МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

Навчально-науковий інститут «Інститут державного управління»
Кафедра права, національної безпеки та європейської інтеграції

Кваліфікаційна робота магістра
на тему

ЕНЕРГЕТИЧНА БЕЗПЕКА ЯК СКЛАДОВА ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ: РОЛЬ ПУБЛІЧНОГО УПРАВЛІННЯ

Виконав студент 2 курсу,
групи ППГЗ-2-24
Спеціальності 281 «Публічне управління та адміністрування»
Освітньо-професійної програми
«Публічна політика та управління в умовах гібридних загроз»
_____ Олег ГРУДЗЕВИЧ

Науковий керівник роботи:
доктор юридичних наук, професор
_____ Лариса ВЕЛИЧКО

Харків – 2025

ЗМІСТ

ВСТУП

Актуальність теми. Повномасштабна агресія Російської Федерації проти України з 24 лютого 2022 року перетворила енергетичний сектор на один із ключових об'єктів гібридної війни. Систематичні ракетні та безпілотні удари по об'єктах енергетичної інфраструктури (понад 25 масованих атак, що призвели до руйнування більше 21 ГВт генеруючих потужностей) поставили безпрецедентні виклики перед системою публічного управління, вимагаючи миттєвої адаптації механізмів державного регулювання до умов активних бойових дій.

Досвід 2022–2025 років виявив як значні досягнення системи публічного управління енергетичною безпекою (екстрена синхронізація з європейською енергосистемою ENTSO-E за три тижні замість запланованих півтора року, збереження 80 % розподільних мереж, ефективна координація міжнародної допомоги на суму понад 1,2 млрд євро), так і критичні вразливості (фрагментація управлінських повноважень, реактивний характер рішень, недостатня захищеність об'єктів від повторних ударів).

Формування ефективної системи протидії гібридним загрозам в енергетичному секторі відбувалося в екстремальних умовах, що призвело до високої залежності від екстраординарних зусиль персоналу – 160 загиблих та понад 300 поранених енергетиків за період повномасштабної війни. Актуальність дослідження визначається потребою переходу від реактивного до проактивного управління, вирішення структурних проблем координації між центральними та регіональними органами влади, імплементації зарубіжного досвіду протидії гібридним загрозам, а також необхідністю забезпечення довгострокової енергетичної стійкості незалежно від розвитку воєнної ситуації.

Стан наукової розробки проблеми. Теоретичні та прикладні аспекти енергетичної безпеки в умовах гібридних загроз протягом значного періоду досліджуються українськими та міжнародними науковцями. В Україні цю проблематику розглядають: Л.Ю. Величко та М.В. Білоконь (гібридні загрози

критичній інфраструктурі та виклики для державного регулювання), Є. Магда (концептуалізація гібридної війни та енергетичного шантажу), О.П. Рябченко (правові засади енергетичної безпеки), О.М. Суходоля, Ю.М. Харазішвілі та Г.Л. Рябцев (модель управління ризиками енергетичної безпеки), А.Л. Помаза-Пономаренко та Д.В. Тарадуда (світовий досвід протистояння гібридній війні), С.М. Бугазіянус (механізми публічного управління та smart grid), Є.В. Кисельов (перспективи розвитку механізмів управління), М. Гранд та О. Свйонтик (енергетична безпека в умовах російсько-української війни), А. Бобко (екологічні та військові загрози енергетичній безпеці), Н. Карачина (антикризове управління енергетикою).

Міжнародний дослідницький доробок представлений публікаціями Міжнародного енергетичного агентства (IEA), Європейського центру передового досвіду з протидії гібридним загрозам (Hybrid CoE), Центру передового досвіду НАТО з енергетичної безпеки (ENSEC COE), Оборонного коледжу НАТО, Гаазького центру стратегічних досліджень, а також дослідженнями Ф. Гоффмана (концепція гібридних загроз), М. Рюле та Ю. Груб'яускаса (енергетика як інструмент гібридної війни), Т. Свейса (кросдоменні стратегії).

Попри значний науковий інтерес до окремих аспектів, бракує комплексних досліджень публічного управління енергетичною безпекою України як складової протидії гібридним загрозам, що поєднують теоретичне обґрунтування, інституційний аналіз, оцінку ефективності та практичні рекомендації з урахуванням досвіду повномасштабної війни. Це дослідження спрямоване на заповнення цієї прогалини.

Метою роботи є комплексний аналіз теоретичних засад, інституційної архітектури, практичного досвіду та системних викликів публічного управління енергетичною безпекою України як складової протидії гібридним загрозам із розробкою науково обґрунтованих рекомендацій щодо підвищення його ефективності.

Для досягнення поставленої мети визначено такі *завдання:*

– узагальнити концептуальні основи гібридних загроз, розкрити їх сутність, типологію та механізми впливу на національну безпеку;

– дослідити поняття, місце та взаємозв'язки енергетичної безпеки в системі протидії гібридним загрозам;

– проаналізувати суб'єкти, механізми та інструменти публічного управління енергетичною безпекою в Україні;

– оцінити ефективність публічного управління у протидії гібридним загрозам в енергетичному секторі України через аналіз досягнень та виявлення системних проблем;

– систематизувати зарубіжний досвід публічного управління енергетичною безпекою в умовах гібридних загроз (країни Балтії, Польща, Німеччина, Ізраїль);

– розробити комплексні рекомендації щодо посилення ролі публічного управління в забезпеченні енергетичної безпеки як складової протидії гібридним загрозам.

Об'єктом дослідження є система публічного управління енергетичною безпекою України в умовах гібридної війни та повномасштабної агресії Російської Федерації (2014-2025 рр.).

Предметом дослідження є механізми, інструменти та практики реалізації публічного управління енергетичною безпекою України у протидії гібридним загрозам.

Методи дослідження. Для досягнення мети дослідження використано комплекс загальнонаукових та спеціальних методів. *Метод термінологічного аналізу застосовано* для розмежування понять «гібридні загрози», «енергетична безпека», «критична інфраструктура», «енергетична стійкість» (resilience); *метод теоретичного узагальнення* використано для систематизації наукових підходів*; системний підхід* застосовано для дослідження енергетичної безпеки як складової національної безпеки (підрозділ 1.1). *Інституційний аналіз* використано для дослідження структури та повноважень органів у сфері енергетичної безпеки; *структурно-функціональний аналіз* застосовано для

визначення ролей різних акторів (РНБО, Кабінет Міністрів, Міненерго, НКРЕКП, НЕК «Укренерго»); нормативно-правовий аналіз використано для вивчення законодавчої бази (підрозділ 1.2).

Метод документального аналізу застосовано для вивчення офіційних стратегій (Енергетична стратегія України до 2050 року, Стратегія національної безпеки України), звітів міжнародних організацій (IEA, ACAPS, ENTSO-E); *статистичний метод* використано для аналізу кількісних показників руйнувань та відновлення інфраструктури (підрозділ 2.1). *Метод експертних оцінок* застосовано для виявлення системних проблем та дисфункцій; *метод кейс-стаді* використано для поглибленого аналізу конкретних практик (синхронізація з ENTSO-E, децентралізація енергетики в територіальних громадах) (підрозділ 2.2).

Компаративний метод використано для порівняльного аналізу зарубіжного досвіду протидії гібридним загрозам в енергетичному секторі (країни Балтії, Польща, Німеччина, Ізраїль); *історичний метод* застосовано для дослідження еволюції систем енергетичної безпеки (підрозділ 3.1). *Метод стратегічного планування* використано для розробки комплексних рекомендацій; метод моделювання застосовано для визначення оптимальних механізмів підвищення ефективності публічного управління (підрозділ 3.2).

*Практичне значення отриманих результатів***.** Результати дослідження мають практичне застосування в науково-дослідній, управлінській та освітній сферах.

