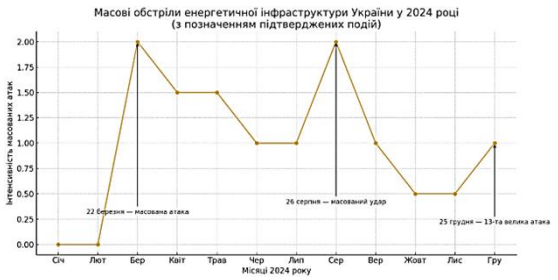

Рисунок 6 – Обстріли енергетичної інфраструктури України у 2024 році

У 2025 році обстріли критичної інфраструктури та енергетичних об'єктів

України залишилися масштабними та системними. Внаслідок цієї атаки пошкоджено чи знищено чисельність енергетичних об’єктів у Київській, Харківській, Одеській, Запорізькій, Кіровоградській, Сумській. У жовтні 2025 року під удари потрапили три важливі енергооб’єкти в Чернігівській області, що призвело до масштабних перебоїв із електропостачанням і газопостачанням в регіоні (рис. 7). Для відновлення пошкодженої інфраструктури Україна співпрацює з міжнародними партнерами, для залучення фінансової допомоги на відновлення енергетичних об’єктів і закупівлю палива. Попри серйозні удари, Збройні сили та ППО України з підтримки міжнародних партнерів продовжують оборону та роботу з відновлення енергосистем.

Рисунок 7 – Обстріли енергетичної інфраструктури України у 2025 році

Відповідно до статистики за період повномасштабного вторгнення, ворог завдав щонайменше понад 400 ударів по військових об’єктах, понад 3600 – по цивільних, а також уразив не менше 3000 по об’єктам критичної інфраструктури.

Для дієвого захисту варто впроваджувати комплексний метод. Цей підхід обґрунтовується неможливістю гарантувати 100% перехоплення засобів повітряного нападу. Значущі кроки для забезпечення стабільного захисту: посилення міцності інфраструктурних об'єктів та модернізація систем автоматичного пожежогасіння; формування підземних резервуарів для енергоносіїв; використання портативних генераторів.

Лише за умови злагоджених зусиль у цих площинах можливо зменшити небезпеки і гарантувати стійкість держави перед поточними проблемами, зокрема за умов військових дій, технічних нападів та стихійних лих.

Посилення безпеки об’єктів енергетики є невіддільною складовою загальної доктрини державності. На нашу думку є декілька значущих кроків для забезпечення стабільного захисту: посилення міцності інфраструктурних об'єктів: життєво важливі об’єкти, енергетичні установи, мережі водопостачання, летовища, медичні заклади та інші стратегічно важливі споруди, мають бути оснащені новітніми охоронними та захисними комплексами. Це включає не лише фізичні перепони, але й упровадження передових методів моніторингу, зокрема відеоспостереження, систем контролю входу, а також механізмів раннього оповіщення про небезпеки; формування підземних резервуарів для енергоносіїв: збереження енергетичних запасів є життєво необхідним для забезпечення сталої діяльності держави в умовах надзвичайних ситуацій.

Сучасні кіберзагрози можуть завдавати більш значної шкоди, ніж традиційні військові дії, тому не слід забувати, що впровадження сучасних заходів кіберзахисту на енергетичних об’єктах і в критичній інфраструктурі є ключовим елементом національної безпеки. Всі ключові інформаційні системи енергетичних підприємств та критичної інфраструктури мають бути захищені сучасними методами шифрування, що гарантують конфіденційність даних навіть у разі несанкціонованого доступу, а також необхідно впроваджувати системи моніторингу, які своєчасно виявляють і блокують кібератаки, запобігаючи їхньому негативному впливу на інфраструктуру та інформаційні ресурси.

Для забезпечення живучості енергосистеми аргументується необхідність впровадження чіткої ієрархії режимів функціонування [22-23]. Концептуальну модель системи «світлофорної індикації» представлено на рис. 8.

