Недоліки стратегічного форсайту та вразливість енергетичної безпеки України в умовах війни: проблеми прогнозування та стійкості

Shortcomings of Strategic Foresight and Vulnerability of Ukraine's Energy Security in Wartime: Problems of Forecasting and Resilience

Юрій Клят [A]
Corresponding author: кандидат технічних наук, доцент начальник Центрального науково-дослідного інституту, e-mail: klyatt@ukr.net, ORCID ID: https://orcid.org/0000-0002-8267-3748

Володимир Гурковський [A]
Доктор наук з держ .упр. професор, начальник відділу, e-mail: volodymyr.gurkovskyi@gmail.com; ORCID ID: https://orcid.org/0000-0003-2021-5204

Олександр Войтко [B]
доктор військових наук, доцент, начальник інституту стратегічних комунікацій, e-mail: o.voytko@ukr.net, ORCID ID: https://orcid.org/0000-0002-4610-4476

Марія Ярмольчик [C]
доктор філософії, начальник науково-дослідної лабораторії, e-mail: LinkinFan357@ukr.net, ORCID ID: https://orcid.org/0000-0001-9917-0189

Андрій Захаржевський [B]
кандидат технічних наук, начальник кафедри територіальної оборони, e-mail: a.zakharzhevskyi12@gmail.com, ORCID ID: https://orcid.org/0000-0001-7019-9949

Володимир Рахімов [B]
доктор філософії заступник начальника інституту стратегічних комунікацій, e-mail: rakhimov@edu.nuou.org.ua, ORCID ID: https://orcid.org/0000-0001-9868-986X

Yuriy Klyat [A]
Corresponding author: Candidate of Technical Sciences, Associate Professor, Head of the Central Research Institute, e-mail: klyatt@ukr.net, ORCID ID: https://orcid.org/0000-0002-8267-3748

Volodymyr Gurkovskyi [A]
Doctor of Public Administration Professor, head of Department, e-mail: volodymyr.gurkovskyi@gmail.com; ORCID ID: https://orcid.org/0000-0003-2021-5204

Oleksandr Voitko [B]
Doctor of Military Sciences, Associate Professor, Head of the Institute of Strategic Communications, e-mail: o.voytko@ukr.net, ORCID ID: https://orcid.org/0000-0002-4610-4476

Mariia Yarmolchyk [C]
Doctor of Philosophy, head of the research laboratory, e-mail: LinkinFan357@ukr.net, ORCID ID: https://orcid.org/0000-0001-9917-0189

Andrii Zakharzhevskyi [B]
Candidate of Technical Sciences, Head of the Department of Territorial Defense, e-mail: a.zakharzhevskyi12@gmail.com, ORCID ID: https://orcid.org/0000-0001-7019-9949

Volodymyr Rakhimov [B]
PhD in Military Sciences Deputy Head of the Institute of Strategic Communications, e-mail: rakhimov@edu.nuou.org.ua, ORCID ID: https://orcid.org/0000-0001-9868-986X

[A] Центральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна
[B] Національний університет оборони України, м. Київ, Україна
[C] Кафедра військової підготовки Державного університету "Київський авіаційний університет", м. Київ, Україна

[A] Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine
[B] National Defense University of Ukraine, Kyiv, Ukraine
[C] Department of Military Training, State University "Kyiv Aviation University", Kyiv, Ukraine

Received: February 15, 2026 | Revised: February 24, 2026 | Accepted: February 28, 2026

DOI: https://doi.org/10.33445/sds.2026.16.1.2

Мета роботи. Визначення причин провалу реалізації стратегічного форсайту у сфері енергетичної безпеки України в умовах повномасштабної війни та обґрунтування управлінської моделі, здатної забезпечити трансляцію форсайт-сценаріїв у обов'язкові інфраструктурні та політичні рішення.

Метод дослідження. Міждисциплінарний підхід, що поєднує інституційно-аналітичний метод, сценарний аналіз, порівняльний аналіз державної політики та огляд літератури; використано емпіричні дані з відкритих джерел, медіа та міжнародних звітів для зіставлення прогнозів з реальними подіями 2022–2026 рр.

Результати дослідження. Встановлено системний розрив між форсайтом і управлінськими рішеннями, зумовлений інституційною інерцією, монополізацією енергосектору та відсутністю превентивних заходів; запропоновано модель "форсайт → управлінські рішення → інфраструктура" з рекомендаціями щодо децентралізації, підземного розміщення об'єктів та інституціоналізації форсайту.

Теоретична цінність дослідження. Дослідження заповнює

Purpose. To identify the reasons for the failure of implementing strategic foresight in Ukraine's energy security sector under full-scale war conditions and to substantiate a management model capable of translating foresight scenarios into mandatory infrastructure and political decisions.

Method. Interdisciplinary approach combining institutional-analytical method, scenario analysis, comparative policy analysis, and literature review; empirical data from open sources, media, and international reports used to compare forecasts with actual events from 2022–2026.

Findings. Identified a systemic gap between foresight and management decisions due to institutional inertia, energy sector monopolization, and lack of preventive measures; proposed a "foresight → management decisions → infrastructure" model with recommendations for decentralization, underground placement of facilities, and institutionalization of foresight.

Theoretical Implications. The study fills gaps in analyzing the translation

прогалини в аналізі трансляції форсайту в управлінські рішення, інтегруючи концепцію “wicked problems” у контекст енергетичної безпеки; розкриває роль монополії як безпекового ризику та обґрунтовує форсайт як обов’язковий елемент державного управління в умовах війни.

Тип статті. Наукова стаття (аналітична, прикладна).

of foresight into management decisions, integrating the “wicked problems” concept into energy security context; reveals monopoly as a security risk and substantiates foresight as a mandatory element of public administration in wartime conditions.

Papertype. Scientific article (analytical, applied).

Ключові слова: стратегічний форсайт, енергетична безпека, державне управління, вразливість інфраструктури, війна, децентралізація, монополія.

Key words: Strategic Foresight, Energy Security, Public Administration, Infrastructure Vulnerability, War, Decentralization, Monopoly.

Вступ

Повномасштабна війна російської федерації проти України радикально змінила уявлення про характер сучасних загроз. Одним із ключових напрямів агресії стали системні удари по критичній інфраструктурі, насамперед по енергетичному сектору. Без стабільного електропостачання зупиняється економіка, ускладнюється функціонування органів державної влади та системи оборони, а також порушується повсякденне життя населення, особливо у великих містах.