У науково-дослідній сфері матеріали роботи формують теоретико-методологічну базу для подальших досліджень механізмів публічного управління енергетичною безпекою в умовах гібридних конфліктів та повномасштабних війн. Узагальнений український досвід 2014-2025 років становить унікальний емпіричний матеріал для міжнародної наукової спільноти, оскільки практики протидії гібридним загрозам в енергетичному секторі під час найбільшого збройного протистояння в Європі після Другої світової війни мають значення для дослідників енергетичної безпеки та публічного управління

критичною інфраструктурою.

У практичній діяльності державних органів результати дослідження надають Раді національної безпеки і оборони України аналітичну основу для вдосконалення координаційних механізмів у сфері енергетичної безпеки. Міністерство енергетики України може використати рекомендації для оптимізації міжвідомчої взаємодії та розвитку децентралізованої генерації. Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг (НКРЕКП), отримує практичні інструменти вдосконалення регуляторних механізмів в умовах надзвичайних ситуацій. НЕК «Укренерго» та оператори систем розподілу можуть застосувати рекомендації щодо підвищення стійкості енергетичної інфраструктури. Апарат Верховної Ради України може використати матеріали при розробці законодавства у сфері захисту критичної інфраструктури та розвитку відновлюваної енергетики.

У навчальному процесі матеріали дослідження можуть бути інтегровані закладами вищої освіти при викладанні дисциплін «Національна безпека», «Публічне управління та адміністрування», «Енергетична безпека», «Управління критичною інфраструктурою», «Протидія гібридним загрозам». Результати можуть бути використані в програмах підготовки та підвищення кваліфікації державних службовців у Національному агентстві України з питань державної служби, ННІ «Інституті державного управління» Харківського національного університету імені В.Н. Каразіна, Національному університеті оборони України імені Івана Черняховського.

Апробація результатів дослідження. Основні положення та результати дослідження обговорювалися на засіданнях кафедри права, національної безпеки та європейської інтеграції ННІ «Інститут державного управління» Харківського національного університету імені В.Н. Каразіна і можуть бути використані в подальшому в науковій та навчальній діяльності кафедри.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ ЯК СКЛАДОВОЇ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

1.1 Гібридні загрози: сутність, типологія та механізми впливу на національну безпеку

Трансформація безпекового середовища на початку XXI століття зумовила появу принципово нових форм міждержавного протистояння, що суттєво відрізняються від класичних моделей конфліктів. Україна, починаючи з 2014 року, стала об'єктом системної гібридної агресії, яка продемонструвала безпрецедентне поєднання воєнних, економічних, енергетичних, інформаційних та кібернетичних інструментів впливу.

Повномасштабне вторгнення Російської Федерації у 2022 році лише підтвердило, що енергетичний сектор є одним із пріоритетних об’єктів гібридного впливу, а отже, потребує комплексного наукового осмислення в контексті забезпечення національної безпеки. Відтак, з’ясування сутності, типології та механізмів впливу гібридних загроз є необхідною теоретичною передумовою для формування ефективної системи публічного управління у сфері енергетичної безпеки.

Концептуалізація поняття «гібридні загрози» є предметом наукових дискусій упродовж останніх двох десятиліть. У праці «Conflict in the 21st Century: The Rise of Hybrid Wars» (2007) американський дослідник Ф. Гоффман запропонував розуміння гібридної війни як комбінації конвенційних можливостей, нерегулярних тактик, терористичних актів та злочинних методів у рамках єдиної кампанії [17, с. 14]. За його твердженням, гібридні загрози охоплюють повний спектр різних способів ведення війни, включаючи конвенційні спроможності, нерегулярні тактики та формування, терористичні

акти, а також кримінальний безлад [17 с. 8]. Ключовим внеском Ф. Гоффмана стало обґрунтування переходу від бінарної моделі конфліктів (конвенційна/нерегулярна війна) до багатовимірної гібридної моделі, що передбачає синергію різнорідних інструментів впливу.

Водночас концепція Ф. Гоффмана зазнала критики за її надмірну орієнтованість на воєнний вимір. У колективній монографії «Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present» (2012) за редакцією В. Мюррея та П. Менсура зазначається, що гібридність не є принципово новим явищем – подібні комбінації методів застосовувалися ще за часів Наполеонівських війн та у В'єтнамі [26, с. 5]. На думку авторів, концепція Ф. Гоффмана перебільшує новизну гібридних загроз, ігноруючи історичний контекст застосування комбінованих методів ведення війни. Проте така критика не враховує якісних трансформацій, що відбулися внаслідок глобалізації та інформаційної революції.

У монографії «Гібридна війна: вижити та перемогти» (2015) український науковець Є. Магда суттєво розширив розуміння гібридної агресії, включивши до неї енергетичний шантаж, інформаційно-психологічні операції та боротьбу за свідомість [58, с. 39]. Принциповим є його акцент на тому, що гібридна війна – це насамперед боротьба за свідомість, нав'язування альтернативних наративів та руйнування ціннісних орієнтирів суспільства. Саме такий підхід дозволяє пояснити роль енергетичного чинника як інструменту не лише економічного тиску, а й психологічного впливу на населення.

Європейський центр передового досвіду з протидії гібридним загрозам (Hybrid CoE) у концептуальній моделі 2021 року визначає гібридні загрози як координовані та синхронізовані дії, що навмисно спрямовані на системні вразливості демократичних держав та інститутів із використанням широкого кола засобів без формального оголошення війни [20, с. 3]. Це визначення враховує еволюцію концепції та сучасні реалії безпекового середовища, зокрема досвід російсько-української війни.

Критичний аналіз наукових підходів дозволяє стверджувати, що жоден із

них окремо не охоплює всієї повноти феномена гібридних загроз. Концепція Ф. Гоффмана надає важливу аналітичну рамку, проте потребує доповнення невоєнними вимірами. Підхід Є. Магди влучно акцентує інформаційно-психологічну складову, але недостатньо систематизує механізми впливу. Визначення Hybrid CoE є найбільш комплексним, однак потребує конкретизації щодо ролі окремих секторів, зокрема енергетичного. На підставі проведеного аналізу пропонуємо розуміти гібридні загрози як комплекс координованих дій державних та недержавних акторів, спрямованих на підрив національної безпеки держави-об'єкта шляхом синхронного застосування воєнних, політичних, економічних, енергетичних, інформаційних та кібернетичних інструментів без формального оголошення війни.

Наукові підходи до класифікації гібридних загроз суттєво різняться залежно від обраних критеріїв. Типологія, запропонована Ф. Гоффманом, ґрунтується на характері акторів та методів: регулярні сили, партизанські формування, терористичні організації та кримінальні структури [17, с. 14]. Така класифікація відображає воєнно-тактичний підхід, проте є недостатньою для аналізу сучасних комплексних загроз.

Доктринальні документи НАТО пропонують розмежування гібридних загроз за критерієм відкритості: приховані (covert) та відкриті (overt), а також за типом актора: державні та недержавні [28]. Документ «Countering Hybrid Threats» (2024) визначає ключові домени гібридного впливу: воєнний, кібернетичний, інформаційний, економічний та субверсивний. Важливо, що НАТО розглядає гібридні загрози не як статичне явище, а як динамічний процес, що потребує постійної адаптації механізмів реагування.

Центр досліджень національної безпеки та стратегічних комунікацій (ЦЕНСС) у дослідженні «Концепція гібридної війни» (2024) виокремлює 12 складових гібридних загроз: воєнну, дипломатичну, економічну, енергетичну, інформаційну, кібернетичну, правову, соціальну, екологічну, демографічну, технологічну та культурну [55]. Такий підхід відображає максимально широке розуміння гібридності, проте може ускладнювати

практичне застосування через надмірну деталізацію. Концептуальна модель Hybrid CoE пропонує класифікацію гібридних загроз за рівнем впливу: тактичний рівень (локальні операції впливу), оперативний рівень (координовані кампанії в кількох секторах), стратегічний рівень (системний вплив на державу в цілому) та глобальний рівень (дестабілізація регіональної або світової безпеки) [20, с. 8]. Цінність такого підходу полягає в можливості оцінки масштабів загрози та відповідної калібровки заходів протидії. У дослідженні Гаазького центру стратегічних досліджень Т. Свейс та співавтори критикують термін «гібридний» як надмірно широкий («catch-all»), що охоплює занадто різнорідні явища [33, с. 15]. Натомість вони пропонують крос-доменний підхід (cross-domain strategies), що акцентує увагу на взаємодії між різними сферами: дипломатичною, інформаційною, воєнною, економічною та правовою (модель DIMEL). На їхню думку, ефективна протидія потребує не стільки класифікації загроз, скільки розуміння механізмів їх взаємопідсилення.