Рисунок 8 – Ієрархія режимів функціонування об'єктів критичної інфраструктури за принципом «світлофорної індикації»

Штатний режим характеризується станом гомеостазу системи, коли зовнішні та внутрішні загрози відсутні або знаходяться в межах допустимих значень (здійснення моніторингу та підтримання системної стійкості).

Режим готовності до надзвичайної ситуації ініціюється отриманням верифікованих розвідданих або прогнозних показників, що свідчать про ймовірну ескалацію небезпеки: кіберзагрози, тероризм, військовими діями, метеорологічні аномалії, тощо. Максимізація захисного потенціалу та підготовка ресурсів до потенційного переходу в активну фазу кризи.

Режим кризової ситуації передбачає стан системи після фактичної реалізації загрози (інциденту), що призвела до деструктивного впливу на життєво важливі функції та життєзабезпечення населення (локалізація наслідків, відновлення функціональності та запобігання системному колапсу).

Наукова аргументація цієї моделі полягає в тому, що аналіз наведених статистичних втрат доводить повну неспроможність традиційної системи реагування. Запропонована модель створює алгоритм превентивної дії. Штатний режим – гомеостаз, режим готовності до надзвичайної ситуації – ініціюється розвідданими, режим кризової ситуації – інцидент відбувся (локалізація, гасіння пожеж під прикриттям ППО та мобільних укриттів, відновлення). Така індикація дозволяє оптимізувати людський ресурс ДСНС України і мінімізувати втрати серед особового складу шляхом завчасного приведення у готовність.

На початку 2026 року ми бачимо, що агресор посилює обстріли об'єктів критичної інфраструктури, а саме об'єкти енергетики. Мета лишити населення України без тепла та світла (в результаті зниження температури повітря), порушення життєзабезпечення, залякування населення та міжнародних партнерів, знищення держави України. Національна безпека в енергетичному секторі – це не тільки стратегічне планування, а і реальна готовність до швидких і ефективних дій, а також активна участь у міжнародній співпраці заради захисту демократичних цінностей і стабільності на глобальному рівні.

Висновки та напрями подальших досліджень. Захист об'єктів енергетичної структури в умовах воєнного стану є одним із найважливіших елементів забезпечення національної безпеки та економічної стабільності України. Враховуючи значні виклики, пов'язані з повномасштабною військовою агресією, руйнування чи виведення з ладу об'єктів енергетики може спричинити масштабні збої в енергопостачанні, що безпосередньо впливає на життєздатність інших критичних систем – транспорту, комунікацій, охорони здоров'я та оборони. Посилення фізичної захищеності цих об'єктів, розвиток автономних та резервних джерел живлення, впровадження сучасних технологій моніторингу та кібербезпеки є надзвичайно актуальними завданнями. Важливим також є підвищення рівня організаційної готовності до кризових ситуацій через створення координаційних центрів, проведення навчань та своєчасне оновлення нормативно-правової бази.

За умов чинного воєнного стану в Україні захист енергетичної інфраструктури – життєво важливого компонента національної безпеки та життєво важливого джерела нації став ключовим підсумком. Військова агресія рф,

спрямована на цілеспрямований саботаж об’єктів української енергетичної системи, включаючи лінії електропередачі, підстанції, теплові електростанції та гідроелектростанції, серйозно порушила стабільність електро- та теплопостачання та створила гуманітарні та соціально-економічні ризики (наприклад, зимові перебої з опаленням, відключення критичної інфраструктури).

Пропонування рекомендацій щодо підвищення стійкості енергетичної системи, включаючи диверсифікацію та децентралізацію джерел енергії, модернізацію інфраструктури та інтеграцію з європейською енергетичною мережею. Створення інституційних механізмів координації державних, приватних та міжнародних суб’єктів для швидкого реагування, відновлення та захисту енергетичних об'єктів. Додатково міжнародна співпраця у сфері безпеки енергетичної інфраструктури сприяє впровадженню передових технологічних рішень і обміну передовим досвідом.