Станом на кінець зими 2025–2026 років Україна переживає, ймовірно, найгострішу енергетичну кризу за весь період повномасштабної війни. Починаючи з жовтня 2025 року російські атаки пошкодили приблизно 8,5 ГВт генеруючих потужностей, переважно теплоелектростанцій і гідроелектростанцій. Для компенсації втрат Україна була змушена імпортувати рекордні обсяги електроенергії з європейських країн — у пікові періоди до 1,9 ГВт. Зокрема, у січні 2026 року імпорт досяг найвищого рівня за весь період війни, що підтверджується даними аналітичних агентств, зокрема ExPro. Це свідчить про те, що енергосистема функціонує в умовах граничного навантаження, і кожна нова хвиля атак здатна суттєво погіршити її стійкість.

Водночас важливо підкреслити, що такі атаки не були несподіваними. Починаючи з перших місяців 2022 року аналітичні центри, міжнародні організації та українські експерти неодноразово попереджали про вразливість централізованої енергосистеми України. Її архітектура — з розгалуженою мережею надземних ліній електропередачі, великими вузловими підстанціями напругою 750 кВ та атомними електростанціями, інтегрованими в єдину мережу — об’єктивно створює зручну ціль для стратегії війни на виснаження. Відповідні оцінки містилися у звітах таких організацій, як RAND, International Energy Agency та NATO Energy Security Centre of Excellence. Подібні висновки лунали також у публічному просторі: зокрема, у матеріалах BBC Україна зазначалося, що удари по енергетичній інфраструктурі були прогнозованими, проте підготовка до них відбувалася із запізненням і здебільшого мала реактивний характер [1].

У цьому контексті постає ключове дослідницьке питання: чому наявність прогнозів, аналітичних оцінок і навіть певних ресурсів не трансформувалася у належний рівень готовності? Іншими словами, чому стратегічний форсайт — інструмент, призначений для ідентифікації майбутніх загроз і трансформації їх у практичні управлінські рішення — не забезпечив очікуваного ефекту?

Ймовірно, проблема полягає не стільки у дефіциті інформації чи масштабах руйнувань (які, безумовно, є значними), скільки у глибших управлінських та інституційних чинниках. Насамперед йдеться про відсутність заздалегідь сформованої стійкої моделі енергозабезпечення, зокрема з елементами децентралізації. Навіть у випадках, коли фінансування виділялося, заходи із захисту об’єктів, створення резервних потужностей або впровадження альтернативних схем енергопостачання часто здійснювалися фрагментарно й несистемно, вже в умовах кризи [1; 12]. У результаті реактивна логіка управління переважала над превентивною.

Таким чином, спостерігається суттєвий розрив між прогнозованістю загроз і реальними управлінськими рішеннями. Удари по підстанціях та вузлах передачі електроенергії не є нетиповими або несподіваними явищами — вони логічно випливають із характеру сучасної війни та неодноразово описувалися в аналітичних документах. Проте архітектура енергосистеми принципово не змінилася: централізований характер управління зберігся, монопольні елементи у сфері передачі та диспетчеризації залишилися, а питання підземного або розосередженого розміщення критичних об'єктів так і не стало пріоритетом. Це свідчить про наявність не лише технічних, а й інституційних та політичних обмежень, пов'язаних із розподілом впливу та інтересів у енергетичному секторі.

З огляду на це метою статті є не лише опис наявних проблем, а й аналіз їхніх причин через призму стратегічного форсайту як інструменту державного управління. Особлива увага приділяється питанню, яким чином цей інструмент може бути інституціоналізований таким чином, щоб сценарії загроз трансформувалися не лише у аналітичні звіти, а й у конкретні інфраструктурні та регуляторні рішення.

Огляд літератури

У звітах OECD стратегічний форсайт розглядається як інструмент підвищення спроможності держави діяти в умовах невизначеності за умови його інтеграції у процеси ухвалення рішень і бюджетування [5]. UNDP дотримується подібного підходу, трактуючи форсайт передусім як механізм управління ризиками, а не лише як інструмент прогнозування [6].

Аналітичні звіти International Energy Agency (IEA**)** зосереджуються на структурній вразливості централізованих енергосистем та обґрунтовують економічну доцільність превентивних інвестицій у підвищення їхньої стійкості порівняно з витратами на відновлення після руйнувань [2]. RAND Corporation вводить поняття "передбачуваної вразливості", підкреслюючи, що атаки на критичну інфраструктуру рідко є несподіваними. Водночас у цих роботах інституційні причини управлінської бездіяльності аналізуються лише фрагментарно [4].

У публікаціях NATO Energy Security Centre of Excellence основна увага приділяється питанням фізичного захисту енергетичних об'єктів і зменшенню залежності енергосистем від надземних елементів мережі [11]. Дослідження European Commission Joint Research Centre демонструють ефективність підземного розміщення міських та енергетичних мереж, однак майже не розглядають політичні та регуляторні бар'єри впровадження таких рішень [10].

Матеріали OECD та World Bank, присвячені конкуренції в мережевих галузях, свідчать, що монополізовані структури можуть знижувати адаптивність інфраструктурних систем [3; 8]. Водночас зв'язок між монополією та національною безпекою в умовах воєнного конфлікту у цих дослідженнях залишається недостатньо розкритим.

Вітчизняні медіапублікації дозволяють зафіксувати емпіричні прояви цієї проблеми. Так, у матеріалі BBC News Україна зазначається, що підготовка до масових блекаутів мала запізнілий і переважно реактивний характер, а відповідальність за резервне енергозабезпечення значною мірою була перекладена на населення та бізнес [1].

Додатково у публікації видання ZN.UA наведено критичну оцінку стану захисту об'єктів критичної інфраструктури на найвищому політичному рівні. Зокрема, наголошується, що навіть сучасні системи протиповітряної оборони не забезпечують повного захисту від дронових атак, а фізичний захист об'єктів залишається недостатнім [12]. Цей матеріал опосередковано підтверджує, що проблема полягає не лише у наявності або відсутності засобів протиповітряної оборони, а й у браку комплексної інфраструктурної стратегії.

Проведений огляд літератури дозволив виявити кілька дослідницьких прогалин, які намагається заповнити це дослідження:

- недостатня увага до аналізу причин, через які результати стратегічного форсайту не трансформуються в обов'язкові управлінські рішення (так званий *implementation gap*);

- обмежене трактування монополії переважно як економічного, а не безпекового ризику;
- технократичний характер обговорення підземної та децентралізованої інфраструктури (зокрема у дослідженнях EIB і JRC) без належного аналізу політичних та регуляторних бар'єрів;
- недостатнє використання досвіду російсько-української війни 2022–2026 років як повноцінного емпіричного матеріалу для розвитку теоретичних підходів.