Узагальнення розглянутих підходів дозволяє запропонувати інтегровану типологію, що враховує як доменну, так і рівневу диференціацію гібридних загроз (табл. 1.1).

Таблиця 1.1 – Типологія гібридних загроз за критерієм домену впливу

Тип загрози	*Характеристика*	*Інструменти реалізації*	*Приклади в енергетичній сфері*
Воєнні	Застосування збройних формувань, регулярних та нерегулярних	Збройні атаки, диверсії, блокади	Ракетні удари по енергоінфраструктурі України (2022-2025)
Енергетичні	Маніпулювання енергопостачанням як інструментом тиску	Ембарго, цінові війни, технічні обмеження	Припинення транзиту газу, блокування Північного потоку
Кібернетичні	Атаки на інформаційні системи критичної інфраструктури	Malware, DDoS-атаки, злам SCADA-систем	Атака BlackEnergy на українські енергомережі (2015–2016)
Інформаційні	Маніпулювання громадською думкою, поширення дезінформації	Фейкові новини, ІПСО, пропаганда	Наративи про «енергетичну кризу через відмову від РФ»

Економічні	Підрив економічної стабільності держави	Санкції, торгові війни, фінансові обмеження	Блокування експорту, обмеження інвестицій в енергосектор

Джерело: складено автором на основі [17; 20; 28; 55]

Аналіз таблиці 1.1 засвідчує, що енергетичні загрози посідають центральне місце в типології гібридних загроз, оскільки виступають водночас самостійним інструментом впливу та каталізатором загроз в інших доменах. Така особлива роль енергетичного домену зумовлена кількома чинниками. По-перше, енергетична інфраструктура є системоутворюючою для функціонування всіх інших секторів економіки та соціальної сфери – без стабільного енергопостачання неможливе функціонування транспорту, промисловості, медичних закладів, комунікаційних систем. По-друге, енергетичний сектор характеризується високою концентрацією критичних об'єктів, знищення або пошкодження яких має мультиплікативний ефект. По-третє, енергетична залежність традиційно використовується як інструмент геополітичного тиску, що робить цей сектор особливо вразливим до маніпуляцій з боку держав-постачальників енергоресурсів.

Експерти Центру передового досвіду НАТО з енергетичної безпеки (ENSEC COE) характеризують енергетичний сектор як «м'яке підчерев'я» критичної інфраструктури, вразливе до комплексного гібридного впливу [4]. За їхніми оцінками, саме поєднання фізичної вразливості енергооб'єктів, їх залежності від цифрових систем управління та стратегічного значення для національної економіки робить енергетику пріоритетною ціллю гібридних операцій. Досвід України 2015-2025 років повною мірою підтверджує цю тезу: від перших кібератак на енергомережі Прикарпаття у грудні 2015 року до систематичних ракетних та дронових ударів по генеруючих потужностях у 2022–2025 роках енергетичний сектор залишається одним із головних об'єктів гібридної агресії.

Важливим аспектом типологічного аналізу є взаємозв'язок між різними типами гібридних загроз. Як свідчить практика, окремі типи загроз рідко застосовуються ізольовано – натомість агресор прагне досягти синергетичного ефекту через їх комбінування. Так, кібератака на системи управління енергомережею може супроводжуватися інформаційною кампанією, спрямованою на підрив довіри населення до спроможності держави забезпечити

енергопостачання. Фізичне руйнування енергетичної інфраструктури посилюється економічним тиском через блокування імпорту необхідного обладнання для відновлення. Такий комплексний підхід значно ускладнює протидію, оскільки потребує координованих зусиль різних державних органів та міжнародних партнерів.

Окремої уваги заслуговує проблема атрибуції гібридних загроз, що є ключовою для їх типологізації та вибору адекватних заходів реагування. Якщо воєнні загрози (ракетні удари, диверсії) зазвичай можуть бути однозначно атрибутовані державі-агресору, то кібернетичні та інформаційні загрози часто реалізуються через проксі-структури, що ускладнює встановлення відповідальності. Це створює для агресора можливість заперечувати свою причетність (plausible deniability) та уникати міжнародно-правових наслідків. У сфері енергетичної безпеки така ситуація проявляється, зокрема, у використанні комерційних структур для реалізації політично мотивованих рішень щодо обмеження постачання енергоресурсів.

Порівняльний аналіз розглянутих типологій дозволяє виокремити їх сильні та слабкі сторони. Доменний підхід (НАТО, ЦЕНСС) забезпечує чітку структуризацію загроз за сферами впливу, проте недостатньо враховує їх взаємозв'язки та динаміку. Рівневий підхід (Погромський) дозволяє оцінити масштаб загрози, але не розкриває її змістовних характеристик. Крос-доменний підхід (Свейс та ін.) акцентує увагу на взаємодії між сферами, однак є складним для практичного застосування. Для цілей дослідження механізмів публічного управління у сфері енергетичної безпеки найбільш продуктивним видається поєднання доменного та рівневого підходів, що дозволяє одночасно ідентифікувати сферу загрози та оцінити її масштаб для калібровки відповідних заходів протидії.

Осмислення механізмів впливу гібридних загроз потребує звернення як до наукових досліджень, так і до доктринальних документів. У дослідженні гібридних загроз транспортній інфраструктурі Л.Ю. Величко та М.В. Білоконь виокремлюють три ключові характеристики механізмів гібридного впливу:

прихованість (складність атрибуції джерела загрози), мультидоменність (одночасне застосування різних інструментів) та асиметрія (експлуатація вразливостей при мінімальних витратах агресора) [43, с. 12]. Ці характеристики є універсальними і повною мірою застосовними до аналізу загроз енергетичній безпеці.

Британський дослідник М. Галеотті акцентує увагу на тому, що гібридна війна передбачає стирання меж між війною та миром, перетворюючи конфлікт на постійний стан [19, с. 27]. Така концептуалізація має важливе значення для розуміння механізмів впливу на енергетичний сектор, який зазнає систематичного тиску як у мирний час (через маніпуляції з постачанням), так і під час відкритого конфлікту (через фізичне руйнування інфраструктури).

Доктрина Герасимова, проаналізована А. Бартловим, обґрунтовує співвідношення 4:1 невоєнних та воєнних методів впливу в сучасних конфліктах [40, с. 165]. Серед невоєнних методів ключове місце займають економічний тиск, інформаційні операції та підтримка внутрішньої опозиції. Енергетичний шантаж у цій моделі виступає інструментом економічного та психологічного впливу одночасно.

Стратегія національної безпеки України (2020) визначає, що Російська Федерація, продовжуючи гібридну війну, системно застосовує політичні, економічні, інформаційно-психологічні, кібер- та воєнні засоби [69]. Документ наголошує на взаємопов'язаності різних форм гібридного впливу та необхідності комплексного підходу до протидії. Важливо, що Стратегія передбачає розробку окремої Стратегії енергетичної безпеки, що підтверджує визнання державою пріоритетності цього напряму.

Рамкова програма ЄС із протидії гібридним загрозам (EU Hybrid Threats Framework, 2016) пропонує операційний протокол реагування: виявлення → оцінка → відповідь [15]. Цей підхід передбачає координацію дій на рівні держав-членів, Європейської Комісії та інших інституцій ЄС. Для енергетичного сектора це означає необхідність інтеграції національних механізмів протидії до загальноєвропейської системи.

На підставі аналізу наукових та доктринальних джерел пропонуємо систематизацію механізмів впливу гібридних загроз на національну безпеку (табл. 1.2).