Подальші дослідження мають зосередитися на розробці інноваційних тактик пожежогасіння на об'єктах енергетики під час загрози повторних ракетних ударів.

Тому, питання захисту енергетичної інфраструктури в Україні в умовах воєнного стану є особливим внеском і вимагає системного та наукового підходу, що забезпечує технологічний, організаційний та стратегічний рівні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бєлай С. В., Євтушенко І. В., Мацюк В. В. Теоретико-методологічні засади підготовки кадрів у сфері захисту критичної інфраструктури України. *Вісник національного університету цивільного захисту України. Серія Державне управління*. 2021. № 2(15). С. 342-350. https://doi.org/10.52363/2414-5866-2021-2-40.
2. Скіцько О., Ширшов Р. Система управління інформаційною безпекою як інструмент підвищення захисту та ефективності об’єктів критичної інфраструктури. *Міжнародний науковий журнал інженерії та сільського господарства*. 2023. № 2(6). С. 12-22. https://doi.org/10.46299/j.isjea.20230206.02.
3. Oleksiuk, V. (2025). Green Energy as a tool for resilience and recovery of Ukraine during the war and in the post-war period. *Modern Economics*, *50*(1), 136-143. https://doi.org/10.31521/modecon.v50(2025)-18.
4. Братель С. Г. Досвід зарубіжних країн у сфері забезпечення безпеки об’єктів критичної інфраструктури. *Південноукраїнський правничий часопис*. 2023. № 3. С. 261-265. https://doi.org/10.32850/sulj.2023.3.41.
5. Umantsiv, Y., & Shkuropadska, D. (2023). National resilience of Ukraine under the martial law. *Scientia Fructuosa*, *151*(5), 4-19. https://doi.org/10.31617/1.2023(151)01.
6. Мельник Д. С. Побудова моделі загроз національній критичній інфраструктурі України як основа забезпечення її безпеки та стійкості. *Вісник Харківського національного університету внутрішніх справ*. 2024. № 1(104). С. 237-250. https://doi.org/10.32631/v.2024.1.20.
7. Статистика повітряних тривог. URL: https://air-alarms.in.ua/?from=2022-02-24&to=2026-01-01#statistic.
8. Яременко О. І., Страхніцький Я. О. Теоретико-методичні основи забезпечення системи захисту критичної інфраструктури держави. *Державне управління: удосконалення та розвиток*. 2022. № 1. https://doi.org/10.32702/2307-2156-2022.1.38.
9. Havrys, A., Yakovchuk, R., Pekarska, O., & Tur, N. (2024). Use of the computer modelling for the analysis of dangerous areas during flooding of territories. *Ecological Engineering & Environmental Technology*, *25*(4), 336-343. https://doi.org/10.12912/27197050/184265.
10. Гаврись А. П., Філіппова В. В., Тур Н. Ю. Інформаційний аналіз систем захисту об’єктів критичної інфраструктури в період дії воєнного стану. *Вісник Львівського державного університету безпеки життєдіяльності*. 2024. № 30. С. 173-187. https://doi.org/10.32447/20784643.30.2024.17.
11. Герасименко О. М. Загрози об’єктам критичної інфраструктури України в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету. Серія Право*. 2024. № 84(3). С. 257-263. https://doi.org/10.24144/2307-3322.2024.84.3.39.
12. Гора І. В., Батюк О. В. Окремі питання захисту об’єктів критичної інфраструктури: зарубіжний досвід. *Соціально-правові студії*. 2021. № 1(11). С. 132-139.
13. Кучма О. М., Котух Є. В. Критична інфраструктура та кіберзагрози: досягнення стратегічних цілей державного аудиту щодо кіберзахисту критичної інфраструктури. *Наукові перспективи*. 2023. № 10(40). С. 161-173. https://doi.org/10.52058/2708-7530-2023-10(40)-161-173.
14. Vhpiliarevych, V., Tocicka, J. W., & Szafrańska, K. (2023). Civil protection and protection of critical infrastructure in Ukraine during the conditions of the martial state. *Journal of Security and Sustainability Issues*, *13*(1), 265-272. https://doi.org/10.47459/jssi.2023.13.29.
15. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні: аналітична доповідь. Київ: НІСД, 2012. 96 с.
16. Мурасов Р., Нікітін А., Мещеряков І., Підгородецький М., Поплавець С. Удосконалення науково-методичного апарату для розрахунку ризиків виникнення та аналізу сценаріїв надзвичайних ситуацій на об’єктах критичної інфраструктури. *Соціальний розвиток і безпека*. 2024. № 14(1). С. 205-217. https://doi.org/10.33445/sds.2024.14.1.17.