Саме ці прогалини визначають дослідницьку нішу статті. Робота не претендує на формування завершеної теоретичної моделі, а радше є спробою поєднати емпіричний досвід війни з наявними теоретичними підходами для пояснення того, чому знання про потенційні загрози не завжди трансформується у практичні управлінські дії.

Використані джерела мають різну аналітичну вагу. Публікації OECD і CSIS застосовано як базові для розуміння стратегічного форсайту як інструменту державного управління; матеріали RAND і NATO ENSEC COE — для аналізу сценаріїв воєнних загроз; дослідження, опубліковані у Central European Journal of International and Security Studies, — для обґрунтування зв'язку між монополізацією інфраструктури та безпековими ризиками. Інші джерела (зокрема окремі звіти IEA та World Bank) використовуються переважно як емпіричні ілюстрації.

Метою дослідження є визначення причин, через які стратегічний форсайт у сфері енергетичної безпеки не забезпечив належного практичного ефекту в умовах повномасштабної війни, а також обґрунтування моделі управління, за якої форсайт-сценарії могли б ставати обов'язковими орієнтирами для інфраструктурних та політичних рішень. Чи є така модель принципово можливою — питання відкрите. Проте без спроби зрозуміти природу розриву між прогнозуванням і дією існує ризик повторення одного й того самого циклу: прогноз → атака → відновлення → новий прогноз.

Методологія дослідження

Методологія цього дослідження не претендує на чистоту одного підходу. Навпаки, вона свідомо має міждисциплінарний характер, оскільки проблема, що розглядається, не може бути повноцінно пояснена в межах однієї наукової дисципліни. У роботі поєднано елементи державного управління (policy analysis, institutionalism), досліджень у сфері національної безпеки (security studies з акцентом на critical infrastructure) та стратегічного планування (foresight як інструмент формування управлінських рішень, а не лише як метод прогнозування).

Ключовим аналітичним підходом виступає інституційно-аналітична перспектива: енергетична інфраструктура розглядається не лише як сукупність технічних об'єктів, а як результат – і водночас чинник – управлінських рішень, регуляторних обмежень, а також розподілу повноважень між державними інституціями та групами інтересів.

Сценарний аналіз застосовано для зіставлення прогнозів, сформульованих у форсайт-документах 2021–2022 років (а також у попередніх аналітичних дослідженнях), із реальними подіями періоду 2022–2026 років. Проведений аналіз показує, що сценарії атак на вузлові елементи енергосистеми — зокрема підстанції 750 кВ, магістральні лінії електропередачі, ключові гідро- та теплоелектростанції — не були непередбачуваними. Вони фігурували у звітах таких організацій, як International Energy Agency (IEA), RAND Corporation та NATO Energy Security Centre of Excellence (ENSEC COE) ще до початку масованих атак восени 2022 року. Отже, характер ударів відповідав базовому сценарію війни на виснаження, а не явищу типу "чорного лебедя".

Інституційний аналіз у межах дослідження використовується як основний інструмент для пояснення причин, через які превентивні рішення блокувалися або відкладалися. Особливу увагу приділено взаємодії між Міністерством енергетики України, НКРЕКП, НЕК "Укренерго", великими учасниками ринку електроенергії та органами місцевого самоврядування. Концентрація управління у сфері передачі електроенергії (фактично

монопольна організаційна структура) розглядається як чинник, що суттєво знижує адаптивність системи. У ситуації, коли рішення щодо резервування потужностей, децентралізації або підземного розміщення інфраструктури мають проходити через вузьке інституційне "горло" одного оператора, альтернативні сценарії розвитку часто не доходять до стадії практичної реалізації.

Аналіз державної політики застосовано для виявлення розриву між задекларованими стратегічними цілями (зокрема положеннями Стратегії енергетичної безпеки України до 2035 року, Енергетичної стратегії до 2050 року та міжнародними зобов'язаннями перед Європейським Союзом) і реальною практикою їх реалізації. Порівняння з міжнародним досвідом — включаючи практики децентралізації енергосистем у країнах Балтії, використання підземних мереж у таких країнах, як Ізраїль і Швейцарія, а також рекомендації щодо забезпечення стійкості інфраструктури, сформульовані OECD і World Bank — свідчить, що український підхід до 2025–2026 років значною мірою залишався ближчим до централізованої моделі енергосистеми, успадкованої від радянського періоду, ніж до сучасних моделей resilient infrastructure.

У цьому контексті виникає певна методологічна напруга. З одного боку, у працях OECD (Strategic Foresight for Better Policies, 2019) та UNDP (Foresight Manual, 2018) наголошується, що форсайт має бути інтегрований у процеси бюджетування, регулювання та просторового планування; інакше його практична цінність є обмеженою. З іншого боку, в умовах повномасштабної війни держава часто не має достатніх ресурсів для довгострокового планування, оскільки пріоритетом стають виживання системи та швидке відновлення після ударів. У зв'язку з цим постає питання: чи можна в таких умовах очікувати домінування превентивної логіки управління? У межах цього дослідження висловлюється припущення, що навіть за умов війни превентивні заходи залишаються критично важливими, оскільки їх відсутність робить кожен цикл відновлення більш дорогим і менш ефективним. Водночас це твердження не є безумовним: існують ситуації, у яких реактивна модель управління стає єдино можливим режимом функціонування.

Окрему увагу приділено ролі монополізації в мережевих галузях. У цьому аспекті використано аналітичні матеріали OECD та World Bank щодо функціонування інфраструктурних ринків, де зазначається, що надмірна концентрація управління може стримувати інновації та диверсифікацію системи. Подібні висновки містяться також у дослідженнях, опублікованих у Central European Journal of International and Security Studies (зокрема у працях Ciuta, Klinke та ін.), де монополізовані енергетичні системи розглядаються як фактор стратегічної вразливості в умовах конфліктів. Український випадок частково підтверджує цю тезу: навіть у ситуаціях, коли технічно існували можливості розвитку локальної генерації або альтернативних мереж, регуляторні та політичні бар'єри стримували відповідні процеси. Водночас слід уточнити, що після 2024 року спостерігаються помітні зрушення у сфері генерації (зокрема у розвитку сонячної, вітрової та малої гідроенергетики). Таким чином, елементи монополізації найбільш виразно проявляються не у сфері генерації, а насамперед у системах передачі та диспетчеризації електроенергії.