Таблиця 1.2 – Механізми впливу гібридних загроз на національну безпеку

Механізм	*Характеристика*	*Інструменти*	*Наслідки для енергетичної безпеки*
Синергетичний	Одночасне застосування різнорідних інструментів із кумулятивним ефектом	Комбінація кібератак, фізичних ударів та інформаційних операцій	Паралізація енергосистеми внаслідок атак на різні компоненти
Каскадний	Послідовне поширення наслідків атаки з одного сектора на інші	Ланцюгова реакція: енергетика → транспорт → виробництво → соціальна сфера	Системна криза внаслідок відключень електроенергії
Асиметричний	Досягнення максимального ефекту при мінімальних витратах агресора	Точкові атаки на вузлові елементи інфраструктури	Виведення з ладу трансформаторних підстанцій
Дестабілізаційний	Підрив довіри населення до держави та її інститутів	Створення дефіциту, провокування протестів, поширення паніки	Соціальне невдоволення через енергетичні кризи

Джерело: складено автором на основі [33; 43; 40; 15]

Синергетичний механізм передбачає координоване застосування інструментів впливу з різних доменів, що створює кумулятивний ефект, значно більший за суму окремих складових. Як зазначають експерти Національної академії наук України, саме синергія фізичних атак на енергоінфраструктуру з кібератаками на системи управління та інформаційними операціями забезпечила безпрецедентний руйнівний ефект російських ударів 2022-2023 років [59]. Характерним прикладом є масовані ракетні атаки жовтня-листопада 2022 року, коли фізичне руйнування генеруючих потужностей супроводжувалося DDoS-атаками на сайти енергокомпаній та інформаційною кампанією, спрямованою на залякування населення перспективою «холодної зими». Протидія

синергетичному механізму потребує не менш координованих дій з боку держави – синхронізації зусиль силових структур, операторів критичної інфраструктури та комунікаційних підрозділів.

Каскадний механізм описує ланцюгову реакцію поширення наслідків атаки з одного сектора на інші. У дослідженні економічної безпеки О.В. Кравчук зазначає, що енергетичний сектор є системоутворюючим, і його дестабілізація автоматично поширюється на транспорт, промисловість, сферу послуг та соціальну інфраструктуру [56, с. 15]. Саме тому енергетика є пріоритетним об'єктом гібридних атак. Каскадний ефект проявляється в чіткій послідовності: відключення електроенергії призводить до зупинки водопостачання та каналізації, що створює загрозу санітарно-епідеміологічній безпеці; припинення опалення в зимовий період загрожує життю та здоров'ю населення; зупинка транспорту паралізує економічну діяльність та логістичні ланцюги. Розуміння каскадної природи загроз є критично важливим для визначення пріоритетів захисту та відновлення інфраструктури.

Асиметричний механізм ґрунтується на експлуатації структурних вразливостей при мінімальних витратах агресора. За даними ACAPS, російські атаки на енергоінфраструктуру України були спеціально спрямовані на періоди пікового навантаження та зимовий період, що дозволяло досягати максимального руйнівного ефекту при обмежених ресурсах [1]. Асиметрія полягає в тому, що вартість однієї крилатої ракети є незрівнянно меншою за вартість знищеного нею трансформатора або турбіни, відновлення яких потребує місяців та значних інвестицій. Крім того, агресор обирає час атаки (зазвичай - пікові години споживання або початок опалювального сезону), тоді як захисник змушений підтримувати готовність постійно. Ця асиметрія витрат та зусиль є однією з ключових переваг гібридної стратегії.

Дестабілізаційний механізм спрямований на підрив довіри населення до держави та її спроможності забезпечити базові потреби. За оцінками DiXi Group, внаслідок атак Україна втратила понад 50 % генеруючих потужностей, що спричинило масштабну гуманітарну кризу та створило ґрунт для соціального

невдоволення [35]. Кінцевою метою дестабілізаційного механізму є не стільки фізичне руйнування, скільки підрив соціального контракту між державою та громадянами. Коли держава не може забезпечити базові потреби – тепло, світло, воду – легітимність влади ставиться під сумнів, що створює сприятливі умови для внутрішньої дестабілізації. Саме тому інформаційний супровід атак на енергоінфраструктуру є невід'ємною частиною гібридної стратегії: пропагандистські наративи про «неспроможність влади» та «марність опору» посилюють психологічний тиск на населення.

Особливого значення набуває роль публічного управління у протидії зазначеним механізмам. На думку М. Рюле з Оборонного коледжу НАТО, ефективна протидія гібридним загрозам потребує не лише військових спроможностей, а й комплексного підходу, що включає міжвідомчу координацію, державно-приватне партнерство та міжнародну співпрацю [31]. Це підкреслює центральну роль системи публічного управління в забезпеченні національної безпеки в умовах гібридних загроз.

Проведений аналіз дозволяє констатувати, що гібридні загрози є комплексним, багатовимірним явищем, яке характеризується поєднанням воєнних та невоєнних інструментів впливу, прихованістю атрибуції та спрямованістю на підрив національної безпеки без формального оголошення війни. Еволюція концепції від вузького воєнно-тактичного розуміння Ф. Гоффмана до сучасних комплексних підходів відображає ускладнення безпекового середовища та необхідність міждисциплінарного аналізу.

Типологія гібридних загроз охоплює воєнний, енергетичний, кібернетичний, інформаційний та економічний домени, кожен із яких має специфічні інструменти реалізації та наслідки для національної безпеки. При цьому енергетичний домен займає особливе місце, оскільки виступає як самостійним інструментом впливу, так і каталізатором загроз в інших сферах.

Механізми впливу гібридних загроз (синергетичний, каскадний, асиметричний та дестабілізаційний) потребують відповідних механізмів протидії з боку системи публічного управління. Саме ефективність державної

політики у сфері енергетичної безпеки визначає спроможність держави протистояти гібридним загрозам. Це зумовлює необхідність детального аналізу місця енергетичної безпеки в системі протидії гібридним загрозам, чому буде присвячено наступний підрозділ.

1.2 Енергетична безпека в системі протидії гібридним загрозам: поняття, місце та взаємозв’язки

Встановлена в попередньому підрозділі центральна роль енергетичного домену у структурі гібридних загроз зумовлює необхідність детального аналізу поняття «енергетична безпека» та його місця в системі національної безпеки. Досвід України 2014-2025 років засвідчив, що енергетичний сектор є не лише об'єктом гібридних атак, а й системоутворюючим елементом національної стійкості. Руйнування понад половини генеруючих потужностей внаслідок систематичних ракетних ударів, кібератаки на системи управління енергомережами, інформаційні кампанії, спрямовані на підрив довіри населення до спроможності держави забезпечити енергопостачання – усе це демонструє комплексний характер гібридних загроз в енергетичній сфері. Відтак, з’ясування сутності енергетичної безпеки, еволюції її розуміння та взаємозв'язків з іншими складовими національної безпеки є необхідною передумовою для формування ефективних механізмів публічного управління в цій сфері.

Концептуалізація поняття «енергетична безпека» має тривалу історію та зазнала суттєвої еволюції. Класичне визначення, запропоноване Міжнародним енергетичним агентством (МЕА), трактує енергетичну безпеку як неперервну доступність енергоресурсів за прийнятними цінами [24]. Це визначення, сформоване під впливом нафтових криз 1970-х років, акцентує увагу на двох ключових аспектах: фізичній доступності енергоресурсів та їх економічній прийнятності. Водночас МЕА розрізняє довгострокову енергетичну безпеку (своєчасні інвестиції в енергопостачання відповідно до економічного розвитку та екологічних потреб) та короткострокову (здатність енергосистеми оперативно реагувати на раптові зміни балансу попиту та пропозиції) [24].