17. Франчук В. І., Пригунов П. Я., Мельник С. І. Безпека об’єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. *Соціально-правові студії*. 2021. № 3(13). С. 142-148.
18. Іваницька О. М., Возненко О. М. Управління ризиками об’єктив критичної інфраструктури. *Фінанси України*. 2024. № 6. С. 93-107. https://doi.org/10.33763/finukr2024.06.093.
19. Bani-Meqdad, M. A. M., Senyk, P., Udod, M., Pylypenko, T., & Sylkin, O. (2024). Cyber-environment in the human rights system: Modern challenges to protect intellectual property law and ensure sustainable development of the region. *International Journal of Sustainable Development and Planning*, *19*(4), 1389-1396. https://doi.org/10.18280/ijsdp.190416.
20. Bohun, V. (2024). Assessing the impact of infrastructure damage on national investment attractiveness during martial law. *Pakistan Journal of Life and Social Sciences*, *22*(2), 10379-10385. https://doi.org/10.57239/pjlss-2024-22.2.00784.
21. Yakovliev, Y., Rogozhin, O., Stefanyshyn, D., Kreta, D., Anpilova, Y., & Myrontsov, M. (2024). Environmental and geological hazards after the explosion of the Kakhovka hydroelectric power plant and rehabilitation options. *Systems, Decision and Control in Energy VI*, 532-537. https://doi.org/10.1007/978-3-031-67091-6_25.
22. *Ukrainian energy sector evaluation and damage assessment - X*. (2023). Cooperation for Restoring the Ukrainian Energy Infrastructure project. https://www.energycharter.org/fileadmin/DocumentsMedia/Occasional/2023_05_24_UA_sectoral_evaluation_and_damage_assessment_Version_X_final.pdf.
23. 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.