Результати

Форсайт як інструмент державного управління в умовах війни – це не просто красива теорія. У мирний час він може бути довгостроковим плануванням, сценаріями розвитку, трендами. Але коли держава працює під постійними ударами, форсайт перетворюється (або мав би перетворитися) на інструмент виживання. Не оптимізації, не ефективності, а саме безперервності базових функцій – світло, тепло, вода, зв'язок, робота критичних об'єктів оборони.

OECD і UNDP пишуть про це досить чітко: форсайт цінний не як прогноз, а як механізм, що переводить знання про можливі кризи в обмеження простору прийнятних рішень. У війні

це означає: якщо сценарій масованих атак на енергетику в зимовий період має високу ймовірність – то рішення, які роблять систему вразливою саме до такого сценарію, мають бути заборонені або суттєво обмежені. У нас цього не сталося. [4; 11].

Розрив між форсайтом і реальними рішеннями виявився стійким і багатошаровим.

По-перше, часовий: підготовка відкладалася до моменту, коли вже починалися блекаути.

По-друге, структурний: централізована архітектура системи залишилася майже без змін, хоча саме вона робила кожен удар по вузловій підстанції катастрофою для цілого регіону.

По-третє: інституційний: ніхто не був персонально відповідальним за те, щоб сценарії високої ймовірності стали обов'язковими вимогами до проєктування, будівництва чи модернізації.

Це не брак інформації. Це брак механізму примусу. Знання про загрози було. Воно фіксувалося в звітах, у внутрішніх документах, у публічних заявах. Але воно не мало сили переписати правила гри. У результаті форсайт фактично виконував роль «аналітичного заспокоювання» ми ж знали, ми ж попереджали, а не інструменту дії.

Окремо стоїть питання монополізованої структури. У сегменті передачі та диспетчеризації концентрація влади в руках одного оператора створює ситуацію, коли будь-які рішення про децентралізацію, альтернативні мережі, локальне резервування мусять проходити через цю ж структуру. А вона за визначенням зацікавлена в збереженні статус-кво. Література (особливо CEJISS огляд 20 років досліджень з енергетичної безпеки) показує: монополізовані системи погано адаптуються до шоків саме через це вузьке горло прийняття рішень. У нас це видно дуже чітко: навіть коли з'являлися проєкти децентралізованої генерації (сонячні станції на об'єктах критичної інфраструктури, малі ГЕС, накопичувачі), вони розвивалися повільно, фрагментарно, з величезними регуляторними бар'єрами. Хоча в генерації вже є помітні зрушення після 2024–2025 років. Тут монополія вже не тотальна.

У цьому дослідженні стратегічний форсайт у сфері енергетичної безпеки пропонується визначати як інституціоналізований механізм державного управління, спрямований на випереджальне виявлення загроз енергетичній інфраструктурі та обов'язкову трансляцію сценаріїв цих загроз у управлінські, бюджетні та інфраструктурні рішення. Такий підхід відповідає рекомендаціям OECD та World Bank щодо управління критичною інфраструктурою в умовах криз [3; 5].

Особливість воєнного форсайту полягає в тому, що загрози енергетичній безпеці мають цілеспрямований і фундаментальний характер. За оцінками міжнародних аналітичних центрів, атаки на енергетичну інфраструктуру в сучасних війнах використовуються як інструмент політичного тиску та примушення до капітуляції, спрямований на підрив стійкості держави та вплив на свідомість цивільного населення [2; 4]. У відкритих джерелах та публічних заявах українських посадових осіб неодноразово наголошувалося, що противник розглядає енергетичну систему, зокрема підстанції електропередачі, як критичні вузли, від стабільності яких залежить робота атомних електростанцій і теплопостачання великих міст [1; 12].

Відповідно до відкритих публікацій, упродовж війни фіксувалися ознаки цілеспрямованого збору інформації щодо об'єктів критичної енергетичної інфраструктури в різних регіонах України. Метою таких дій, за оцінками експертів, є створення умов для масштабного порушення роботи енергосистеми та використання енергетичної уразливості як інструменту політичного тиску [1; 4]. Саме цей факт підкреслює, що йдеться не про абстрактні ризики, а про реалізовані та повторювані сценарії загроз, які мали бути враховані в рамках стратегічного форсайту.

З огляду на це, стратегічний форсайт у державному управлінні в умовах війни має виконувати три взаємопов'язані функції.

По-перше, аналітичну, пов'язану з ідентифікацією критичних вузлів енергосистеми та сценаріїв їх ураження.

По-друге, нормативно-обмежувальну, що передбачає встановлення обов'язкових вимог до просторового розміщення, резервування та захисту об'єктів інфраструктури. Інституційну, яка полягає у закріпленні відповідальності органів влади за реалізацію форсайт-сценаріїв у конкретних інфраструктурних рішеннях.

Стратегічний форсайт у сфері енергетичної безпеки в умовах повномасштабної війни доцільно розглядати не як допоміжний аналітичний інструмент, а як обов'язковий елемент системи державного управління. Від його ефективності безпосередньо залежить стійкість держави, безпека цивільного населення та здатність країни протистояти агресору.

Розрив між стратегічним форсайтом і управлінськими рішеннями в Україні

Однією з ключових причин вразливості енергетичної системи України в умовах повномасштабної війни є стійкий розрив між наявними форсайт-оцінками загроз та фактичними управлінськими рішеннями, що ухвалювалися на державному й місцевому рівнях. Цей розрив проявляється у домінуванні реактивної логіки управління над превентивною. Коли інфраструктурні та організаційні заходи здійснюються вже після реалізації негативних сценаріїв.

Міжнародні аналітичні центри неодноразово наголошували, що удари по енергетичній інфраструктурі України мають системний характер і спрямовані на досягнення стратегічних цілей підрив життєзабезпечення великих міст, створення гуманітарної напруги та формування політичного тиску на керівництво держави [2; 4]. У цьому сенсі енергетична інфраструктура стала не побічною, а однією з пріоритетних цілей воєнної кампанії.

Стаття *The New York Times* на початку 2026 року, присвячена ударам по енергетичних об'єктах у центральних регіонах України, засвідчує, що атаки призводили не лише до перебоїв з електропостачанням, а й до масштабних проблем із теплопостачанням у зимовий період, що безпосередньо впливало на цивільне населення [14]. У матеріалі підкреслюється, що навіть за наявності часткового відновлення електромереж, теплоенергетичні системи виявилися значно менш адаптованими до тривалих відключень. Це свідчить про відсутність комплексного підходу до інфраструктурної стійкості.