Європейський підхід до енергетичної безпеки суттєво еволюціонував після газових криз 2006 та 2009 років. Європейська стратегія енергетичної безпеки (2014) визначає п’ять ключових вимірів: диверсифікація джерел та маршрутів

постачання, розвиток внутрішнього енергоринку, підвищення енергоефективності, нарощування власного виробництва та координація зовнішньої енергетичної політики [14]. Після повномасштабного вторгнення Росії в Україну у 2022 році план REPowerEU радикально переформатував європейський підхід, визначивши стратегічну мету повної незалежності від російських енергоносіїв та прискореного переходу до відновлюваних джерел енергії [14]. Таким чином, європейське розуміння енергетичної безпеки трансформувалося від вузького фокусу на безпеку постачання до комплексної концепції енергетичної стійкості (energy resilience).

Український підхід до визначення енергетичної безпеки закріплено в низці нормативно-правових актів та наукових досліджень. Енергетична стратегія України до 2050 року (2023) визначає енергетичну безпеку як надійне та економічно обґрунтоване забезпечення потреб суспільства та економіки в енергетичних продуктах [71]. Стратегія акцентує увагу на трьох пріоритетах: децентралізації енергетичної системи, диверсифікації джерел енергії та інтеграції до європейського енергетичного ринку. Принциповим є визнання енергетичної безпеки складовою національної безпеки та її зв’язку з кліматичною політикою [71].

Закон України «Про національну безпеку України» (2018, у редакції 2022 року) визначає енергетичну безпеку як один із секторів національної безпеки, що підлягає захисту від зовнішніх та внутрішніх загроз [66]. Закон встановлює інституційну рамку забезпечення енергетичної безпеки, включаючи повноваження Ради національної безпеки і оборони України, Кабінету Міністрів України та профільних міністерств. Важливим є зв’язок із Законом України «Про критичну інфраструктуру» (2021), який відносить об'єкти енергетичного сектора до критичної інфраструктури, що потребує особливого захисту [66].

Українська наукова думка пропонує власні підходи до концептуалізації енергетичної безпеки. О.П. Рябченко в дослідженні 2025 року визначає енергетичну безпеку як стан стабільного функціонування енергетичної системи держави без суттєвих перебоїв від зовнішніх або внутрішніх загроз [76].

Дослідниця наголошує на еволюції поняття від фокусу на фізичній доступності енергоресурсів до концепції енергетичної стійкості (resilience), що набула особливої актуальності в умовах повномасштабної війни. Принциповим є її висновок про енергетичну безпеку як фундамент національної безпеки в цілому [76].

Критичний аналіз наукових підходів дозволяє виокремити еволюцію концепції енергетичної безпеки через три етапи. Перший етап (1970-ті – 2000-ні роки) характеризувався фокусом на фізичній доступності енергоресурсів та стабільності цін. Цей підхід сформувався під впливом нафтових криз 1973 та 1979 років, коли арабські країни-експортери використали «нафтову зброю» проти західних держав. Основним завданням енергетичної політики на цьому етапі було забезпечення стабільних поставок вуглеводнів за прийнятними цінами, що досягалося через стратегічні резерви, довгострокові контракти та диверсифікацію постачальників.

Другий етап (2006–2022) був позначений увагою до диверсифікації джерел і маршрутів, енергоефективності та переходу до відновлюваних джерел. Газові кризи 2006 та 2009 років, спричинені конфліктами між Росією та Україною щодо транзиту, продемонстрували вразливість європейської енергетичної системи. На цьому етапі концепція енергетичної безпеки розширилася, включивши екологічний вимір (декарбонізація) та технологічний (розвиток відновлюваних джерел енергії). Паризька кліматична угода (2015) остаточно закріпила зв’язок між енергетичною безпекою та кліматичною політикою.

Третій етап (з 2022 року) характеризується домінуванням концепції енергетичної стійкості (resilience), що передбачає здатність енергосистеми протистояти гібридним загрозам, швидко відновлюватися після атак та адаптуватися до нових викликів. Повномасштабне вторгнення Росії в Україну кардинально змінило безпекову парадигму: енергетика з об'єкта економічної політики перетворилася на поле битви. Систематичні ракетні та дронові удари по українській енергоінфраструктурі продемонстрували, що класичні підходи до енергетичної безпеки є недостатніми в умовах гібридної війни. Концепція

resilience передбачає не лише захист від загроз, а й здатність до швидкого відновлення й адаптації, що потребує принципово нових підходів до проєктування, експлуатації та захисту енергетичних систем.

На підставі проведеного аналізу пропонуємо авторське визначення: енергетична безпека – це стан захищеності національних інтересів у сфері енергетики, що характеризується надійним та економічно обґрунтованим забезпеченням потреб суспільства в енергоресурсах, стійкістю енергетичної інфраструктури до зовнішніх і внутрішніх загроз, включаючи гібридні, та здатністю енергосистеми до швидкого відновлення після кризових ситуацій.

Визначення місця енергетичної безпеки в системі національної безпеки потребує аналізу як нормативно-правової бази, так і концептуальних підходів міжнародних організацій. НАТО визначає енергетичну безпеку як життєво важливий елемент стійкості (resilience) Альянсу до гібридних та кібернетичних загроз [29]. Саміт НАТО у Вільнюсі (2023) підтвердив, що захист критичної енергетичної інфраструктури є невід'ємною складовою колективної безпеки, а досвід України розглядається як ключовий для формування відповідних спроможностей союзників [29].

Дослідження Науково-технічної організації НАТО (STO) «Енергетична безпека в епоху гібридної війни» (2024) пропонує концептуальну модель місця енергетичної безпеки в системі протидії гібридним загрозам [27]. Згідно з цією моделлю, енергетика є одним із ключових доменів, у яких реалізуються гібридні загрози, поряд із кібернетичним, інформаційним та економічним доменами. Принциповим є висновок про каскадні ефекти (cascading effects): атаки на енергетичну інфраструктуру спричиняють ланцюгову реакцію в інших секторах – транспорті, комунікаціях, охороні здоров’я, промисловості [27].

М. Рюле та Ю. Груб’яускас у дослідженні для Оборонного коледжу НАТО (2015) обґрунтовують центральну роль енергетики в гібридних стратегіях сучасних конфліктів [32]. На їхню думку, енергетичний шантаж (зокрема газовий шантаж Росії щодо Європи) є типовим інструментом гібридної війни, що поєднує економічний тиск із психологічним впливом на населення та

політичним тиском на уряди [32]. Дослідники наголошують, що саме енергетична безпека стала ядром (core) національної безпеки як для НАТО, так і для України.

В українському контексті місце енергетичної безпеки визначається системою нормативно-правових актів. Стратегія національної безпеки України (2020) визнає енергетичну безпеку однією з ключових складових національної безпеки та наголошує на необхідності захисту енергетичної інфраструктури від гібридних загроз [66]. Енергетична стратегія до 2050 року (2023) конкретизує це положення, визначаючи три рівні забезпечення енергетичної безпеки: стратегічний (довгострокова політика диверсифікації та декарбонізації), оперативний (забезпечення надійності енергопостачання) та тактичний (захист критичної інфраструктури від атак) [71].

Особливого значення набуває інституційний вимір забезпечення енергетичної безпеки. Відповідно до чинного законодавства, ключову роль відіграють: Рада національної безпеки і оборони України (координація політики у сфері національної безпеки), Кабінет Міністрів України (формування та реалізація енергетичної політики), Міністерство енергетики (галузеве управління), Національна комісія з регулювання енергетики та комунальних послуг (регулювання ринків), оператори систем передачі та розподілу (технічне функціонування). Війна виявила необхідність посилення координації між цими інституціями та залучення нових акторів -Збройних Сил України (захист об'єктів), Державної служби з надзвичайних ситуацій (ліквідація наслідків атак), міжнародних партнерів (постачання обладнання для відновлення).

Важливим аспектом є зв'язок енергетичної безпеки з концепцією критичної інфраструктури. Закон України «Про критичну інфраструктуру» (2021) визначає об'єкти енергетичного сектора як критичну інфраструктуру, що потребує особливого захисту [66]. До таких об’єктів належать електростанції (атомні, теплові, гідро), магістральні лінії електропередач, трансформаторні підстанції, газотранспортна система, нафтопроводи та нафтопереробні заводи. Закон встановлює обов'язок операторів критичної інфраструктури розробляти плани

захисту та забезпечення безперервності функціонування, що є важливим елементом протидії гібридним загрозам.