REFERENCES

1. Bielai, S. V., Yevtushenko, I. V., & Matsiuk, V. V. (2021). Theoretical and methodological foundations of personnel training in the field of critical infrastructure protection in Ukraine. *Bulletin of the National University of Civil Protection of Ukraine. Public Administration Series*, *2*(15), 342-350. https://doi.org/10.52363/2414-5866-2021-2-40.
2. Skitsko, O., & Shyrshov, R. (2023). Information security management system as a tool for improving the protection and efficiency of critical infrastructure facilities. *International Scientific Journal of Engineering and Agriculture*, *2*(6), 12-22. https://doi.org/10.46299/j.isjea.20230206.02.
3. Oleksiuk, V. (2025). Green Energy as a tool for resilience and recovery of Ukraine during the war and in the post-war period. *Modern Economics*, *50*(1), 136-143. https://doi.org/10.31521/modecon.v50(2025)-18.
4. Bratel, S. G. (2023). Experience of foreign countries in the field of critical infrastructure security. *South Ukrainian Law Journal*, (3), 261-265. https://doi.org/10.32850/sulj.2023.3.41.
5. Umantsiv, Y., & Shkuropadska, D. (2023). National resilience of Ukraine under the martial law. *Scientia Fructuosa*, *151*(5), 4-19. https://doi.org/10.31617/1.2023(151)01.
6. Melnik, D. S. (2024). Building a model of threats to Ukraine's national critical infrastructure as a basis for ensuring its security and stability. *Bulletin of Kharkiv National University of Internal Affairs*, *1*(104), 237-250. https://doi.org/10.32631/v.2024.1.20.
7. *Air raid statistics*. (2026). https://air-alarms.in.ua/?from=2022-02-24&to=2026-01-01#statistic.
8. Yaremenko, O. I., & Strakhnitsky, Y. O. (2022). Theoretical and methodological foundations for ensuring the protection of the state's critical infrastructure. *Public Administration: Improvement and Development*, (1). https://doi.org/10.32702/2307-2156-2022.1.38.
9. Havrys, A., Yakovchuk, R., Pekarska, O., & Tur, N. (2024). Use of the computer modelling for the analysis of dangerous areas during flooding of territories. *Ecological Engineering & Environmental Technology*, *25*(4), 336-343. https://doi.org/10.12912/27197050/184265.
10. Havrys, A. P., Filippova, V. V., & Tur, N. Yu. (2024). Information analysis of critical infrastructure protection systems during martial law. *Bulletin of Lviv State University of Life Safety*, (30), 173-187. https://doi.org/10.32447/20784643.30.2024.17.
11. Gerasimenko, O. M. (2024). Threats to critical infrastructure facilities in Ukraine under martial law. *Scientific Bulletin of Uzhhorod National University. Law Series*, *84*(3), 257–263. https://doi.org/10.24144/2307-3322.2024.84.3.39.
12. Gora, I. V., & Batyuk, O. V. (2021). Selected issues of critical infrastructure protection: Foreign experience. *Social and Legal Studies*, (11), 132-139.
13. Kuchma, O. M., & Kotukh, Ye. V. (2023). Critical infrastructure and cyber threats: Achieving the strategic goals of state audit regarding cyber protection of critical infrastructure. *Scientific Perspectives*, *10*(40), 161-173. https://doi.org/10.52058/2708-7530-2023-10(40)-161-173.
14. Vhpiliarevych, V., Tocicka, J. W., & Szafrańska, K. (2023). Civil protection and protection of critical infrastructure in Ukraine during the conditions of the martial state. *Journal of Security and Sustainability Issues*, *13*(1), 265-272. https://doi.org/10.47459/jssi.2023.13.29.
15. Biryukov, D. S., & Kondratov, S. I. (2012). *Critical infrastructure protection: Problems and prospects for implementation in Ukraine: Analytical report*. NISD.
16. Murasov, R., Nikitin, A., Meshcheryakov, I., Pidgorodetsky, M., & Poplavets, S. (2024). Improving the scientific and methodological apparatus for calculating the risks of occurrence and analysing scenarios of emergency situations at critical infrastructure facilities. *Social Development and Security*, *14*(1), 205-217. https://doi.org/10.33445/sds.2024.14.1.17.
17. Franchuk, V. I., Prygunov, P. Ya., & Melnyk, S. I. (2021). Security of critical infrastructure facilities in Ukraine: Organisational and regulatory issues and approaches. *Social and Legal Studies*, (13), 142-148.
18. Ivanytska, O. M., & Voznenko, O. M. (2024). Risk management of critical infrastructure facilities. *Finance of Ukraine*, (6), 93-107. https://doi.org/10.33763/finukr2024.06.093.
19. Bani-Meqdad, M. A. M., Senyk, P., Udod, M., Pylypenko, T., & Sylkin, O. (2024). Cyber-environment in the human rights system: Modern challenges to protect intellectual property law and ensure sustainable development of the region. *International Journal of Sustainable Development and Planning*, *19*(4), 1389-1396. https://doi.org/10.18280/ijsdp.190416
20. Bohun, V. (2024). Assessing the impact of infrastructure damage on national investment attractiveness during martial law. *Pakistan Journal of Life and Social Sciences*, *22*(2), 10379-10385. https://doi.org/10.57239/pjlss-2024-22.2.00784.