Аналогічні висновки містяться в повідомленнях агентства *Reuters*, де зафіксовано, що дронові атаки на енергетичні об'єкти в окремих промислових містах призводили до вимушених відключень електроенергії та тепла навіть за відсутності повного руйнування генеруючих потужностей [15]. Це вказує на критичну залежність локальних систем життєзабезпечення від окремих вузлових елементів мережі та недостатній рівень резервування.

З точки зору стратегічного форсайту, подібні наслідки не можуть вважатися непередбачуваними. Сценарії масованих атак на енергетичну інфраструктуру, зокрема в зимовий період, систематично фігурували у відкритих аналітичних оцінках міжнародних організацій та експертних спільнот ще з 2022 року [2; 5; 11]. Проте на практиці ці сценарії не були трансформовані у рішення, що змінювали б базову архітектуру енергосистеми, зменшували роль критичних вузлів або забезпечували автономність локальних систем теплопостачання.

Емпіричні дані, зафіксовані у міжнародних медіа, підтверджують, що проблема енергетичної вразливості України має не випадковий, а системний характер. Вона зумовлена не браком інформації про загрози, а відсутністю ефективного механізму перетворення стратегічного форсайту на обов'язкові управлінські рішення, здатні змінити інфраструктурну реальність ще до настання кризових подій.

Вразливість енергетичної системи України не може пояснюватися виключно масштабами ракетних чи дронових атак. Її першопричина управлінська. Держава знала про загрози, але не вбудувала це знання у систему обов'язкових рішень. У таких умовах стратегічний форсайт фактично виконував роль аналітичного алібі, а не інструменту дії.

Збереження централізованої архітектури енергосистеми в умовах війни слід розглядати не як технічну інерцію, а як інституційний вибір. Цей вибір призвів до концентрації

ризиків у вузлових точках передусім на магістральних підстанціях і міських енергетичних вузлах, ураження яких мало непропорційно великі системні наслідки.

У сучасних дослідженнях з безпекових студій енергетична безпека дедалі частіше розглядається не лише як питання наявності ресурсів або технічної надійності мереж, а як інституційно зумовлена категорія, тісно пов'язана зі структурою ринку, моделлю управління та розподілом влади у стратегічних секторах. Систематичний огляд двадцятирічного масиву наукової літератури, здійснений у журналі *Central European Journal of International and Security Studies*, засвідчує, що одним із ключових недооцінених чинників енергетичної вразливості є монополізація енергетичних систем, особливо в умовах криз і збройних конфліктів [16].

У рамках security studies монополія в енергетичному секторі розглядається не лише як економічна проблема, а як фактор стратегічної крихкості. CEJISS підкреслює, що централізовані та монополізовані енергетичні системи мають обмежену здатність до адаптації, оскільки ухвалення рішень зосереджене у вузькому колі акторів, а альтернативні сценарії розвитку інфраструктури фактично виключаються з політичного порядку денного [16].

Аналітичні матеріали OECD та World Bank підтверджують цей висновок, зазначаючи, що у мережевих галузях монополія знижує інноваційну динаміку, гальмує диверсифікацію джерел генерації та обмежує можливості швидкого впровадження резервних рішень [3; 8]. В умовах війни такі обмеження трансформуються з економічних у безпекові, оскільки централізовані системи стають вразливими до цілеспрямованих ударів по окремих вузлових елементах.

Український кейс підтверджує ці теоретичні положення. Збереження домінування великих операторів у сфері генерації та розподілу електроенергії обмежило розвиток локальної та розподіленої генерації, а також альтернативних енергетичних мереж на муніципальному рівні. Як наслідок, навіть за наявності фінансових ресурсів і технічних можливостей, впровадження децентралізованих рішень відбувалося повільно або фрагментарно, що не відповідало сценаріям загроз, описаним у форсайт-документах [2; 5].

З позицій стратегічного форсайту монополізована модель енергетики створює додатковий інституційний розрив між знанням про загрози та практикою управління. Форсайт передбачає множинність сценаріїв і варіантів дій, тоді як монополія фактично звужує спектр допустимих рішень до тих, що не підривають існуючу структуру ринку. У результаті стратегічні рекомендації щодо децентралізації, резервування та підземного розміщення інфраструктури залишаються на рівні декларацій.

Важливим є також безпековий аспект політичної економії енергетики. CEJISS звертає увагу на те, що у країнах із високим рівнем концентрації енергетичних активів виникає феномен «інституційного блокування», коли ключові рішення ухвалюються з огляду на стабільність існуючих бізнес-моделей, а не на вимоги національної безпеки [16]. В умовах війни це призводить до ситуації, коли технічно можливі та стратегічно доцільні рішення не реалізуються через політичні та регуляторні обмеження.

Монополію в енергетичному секторі доцільно розглядати як системний ризик енергетичної безпеки, який посилює наслідки воєнних атак і знижує ефективність стратегічного форсайту. Усунення цього ризику вимагає не лише технічних інвестицій, а й переосмислення ролі антимонопольної політики як складової національної безпеки, що відповідає підходам, сформульованим у працях OECD, World Bank та сучасних безпекових дослідженнях.

Логічна модель "форсайт → управлінські рішення → інфраструктура"

Попередній аналіз засвідчив, що центральною проблемою енергетичної безпеки України в умовах повномасштабної війни є не відсутність знань про загрози, а інституційний розрив між стратегічним форсайтом, управлінськими рішеннями та реальною інфраструктурною архітектурою. Для концептуалізації цього розриву та його наслідків доцільно застосувати логічну модель "форсайт → управлінські рішення → інфраструктура", яка

дозволяє простежити причинно-наслідкові зв'язки між аналітичними оцінками майбутніх загроз і матеріалізованими результатами державної політики.

У працях OECD, Світового банку та RAND послідовно наголошується, що стратегічний форсайт набуває реальної безпекової цінності лише за умови, коли він обмежує простір допустимих управлінських рішень і впливає на розподіл ресурсів та просторове планування інфраструктури [3; 4; 5]. Якщо ж форсайт залишається відокремленим від процесів бюджетування та регулювання, він втрачає здатність запобігати реалізації негативних сценаріїв.

Таблиця, яку ми зробили для порівняння "Було" і "Має бути", вийшла досить жорсткою – можливо, навіть занадто дихотомічною. Реальність завжди складніша: деякі превентивні елементи таки впроваджувалися (зростання імпорту з ЄС, окремі децентралізовані рішення для лікарень і об'єктів оборони, спроби підземного резервування в кількох містах). Але загальна картина лишається: реактивна логіка домінує. Превентивна – з'являється епізодично, часто вже після чергової хвилі ударів.