Систематизація наукових та доктринальних підходів дозволяє запропонувати модель місця енергетичної безпеки в системі національної безпеки (табл. 1.3).

Таблиця 1.3 – Місце енергетичної безпеки в системі національної безпеки

Рівень	*Характеристика*	*Механізми забезпечення*
Стратегічний	Довгострокова політика енергетичної незалежності	Диверсифікація джерел, декарбонізація, інтеграція до ЄС
Оперативний	Надійність функціонування енергосистеми	Резервування потужностей, балансування попиту/пропозиції
Тактичний	Захист критичної інфраструктури	Фізичний захист, кіберзахист, протиповітряна оборона
Кризовий	Відновлення після атак	Аварійно-відновлювальні роботи, мобільні генератори, імпорт

Джерело: складено автором на основі [71; 29; 27; 32]

Енергетична безпека перебуває у складних взаємозв’язках з іншими складовими національної безпеки, що зумовлює необхідність комплексного підходу до її забезпечення. Аналіз цих взаємозв’язків дозволяє виокремити чотири ключові пари: енергетична – економічна безпека, енергетична – воєнна безпека, енергетична -кібербезпека та енергетична – соціальна стабільність.

Енергетична та економічна безпека. Взаємозв’язок між енергетичною й економічною безпекою є найбільш очевидним та добре дослідженим. В.В. Ксендзук у дослідженні 2024 року оцінює економічні втрати України від атак на енергоінфраструктуру в понад 10 мільярдів доларів США [57]. Ці втрати включають прямі збитки від руйнування об’єктів, витрати на відновлення, економічні втрати від зупинки виробництва та зниження ВВП через енергодефіцит. Водночас енергетичний сектор є ключовим для економічного зростання: за оцінками Секретаріату Енергетичної хартії, Україна втратила понад 50 % генеруючих потужностей внаслідок атак, що суттєво обмежує можливості економічного відновлення [10].

Енергетична та воєнна безпека. Зв’язок енергетичної та воєнної безпеки

набув особливої гостроти в умовах повномасштабної війни. Звіт NATO STO (2024) констатує, що енергетична інфраструктура стала пріоритетною воєнною ціллю, а її захист потребує інтеграції цивільних і військових зусиль [27]. Протиповітряна оборона енергетичних об'єктів, маскування та розосередження потужностей, швидке відновлення після атак – усе це потребує координації між енергетичним сектором та Збройними Силами. Водночас функціонування самих Збройних Сил залежить від надійного енергопостачання: паливо для техніки, електроенергія для систем зв'язку та управління, опалення казарм і шпиталів.

Енергетична безпека та кібербезпека. Взаємозалежність енергетичної та кібербезпеки є однією з найбільш критичних у сучасних умовах. Атаки BlackEnergy на українські енергомережі у 2015-2016 роках продемонстрували вразливість систем диспетчерського управління (SCADA) до кіберзагроз [27]. Ці атаки, здійснені російськими хакерськими групами, призвели до відключення електроенергії для сотень тисяч споживачів і стали першими в історії підтвердженими випадками кібератак, що спричинили реальні перебої в енергопостачанні.

Сучасні енергосистеми все більше залежать від цифрових технологій: автоматизовані системи управління, «розумні» мережі (smart grids), віддалений моніторинг – усе це створює нові вектори атак. Інтеграція інформаційних технологій в операційні процеси енергетики (IT/OT convergence) підвищує ефективність, але водночас розширює поверхню атаки. Кібератака на систему управління може мати такі самі наслідки, як фізичне руйнування об'єкта, але при значно менших витратах та ризиках для агресора.

Біла книга реформ VoxUkraine (2025) наголошує на необхідності посилення кіберзахисту енергетичної інфраструктури як пріоритету реформи сектора [38]. Серед рекомендацій – впровадження міжнародних стандартів кібербезпеки для критичної інфраструктури, створення галузевого центру реагування на кіберінциденти (CERT), регулярне тестування на проникнення та навчання персоналу. Важливим є також обмін інформацією про загрози між операторами, державними органами та міжнародними партнерами.

Енергетична безпека та соціальна стабільність. Зв’язок енергетичної безпеки із соціальною стабільністю є критично важливим для легітимності державної влади. А. Бобко в дослідженні 2024 року наголошує, що тривалі відключення електроенергії (blackouts) можуть спричинити соціальне невдоволення та протести, підриваючи довіру населення до держави [41]. Це особливо актуально в зимовий період, коли відсутність опалення й електроенергії створює загрозу життю та здоров’ю громадян. Енергетична бідність (energy poverty, нездатність домогосподарств забезпечити достатній рівень енергоспоживання) є додатковим чинником соціальної напруженості [41].

Досвід України взимку 2022-2023 років продемонстрував критичну роль енергетичної безпеки для соціальної стабільності. Масові відключення електроенергії, що тривали по 10-12 годин на добу, створили надзвичайно складні умови для населення: відсутність опалення, неможливість приготувати їжу, обмеження доступу до інформації та комунікацій. Проте, всупереч очікуванням агресора, ці випробування не підірвали підтримку населенням курсу на опір, а навпаки – консолідували суспільство. Це свідчить про те, що взаємозв'язок між енергетичною безпекою та соціальною стабільністю є більш складним, ніж лінійна залежність, і опосередковується такими чинниками, як рівень довіри до влади, розуміння причин кризи й наявність альтернативних джерел підтримки.

Окремої уваги заслуговує взаємозв’язок *енергетичної та екологічної безпеки,* який набуває дедалі більшого значення в контексті кліматичної політики. А. Бобко наголошує на необхідності врахування екологічних аспектів при забезпеченні енергетичної безпеки, зокрема переходу до відновлюваних джерел енергії як засобу одночасного досягнення енергетичної незалежності та декарбонізації [41]. Водночас війна створила нові екологічні виклики: пошкодження нафтопереробних заводів, витоки палива, ризики для ядерної безпеки (Запорізька АЕС). Це додатково ускладнює баланс між короткостроковими потребами енергопостачання та довгостроковими цілями екологічної безпеки.

Систематизація взаємозв'язків енергетичної безпеки з іншими складовими національної безпеки представлена в таблиці 1.4.

Таблиця 1.4 – Взаємозв'язки енергетичної безпеки з іншими складовими національної безпеки

Складова НБ	*Вплив енергетичної безпеки*	*Вплив на енергетичну безпеку*	*Приклади (Україна 2022–2025)*
Економічна	Енергозабезпечення виробництва, стабільність цін	Інвестиції в енергосектор, платоспроможність	Втрати $10+ млрд від атак
Воєнна	Паливо для ЗСУ, електроенергія для систем управління	ППО енергооб'єктів, воєнні пріоритети	Координація захисту ТЕС/ТЕЦ
Кібербезпека	Захист SCADA-систем, smart grids	Кібератаки на енергомережі	BlackEnergy, Industroyer
Соціальна	Опалення, освітлення, базові потреби	Громадська підтримка реформ	Blackout'и зими 2022–2023
Екологічна	Викиди, відходи, зелений курс	Екологічні обмеження, RES	Перехід до ВДЕ

Джерело: складено автором на основі [27; 57; 10; 38; 41]

Проведений аналіз засвідчує суттєву еволюцію концепції енергетичної безпеки – від вузького розуміння як фізичної доступності енергоресурсів до комплексної концепції енергетичної стійкості (resilience). В умовах гібридних загроз енергетична безпека набуває статусу системоутворюючого елемента національної безпеки, оскільки енергетичний сектор є одночасно об'єктом гібридних атак та фундаментом функціонування всіх інших секторів.

Запропоноване авторське визначення енергетичної безпеки як стану захищеності національних інтересів у сфері енергетики, що характеризується надійним забезпеченням потреб суспільства, стійкістю інфраструктури до загроз та здатністю до швидкого відновлення, враховує сучасні реалії гібридного протистояння й досвід України 2022-2025 років.