21. Yakovliev, Y., Rogozhin, O., Stefanyshyn, D., Kreta, D., Anpilova, Y., & Myrontsov, M. (2024). Environmental and geological hazards after the explosion of the Kakhovka hydroelectric power plant and rehabilitation options. *Systems, Decision and Control in Energy VI*, 532-537. https://doi.org/10.1007/978-3-031-67091-6_25.
22. *Ukrainian energy sector evaluation and damage assessment - X*. (2023). Cooperation for Restoring the Ukrainian Energy Infrastructure project. https://www.energycharter.org/fileadmin/DocumentsMedia/Occasional/2023_05_24_UA_sectoral_evaluation_and_damage assessment Version X final.pdf.
23. *On critical infrastructure: Law of Ukraine No. 1882-IX*. (2021). https://zakon.rada.gov.ua/laws/show/1882-20#Text.

IMPROVING THE PROTECTION OF UKRAINE ENERGY INFRASTRUCTURE FACILITIES UNDER MARTIAL LAW

P. Bosak, M. Lavrivskyi*, *O. Liubovetskyi, H. Bosak, V. Vorobets

Lviv State University of Life Safety, Ukraine

KEYWORDS:

critical infrastructure facilities, civil protection, energy security, martial law, cyber threats, fire safety, resilience.

ABSTRACT

This article examines the crucial issue of ensuring the resilience and protection of Ukraine's energy infrastructure under martial law, particularly in the context of full-scale military aggression by an aggressor state. The energy sector is identified as the primary target of hostile attacks aimed at destabilising the national economy, defence capabilities and social services. The study provides a comprehensive analysis of the security status of Ukraine's energy system, highlighting the multidimensional nature of contemporary threats. These include direct physical destruction via missile and drone strikes, the outbreak of large-scale fires in oil-filled equipment, large-scale cyberattacks on control systems, and hybrid methods of destabilisation. The study's methodology employs a comprehensive approach combining statistical analysis of attack patterns, comparative analysis of threat types, and conceptual modelling. The authors analysed statistical data on infrastructure losses for the period 2022–2025. The study reveals a shift in the aggressor's tactics: from targeting thermal power stations in 2022 to focusing on electricity distribution and transmission networks in 2024–2025. It is noted that direct losses to the energy sector have reached a critical level, estimated at billions of dollars, requiring immediate strategic countermeasures in the field of civil protection. The key theoretical contribution of this article is the development and scientific justification of a hierarchical three-level security management model based on the 'traffic light' principle. This model allows for the application of differentiated response protocols depending on the threat level to optimise the operations of the State Emergency Service of Ukraine. The 'green level' (normal mode) corresponds to a state of system homeostasis, where threats are absent or within acceptable limits, and focuses on monitoring. The 'Yellow Level' (standby mode) is initiated upon receipt of verified information about a potential escalation (e.g. cyber threats, meteorological anomalies or military manoeuvres). The 'Red Level' (crisis mode) is activated following an incident to contain damage, extinguish fires, prevent system collapse and ensure the survival of vital functions. The article argues that, to ensure long-term resilience, a transition is required from the vulnerable, centralised architecture of the Soviet era to a flexible, decentralised network. The proposed set of measures includes the construction of underground energy storage facilities, the installation of modern automatic fire-extinguishing systems, the deployment of autonomous power supply systems (microgrids) and the convergence of physical protection (engineering barriers, anti-drone nets) with integrated cyber protection of information systems. The implementation of these measures aims to minimise response times to emergencies and safeguard the civilian population's life-support systems during military operations.