Ось як це виглядає після кількох ітерацій перегляду (ми спочатку зробили таблицю надто "ідеальною", потім почали додавати нюанси, врешті вирішили залишити її приблизно такою, але з уточненнями в коментарях):

Таблиця: Порівняння трансляції форсайту в рішення та інфраструктуру

Вимір	Було (реальність 2022-2026)	Має бути (нормативна модель за літературою)	Коментар
Роль форсайту	Дорадчий, необов'язковий	Інституціоналізований, обов'язковий елемент державного управління	Окремі сценарії використовувались для аргументації в переговорах з партнерами
Зв'язок з бюджетом	Слабкий або відсутній	Пряма інтеграція сценаріїв у бюджетні пріоритети	Після 2024-го з'явились деякі зміни
Архітектура енергосистеми	Висока централізація, залежність від вузлових об'єктів	Децентралізована система з локальними мережами та резервуванням	У генерації вже є зрушення, у передачі майже без змін
Просторове розміщення	Переважно надземна інфраструктура	Пріоритет підземному розміщенню критичних елементів	Дуже повільно, поодинокі проєкти в містах
Реакція на загрози	Реактивна: відновлення після ударів	Превентивна: підготовка до найгірших сценаріїв	Реактивність досі домінує, але є окремі превентивні елементи (імпорт, накопичувачі)
Структура ринку	Домінування великих операторів у передачі та диспетчеризації	Диверсифікація та антимонопольні механізми як елементи безпеки	У генерації конкуренція росте, у передачі -ні
Захист населення	Значна частина відповідальності перекладена на людей та бізнес	Централізована муніципальна політика стійкості	Зміни є, але повільні й нерівномірні

Джерело: *Складено автором.*

Ця таблиця не претендує на вичерпність. Вона радше діагностичний інструмент, який показує, де саме рветься ланцюг. Ми свідомо залишили її неідеальною: з уточненнями, бо реальність саме така – не чорно-біла.

Логічна модель "форсайт → управлінські рішення → інфраструктура" добре пояснює, чому вразливість стала системною. Вона не була неминучою. Вона була результатом конкретних (або відсутніх) рішень, які не враховували сценарії, що вже були описані. І саме тому енергетична безпека в умовах цієї війни – це wicked problem: немає простого рішення, є постійне управління ризиками, постійна боротьба з інституційною інерцією [17].

Подібної позиції дотримується і *Center for Strategic and International Studies* (CSIS), зокрема *Risk and Foresight Group*, яка розглядає форсайт як інструмент зменшення стратегічної

несподіванки та підвищення інституційної готовності держав до криз високої інтенсивності [18]. У публікаціях CSIS підкреслюється, що ключовою помилкою багатьох держав є формальне використання форсайту без його закріплення у процесах ухвалення рішень, що повністю корелює з українським кейсом.

Ми не стверджуємо, що все можна було зробити ідеально. Але ми стверджуємо, що розрив між знанням і дією був і залишається головною причиною вразливості більшою, ніж кількість ракет чи дронів.

Обговорення

Отримані результати дослідження дозволяють розглянути проблему енергетичної вразливості України в умовах повномасштабної війни у ширшому інституційному та аналітичному контексті. Проведений аналіз показує, що удари по енергетичній інфраструктурі не були непередбачуваними подіями. Сценарії атак на ключові елементи енергосистеми, зокрема вузлові підстанції, магістральні лінії електропередачі та об'єкти генерації, систематично розглядалися у звітах міжнародних аналітичних центрів і дослідницьких організацій.

Таким чином, результати дослідження підтверджують, що проблема полягає не у відсутності інформації про потенційні загрози, а у механізмах її використання в системі державного управління. Виявлений розрив між прогнозуванням і практичними рішеннями відповідає явищу, яке в літературі з державної політики описується як *implementation gap*. У досліджуваному випадку цей розрив проявляється у домінуванні реактивної моделі управління, коли інфраструктурні рішення приймаються переважно після реалізації кризових сценаріїв.

Порівняння отриманих результатів з міжнародними підходами до управління критичною інфраструктурою демонструє, що стратегічний форсайт у більшості сучасних моделей розглядається як інструмент, інтегрований у процеси бюджетування, регулювання та інфраструктурного планування. У цьому випадку він виконує функцію обмеження простору допустимих управлінських рішень, спрямованих на зменшення стратегічної несподіванки. Проте емпіричні дані свідчать, що у сфері енергетичної безпеки України форсайт переважно використовувався як аналітичний або дорадчий інструмент.

Окремий аспект обговорення пов'язаний зі структурними характеристиками енергетичної системи. Централізована архітектура енергосистеми та висока концентрація управління у сфері передачі електроенергії створюють додаткові обмеження для адаптації до кризових ситуацій. У сучасних безпекових дослідженнях подібні системи розглядаються як більш уразливі до цілеспрямованих атак, оскільки пошкодження окремих вузлових елементів може мати непропорційно великі системні наслідки.

Водночас аналіз показує, що навіть у межах централізованої системи відбуваються окремі процеси адаптації, зокрема розвиток локальної генерації та використання альтернативних джерел енергії. Однак ці процеси мають переважно фрагментарний характер і не формують цілісної моделі інфраструктурної стійкості.

Таким чином, результати дослідження свідчать, що енергетична безпека в умовах війни формується на перетині технічних, інституційних та політичних факторів. Саме взаємодія цих факторів визначає здатність держави перетворювати прогнозування загроз на практичні рішення, спрямовані на підвищення стійкості критичної інфраструктури. Розгляд цієї проблеми у такому контексті створює підстави для формулювання узагальнених висновків щодо ролі стратегічного форсайту у системі державного управління енергетичною безпекою.

Висновки

Проведене дослідження дозволило проаналізувати проблему енергетичної вразливості України в умовах повномасштабної війни крізь призму стратегічного форсайту та інституційних механізмів державного управління. Отримані результати свідчать, що атаки на енергетичну

інфраструктуру не були випадковими або непередбачуваними подіями. Навпаки, сценарії системних ударів по ключових елементах енергосистеми — підстанціях, магістральних мережах та об'єктах генерації — були відображені у низці міжнародних аналітичних досліджень і експертних прогнозів ще на початкових етапах війни.