Місце енергетичної безпеки в системі національної безпеки визначається на чотирьох рівнях: стратегічному (довгострокова політика), оперативному (надійність енергопостачання), тактичному (захист інфраструктури) та

кризовому (відновлення після атак). Ефективна протидія гібридним загрозам потребує координації зусиль на всіх рівнях та інтеграції цивільних і військових спроможностей.

Взаємозв'язки енергетичної безпеки з економічною, воєнною, кібернетичною, екологічною безпекою та соціальною стабільністю мають двосторонній характер і зумовлюють необхідність комплексного, міжсекторального підходу до її забезпечення. Каскадні ефекти від атак на енергетичну інфраструктуру поширюються на всі сектори національної безпеки, що робить енергетику ключовим елементом стійкості держави до гібридних загроз. Це актуалізує потребу аналізу зарубіжного досвіду протидії гібридним загрозам в енергетичній сфері, чому буде присвячено наступний підрозділ.

РОЗДІЛ 2
АНАЛІЗ ПУБЛІЧНОГО УПРАВЛІННЯ ЕНЕРГЕТИЧНОЮ БЕЗПЕКОЮ УКРАЇНИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

2.1 Суб’єкти, механізми та інструменти публічного управління енергетичною безпекою в Україні

Теоретичне обґрунтування ролі публічного управління в забезпеченні енергетичної безпеки, здійснене в першому розділі, потребує конкретизації через аналіз інституційної архітектури та механізмів управління в Україні. Повномасштабна російсько-українська війна, що триває з 24 лютого 2022 року, продемонструвала як сильні сторони, так і критичні вразливості системи публічного управління енергетичним сектором. Систематичні ракетні та дронові атаки на енергетичну інфраструктуру виявили необхідність чіткого розмежування повноважень між органами влади, ефективної міжвідомчої координації та оперативного реагування на кризові ситуації. Відтак, аналіз суб'єктного складу та механізмів публічного управління енергетичною безпекою є необхідною передумовою для оцінки ефективності державної політики в цій сфері.

Публічне управління енергетичною безпекою України характеризується багаторівневою структурою, що включає органи стратегічного планування, галузевого регулювання та оперативного управління. Згідно із Законом України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII (із змінами), ключовими суб’єктами забезпечення національної безпеки у сфері енергетики є Рада національної безпеки і оборони України, Кабінет Міністрів України, Міністерство енергетики, галузеві регулятори та оператори критичної інфраструктури [66]. У Стратегії національної безпеки України, затвердженій Указом Президента України від 14 вересня 2020 року № 392/2020, енергетична

безпека визначена як один із пріоритетних секторів, що потребує комплексного захисту від зовнішніх та внутрішніх загроз, включаючи гібридні [70].

Стратегічний рівень управління представлений Радою національної безпеки і оборони України, яка відповідно до Конституції України та Закону України «Про національну безпеку України» координує та контролює діяльність органів виконавчої влади у сфері національної безпеки й оборони [66]. У контексті енергетичної безпеки цей орган здійснює стратегічне планування, приймає рішення щодо протидії загрозам критичній інфраструктурі та координує міжвідомчу взаємодію в кризових ситуаціях. В умовах повномасштабної війни роль РНБО суттєво зросла: саме цей орган ініціював низку рішень щодо посилення захисту енергетичної інфраструктури, введення надзвичайних заходів у сфері енергопостачання та координації міжнародної допомоги.

Загальне керівництво державною політикою у сфері енергетики здійснює Кабінет Міністрів України, який забезпечує її реалізацію через систему центральних органів виконавчої влади. Відповідно до Енергетичної стратегії України до 2050 року Кабмін визначає пріоритети розвитку енергетичного сектора, затверджує державні програми та забезпечує їх фінансування [71]. Важливим інструментом урядової політики став Проєкт Плану відновлення України (2022), який передбачає масштабну реконструкцію енергетичної інфраструктури з акцентом на децентралізацію та інтеграцію відновлюваних джерел енергії [73]. Уряд також координує залучення міжнародної технічної допомоги для відновлення енергетичного сектора та здійснює оперативне управління в кризових ситуаціях.

Центральним органом виконавчої влади, що забезпечує формування й реалізацію державної політики в електроенергетичному, ядерно-промисловому, нафтогазовому, вугільно-промисловому та торфодобувному комплексах, є Міністерство енергетики України. Відповідно до покладених функцій Міненерго розробляє нормативно-правові акти, здійснює стратегічне планування розвитку галузі, координує діяльність підприємств енергетичного сектора та представляє Україну в міжнародних енергетичних організаціях [71]. В умовах війни

Міністерство енергетики України набуло додаткових функцій щодо координації відновлювальних робіт, розподілу гуманітарної допомоги та взаємодії з міжнародними партнерами. Дослідники Л. Ю. Величко та М. В. Білоконь наголошують, що ефективність міжвідомчої координації між Міненерго та іншими органами (зокрема, Міністерством цифрової трансформації України) є критично важливою для протидії гібридним загрозам [43].

Особливе місце в системі публічного управління енергетичною безпекою посідає Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг (НКРЕКП). Відповідно до Закону України «Про Національну комісію, що здійснює державне регулювання у сферах енергетики та комунальних послуг» від 22 вересня 2016 року № 1540-VIII (із змінами, редакція від 28 серпня 2025 року), НКРЕКП є незалежним державним колегіальним органом, метою діяльності якого є державне регулювання, моніторинг та контроль за діяльністю суб’єктів господарювання у сферах енергетики та комунальних послуг [67].

Регуляторна діяльність Комісії охоплює такі сфери: виробництво, передача, розподіл та постачання електричної енергії; транспортування, розподіл та постачання природного газу; виробництво теплової енергії; централізоване водопостачання та водовідведення. До ключових повноважень НКРЕКП належать ліцензування діяльності у сферах енергетики, формування тарифної політики, затвердження правил ринку електричної енергії та природного газу, контроль за дотриманням ліцензійних умов, а також захист прав споживачів [67].

В умовах російсько-української війни роль НКРЕКП суттєво трансформувалася. Комісія забезпечує оперативне регулювання в умовах надзвичайних ситуацій: затверджує тимчасові порядки роботи ринку електроенергії в умовах дефіциту потужностей, регулює тарифи для забезпечення фінансової стійкості енергокомпаній, координує відновлення ліцензійної діяльності на деокупованих територіях. Зокрема, Постанова НКРЕКП «Про затвердження Тимчасового порядку врегулювання відносин на ринку електричної енергії» від 12 квітня 2022 року № 386 встановила механізми

функціонування ринку в умовах воєнного стану, що дозволило зберегти базові ринкові принципи навіть в умовах масованих атак на інфраструктуру [64].

Водночас дослідники вказують на певні проблеми в діяльності регулятора. Зокрема, С. М. Бугазіянус наголошує на фрагментації управлінських повноважень між НКРЕКП, Міненерго та іншими органами, що ускладнює прийняття оперативних рішень у кризових ситуаціях [42]. Крім того, незалежність регулятора періодично ставиться під сумнів через політичний тиск щодо тарифних рішень. Експерти Європейського центру Енергетичної хартії рекомендують посилення інституційної незалежності НКРЕКП як передумову ефективного функціонування енергетичних ринків [10].

Важливу роль у системі публічного управління енергетичною безпекою відіграють оператори критичної інфраструктури, які забезпечують безпосереднє функціонування енергетичних систем. Відповідно до Закону України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX (із змінами, редакція від 21 вересня 2024 року), до об'єктів критичної інфраструктури в енергетичному секторі належать об'єкти генерації електроенергії (атомні, теплові, гідроелектростанції), магістральні електромережі та трансформаторні підстанції, газотранспортна система, а також об’єкти зберігання нафти й газу [65].