Водночас аналіз показує, що наявність відповідних прогнозів і аналітичних оцінок не була трансформована у системні превентивні управлінські рішення. У цьому контексті ключовою проблемою виявляється не дефіцит інформації про потенційні загрози, а інституційний розрив між прогнозуванням ризиків і їх врахуванням у державній політиці. Такий розрив проявляється у домінуванні реактивної моделі управління, коли основні заходи щодо підвищення стійкості енергосистеми здійснюються вже після реалізації кризових сценаріїв.

Результати дослідження також свідчать, що структурні особливості енергетичної системи України — передусім її централізований характер та концентрація управління у сфері передачі електроенергії — підвищують системну вразливість інфраструктури в умовах воєнних загроз. Пошкодження окремих вузлових елементів енергосистеми може призводити до масштабних каскадних наслідків для функціонування економіки, органів державної влади та систем життєзабезпечення населення.

Узагальнення результатів дослідження дозволяє зробити висновок, що проблема енергетичної безпеки в умовах війни має комплексний характер і формується на перетині технічних, інституційних та політичних факторів. Підвищення стійкості енергетичної системи потребує не лише модернізації інфраструктури або розширення технічних засобів захисту, а й удосконалення механізмів державного управління, здатних забезпечити інтеграцію стратегічного форсайту у процеси формування політики, планування розвитку критичної інфраструктури та ухвалення управлінських рішень.

Таким чином, стратегічний форсайт може виконувати ефективну роль лише за умови його інституційної інтеграції у систему державного управління. Перетворення прогнозування загроз на обов'язковий елемент інфраструктурного та регуляторного планування є важливою передумовою зменшення енергетичної вразливості держави та підвищення стійкості критичної інфраструктури в умовах воєнних загроз.

Рекомендації

Результати дослідження дозволяють сформулювати систему рекомендацій, спрямованих на усунення виявленого розриву між стратегічним форсайтом, управлінськими рішеннями та реальною архітектурою енергетичної інфраструктури.

Автори статті не претендують на те, що ці рекомендації готовий план дій, який хтось візьме й виконає завтра. Це радше система напрямків, які випливають з діагнозу, але з розумінням, що в умовах війни + післявоєнної реконструкції багато з них звучать утопічно. І все ж без спроби їх сформулювати ми просто продовжуємо той самий цикл.

1. Стратегічний форсайт у сфері енергетичної безпеки потрібно зробити обов'язковим елементом державного управління, а не опціональним аналітичним продуктом. Це означає:

нормативно закріпити: жодна державна програма, жоден проєкт модернізації чи будівництва критичної інфраструктури не затверджується без інтеграції форсайт-сценаріїв (принаймні сценаріїв високої ймовірності);

прив'язати до бюджета: капітальні видатки на енергетику мають проходити через фільтр "чи враховує це найгірші сценарії з форсайту";

ввести персональну відповідальність: якщо сценарій реалізувався, а превентивні заходи не були зроблені це питання до конкретних посадовців (OECD і CSIS це прямо прописують як необхідну умову). Тут є сумнів: чи реально ввести таку жорстку відповідальність у воєнний час, коли рішення часто ухвалюються в режимі "вижити сьогодні"? Можливо, спочатку – пілотний режим на окремих регіонах чи об'єктах.

2. Перейти від реактивної парадигми (“відновимо після удару”) до випереджальної (“зробимо так, щоб удар завдавав мінімальної шкоди”). Це не гасло. Це означає закладати вимоги стійкості вже на етапі проєктування не модернізувати постфактум. Wicked problem не вирішується раз і назавжди, але її можна зробити менш гострою, якщо постійно знижувати вразливість вузлів. Практично: при будь-якому новому будівництві чи капремонті: обов’язкове обґрунтування, чому не обрано децентралізований/підземний/резервований варіант.

3. Підземне розміщення критичних елементів енергетичної та суміжної інфраструктури визначити як довгостроковий стратегічний пріоритет держави. Не косметичні заходи, а системну державну політику. Йдеться про:

підстанції класу 330–750 кВ (де це технічно можливо – мікротунелі, підземні камери);

магістральні кабельні лінії в містах;

інтеграцію з муніципальними підвалами, технічними поверхами, підземними коридорами (як у деяких європейських країнах уже роблять для комунікацій);

резервні локальні джерела, розміщені під землею поруч зі споживачем. Переваги очевидні (NATO ENSEC, IEA, EIB це детально описують): зниження вразливості до ракет, дронів, диверсій, екстремальної погоди. Але ми розуміємо бар’єри: це дорого, довго, потребує зміни норм, землекористування, координації з містами. Тому поетапно: спочатку ключові міста (Київ, Харків, Одеса, Львів), потім інші обласні центри. Сумнів: чи знайдуться гроші й політична воля саме зараз? Досвід 2022–2026 показує, що на відновлення витрачають мільярди, але на превентивну трансформацію – набагато менше.

4. Стимулювати локальну та розподілену генерацію плюс альтернативні мережі на муніципальному рівні. Конкретно:

регуляторні зміни для спрощення підключення малих і середніх джерел (сонце, вітер, накопичувачі, когенерація);

механізми, щоб громади могли створювати власні мікромережі з резервуванням;

розгляд антимонопольної політики в енергетиці як частини національної безпеки (CEJISS це називає ключовим недооціненим чинником). У генерації вже є прогрес: після 2024–2025 років децентралізовані потужності помітно зросли. Але в передачі й диспетчеризації ситуація майже не змінилася. Тут потрібні структурні рішення.

5. Останнє, найважливіше й найскладніше інституціоналізувати перехід від “знання” до “дії”. Без цього всі попередні пункти залишаться на папері. Потрібен механізм, який би змушував: якщо сценарій описаний як високої ймовірності рішення, що суперечать йому, мають проходити через публічне обґрунтування або блокуватися. Це може бути спеціальний комітет, або обов’язковий аудит, або інтеграція в РНБО/Кабмін. Але головне щоб це не було черговою формальністю заради форми.

Чи реально це все реалізувати в умовах війни та подальшої реконструкції? Велике питання. Досвід показує: технічно можливо багато, ресурси знаходяться (особливо з допомогою міжнародних партнерів), але інституційна інерція, політична економія енергосектору, короткострокові пріоритети часто перемагають. Тому ці рекомендації не рецепт, а радше каркас, який варто постійно перевіряти на реальність і коригувати.

Якщо не рухатися в цьому напрямку ми просто будемо щоразу повторювати: прогноз → удар → героїчне відновлення → новий прогноз → новий удар.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. BBC News Україна. Удари РФ по енергетиці України: наслідки для цивільного населення.URL: https://www.bbc.com/ukrainian/articles/cq6v82gy094o (дата звернення: 10.01.2026).
2. RAND Corporation. *Russia's Attacks on Ukraine's Energy Infrastructure*.URL: https://www.rand.org/
3. World Bank. *Resilient Infrastructure for Sustainable Development*.Washington, DC : World Bank, 2021.URL: https://www.worldbank.org
4. NATO Energy Security Centre of Excellence. *Energy Infrastructure Protection and Resilience*.Vilnius: NATO ENSEC COE, 2022.URL: https://enseccoe.
5. Organisation for Economic Co-operation and Development (OECD). *Strategic Foresight for Better Policies*.Paris : OECD Publishing, 2019.URL: https://www.oecd.org.
6. United Nations Development Programme (UNDP). *Foresight Manual*.New York : UNDP, 2018.URL: https://www.undp.org
7. Miles I., Saritas O., Sokolov A. *Foresight for Science, Technology and Innovation*.Cheltenham : Edward Elgar Publishing, 2016.
8. European Commission. *Energy Market Design and Competition Policy*.Brussels, 2020.URL: https://energy.ec.europa.eu
9. Міністерство енергетики України. Стан енергетичної системи в умовах воєнного стану. URL: https://www.mev.gov.ua
10. European Investment Bank. *Underground Infrastructure and Urban Resilience*. Luxembourg : EIB, 2021. URL: https://www.eib.org.
11. International Energy Agency. *Energy Security and Resilience*. Paris : IEA, 2022. URL: https://www.iea.org/topics/energy-security.
12. ZN.UA. Patriot не для дронів: захист критичної інфраструктури України. URL: https://zn.ua/ukr/POLITICS/patriot-ne-dlja-droniv-zelenskij-rozkritikuvav-zakhist-kritichnikh-objektiv.html
13. International Energy Agency. *Energy Security and Resilience*. URL: https://www.iea.org/topics/energy-security
14. The New York Times. Russian Strike Leaves Ukrainian City Struggling to Restore Heat. URL: https://www.nytimes.com/2026/01/08/world/europe/ukraine-dnipro-power-russia-strike-heat.html
15. Reuters. Russian drone attack forces power cuts in Ukraine's Kryvyi Rih, military says. URL: https://www.reuters.com/world/russian-drone-attack-forces-power-cuts-ukraines-kryvyi-rih-military-says-2026-01-14/
16. Ciuta F., Klinke I., et al. Energy Security in Security Studies: A Systematic Review of Twenty Years of Literature. *Central European Journal of International and Security Studies*. URL: https://cejiss.org/energy-security-in-security-studies-a-systematic-review-of-twenty-years-of-literature
17. Brown M., et al. Energy Security as a Wicked Problem: A Foresight Approach to Developing a Grand Strategy for Resilience. *The Solutions Journal*. URL: https://thesolutionsjournal.com/energy-security-as-a-wicked-problem-a-foresight-approach-to-developing-a-grand-strategy-for-resilience/
18. Center for Strategic and International Studies. Risk and Foresight Group. Washington, DC: CSIS. URL: https://www.csis.org/programs/international-security-program/risk-and-foresight-group

19. International Energy Agency. *Summit on the Future of Energy Security: Background Paper*. Paris : IEA, 2023. URL: https://www.iea.org

References

1. BBC News Ukrayina. Udary RF po enerhetytsi Ukrayiny: naslidky dlya tsyvil'noho naselennya. https://www.bbc.com/ukrainian/articles/cq6v82gy094
2. RAND Corporation. Russia's Attacks on Ukraine's Energy Infrastructure. https://www.rand.org/
3. World Bank. Resilient Infrastructure for Sustainable Development. Washington, DC: World Bank, 2021. https://www.worldbank.org
4. NATO Energy Security Centre of Excellence. Energy Infrastructure Protection and Resilience. Vilnius: NATO ENSEC COE, 2022. https://enseccoe.org
5. Organisation for Economic Co-operation and Development (OECD). Strategic Foresight for Better Policies. Paris: OECD Publishing, 2019. https://www.oecd.org (data zvernennia: 11.01.2026).
6. United Nations Development Programme (UNDP). Foresight Manual. New York: UNDP, 2018. https://www.undp.org
7. Miles I., Saritas O., Sokolov A. Foresight for Science, Technology and Innovation. Cheltenham: Edward Elgar Publishing, 2016.
8. European Commission. Energy Market Design and Competition Policy. Brussels, 2020. https://energy.ec.europa.eu
9. Ministerstvo enerhetyky Ukrayiny. Stan enerhetychnoyi systemy v umovakh voyennoho stanu. https://www.mev.gov.ua
10. European Investment Bank. Underground Infrastructure and Urban Resilience. Luxembourg: EIB, 2021. https://www.eib.org
11. International Energy Agency. Energy Security and Resilience. Paris: IEA, 2022. https://www.iea.org/topics/energy-security
12. ZN.UA. Patriot ne dlya droniv: zakhyst krytychnoyi infrastruktury Ukrayiny. https://zn.ua/ukr/POLITICS/patriot-ne-dlja-droniv-zelenskij-rozkritikuvav-zakhist-kritichnikh-objektiv.html
13. International Energy Agency. Energy Security and Resilience. https://www.iea.org/topics/energy-security
14. The New York Times. Russian Strike Leaves Ukrainian City Struggling to Restore Heat. https://www.nytimes.com/2026/01/08/world/europe/ukraine-dnipro-power-russia-strike-heat.html
15. Reuters. Russian drone attack forces power cuts in Ukraine's Kryvyi Rih, military says. https://www.reuters.com/world/russian-drone-attack-forces-power-cuts-ukraines-kryvyi-rih-military-says-2026-01-14/
16. Ciuta F., Klinke I., et al. Energy Security in Security Studies: A Systematic Review of Twenty Years of Literature. Central European Journal of International and Security Studies. https://cejiss.org/energy-security-in-security-studies-a-systematic-review-of-twenty-years-of-literature
17. Brown M., et al. Energy Security as a Wicked Problem: A Foresight Approach to Developing a Grand Strategy for Resilience. The Solutions Journal. https://thesolutionsjournal.com/energy-security-as-a-wicked-problem-a-foresight-approach-to-developing-a-grand-strategy-for-resilience/
18. Center for Strategic and International Studies. Risk and Foresight Group. Washington, DC: CSIS. URL: https://www.csis.org/programs/international-security-program/risk-and-foresight-group
19. International Energy Agency. Summit on the Future of Energy Security: Background Paper. Paris: IEA, 2023. https://www.iea.org