Ключову роль у забезпеченні стабільного функціонування об’єднаної енергетичної системи України відіграє Національна енергетична компанія «Укренерго» як оператор системи передачі електроенергії. Закон України «Про ринок електричної енергії» від 13 квітня 2017 року № 2019-VIII (із змінами, редакція від 28 серпня 2025 року) визначає оператора системи передачі як суб’єкта господарювання, що здійснює передачу електроенергії магістральними й міждержавними електромережами, забезпечує диспетчерське управління та відповідає за балансування системи [68]. В умовах війни компанія виконує критичну функцію оперативного управління енергосистемою в умовах постійних атак та дефіциту генеруючих потужностей: координує графіки обмежень споживання, організовує аварійні відключення й забезпечує

синхронну роботу з європейською енергосистемою ENTSO-E.

Доставку електроенергії кінцевим споживачам на регіональному рівні забезпечують оператори систем розподілу (ОСР). В Україні функціонує понад 30 ОСР, найбільшими з яких є компанії групи ДТЕК, АТ «Харківобленерго», АТ «Львівобленерго». Ці оператори відповідають за технічний стан розподільчих мереж, оперативне усунення аварій і відновлення електропостачання після атак. Законодавство про ринок електроенергії встановлює вимоги до якості послуг ОСР, включаючи показники надійності та нормативні терміни відновлення електропостачання [68].

Функціонування газотранспортної системи забезпечує АТ «Оператор ГТС України», який здійснює транспортування природного газу територією України, включаючи транзит до європейських країн. Газотранспортна система України є однією з найбільших у Європі та має стратегічне значення для енергетичної безпеки континенту. В умовах війни оператор ГТС забезпечує безперебійне постачання газу споживачам, попри систематичні атаки на газову інфраструктуру [71].

Найбільшою державною енергетичною компанією є НАК «Нафтогаз України», що здійснює видобуток, транспортування та постачання природного газу. Компанія відіграє ключову роль у забезпеченні енергетичної безпеки через формування запасів газу в підземних сховищах, імпорт газу з альтернативних джерел та постачання газу населенню й промисловості. Проєкт Плану відновлення України передбачає реформування корпоративного управління «Нафтогазу» для підвищення ефективності та прозорості [73].

Механізми публічного управління енергетичною безпекою являють собою сукупність інструментів, методів та процедур, що використовуються органами влади для досягнення цілей державної політики у сфері енергетики. Дослідник С. М. Бугазіянус визначає механізм публічного управління як цілісну систему практичних заходів, засобів, важелів і стимулів, за допомогою яких органи влади здійснюють цілеспрямований вплив на енергетичну сферу [42]. У науковій літературі виокремлюють організаційно-правовий механізм управління

енергетичною безпекою як багаторівневу систему, що інтегрує нормативно-правові акти, інституційні структури, функціональні процедури та інструменти впливу.

Нормативно-правовий механізм включає систему законів, підзаконних актів та регуляторних документів, що визначають правила функціонування енергетичного сектора. Базовими законодавчими актами є Закон України «Про ринок електричної енергії» від 13 квітня 2017 року № 2019-VIII, Закон України «Про ринок природного газу» від 9 квітня 2015 року № 329-VIII, Закон України «Про Національну комісію, що здійснює державне регулювання у сферах енергетики та комунальних послуг» від 22 вересня 2016 року № 1540-VIII та Закон України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX. Ці закони імплементують вимоги Третього енергетичного пакету ЄС та створюють правову основу для функціонування конкурентних енергетичних ринків [67].

Інституційний механізм передбачає розподіл повноважень між органами публічної влади та забезпечення їх координації. Дослідники А. Л. Помаза-Пономаренко й Д. В. Тарадуда наголошують на подвійній ролі вітчизняних державних органів у протистоянні гібридній війні: відстоювання суверенітету та територіальної цілісності, а також захист енергетичної безпеки й об'єктів критичної інфраструктури [63]. Науковці акцентують увагу на необхідності посилення міжвідомчої координації та залучення міжнародної технічної допомоги, зокрема з боку НАТО.

Економічний механізм включає інструменти тарифної політики, інвестиційного стимулювання та фінансової підтримки енергетичного сектора. Тарифне регулювання здійснює НКРЕКП з метою забезпечення фінансової стійкості енергокомпаній та доступності енергоресурсів для споживачів. Законодавство про ринок електроенергії передбачає механізми підтримки відновлюваної енергетики («зелений» тариф, аукціони) та спеціальні обов'язки для забезпечення загальносуспільних інтересів [68]. В умовах війни економічний механізм доповнено інструментами державної підтримки для відновлення

пошкодженої інфраструктури й компенсації збитків енергокомпаніям.

Технологічний механізм передбачає впровадження інноваційних рішень для підвищення надійності та захищеності енергосистеми. До таких рішень належать системи автоматизованого управління (SCADA), інтелектуальні мережі (smart grid), системи накопичення енергії, розподілена генерація. Дослідники Л. Ю. Величко та М. В. Білоконь зазначають, що кібербезпека енергетичних систем є критичним елементом технологічного механізму, враховуючи зростаючу кількість кібератак на об'єкти критичної інфраструктури [43].

Механізм міжнародної співпраці забезпечує інтеграцію України до європейського енергетичного простору та залучення міжнародної підтримки. Ключовими напрямами є синхронізація з континентальною європейською енергосистемою ENTSO-E (реалізована в березні 2022 року), участь в Енергетичному Співтоваристві, співробітництво з Міжнародним енергетичним агентством (МЕА). Спільна робоча програма Україна-МЕА на 2025-2026 роки визначає пріоритети співпраці у сферах енергетичної безпеки, відновлення інфраструктури та чистої енергетичної трансформації [21].

Систематизація суб'єктів та механізмів публічного управління енергетичною безпекою дозволяє представити їх у формі узагальнюючої таблиці (табл. 2.1).

Таблиця 2.1 – Суб'єкти та механізми публічного управління енергетичною безпекою України

Суб'єкт	*Рівень управління*	*Основні функції*	*Ключові механізми*
РНБО	Стратегічний	Координація політики нацбезпеки, прийняття рішень щодо загроз КІ	Рішення РНБО, укази Президента
Кабмін	Стратегічний/ Оперативний	Формування держполітики, затвердження програм	Постанови, розпорядження, держпрограми
Міненерго	Галузевий	Галузеве управління, нормотворчість	НПА, координація, стратегії
НКРЕКП	Регуляторний	Тарифоутворення, ліцензування, контроль	Постанови, ліцензії, тарифи

Продовження таблиці 2.1

Суб'єкт	*Рівень управління*	*Основні функції*	*Ключові механізми*
НЕК «Укренерго»	Операційний	Передача електроенергії, диспетчеризація	Технічне управління, балансування
ОСР	Операційний	Розподіл електроенергії, обслуговування мереж	Технічне обслуговування, відновлення
Оператор ГТС	Операційний	Транспортування газу, транзит	Технічне управління ГТС
НАК «Нафтогаз»	Операційний	Видобуток, постачання газу	Закупівлі, зберігання, постачання

Джерело: складено автором на основі [71; 66; 70; 67; 65; 68]

Представлена таблиця демонструє чітку ієрархію суб’єктів публічного управління енергетичною безпекою, від стратегічного рівня до операційного. Така багаторівнева структура забезпечує розподіл функцій та відповідальності, проте водночас створює виклики для ефективної координації, особливо в кризових ситуаціях. Як свідчить досвід російсько-української війни, оперативність прийняття рішень значною мірою залежить від налагодженості горизонтальних зв’язків між суб’єктами різних рівнів управління.

Окрім інституційних механізмів, публічне управління енергетичною безпекою спирається на систему інструментів, спрямованих на підвищення стійкості енергетичної системи до зовнішніх і внутрішніх загроз. За функціональним призначенням ці інструменти можна класифікувати на чотири групи: превентивні (запобігання загрозам), захисні (мінімізація наслідків), відновлювальні (швидке повернення до нормального функціонування) та адаптаційні (пристосування до нових умов).

До превентивних інструментів належать система моніторингу загроз критичній інфраструктурі, що функціонує у взаємодії зі Службою безпеки України та розвідувальними органами; програми технічного обслуговування та модернізації об’єктів енергетичної інфраструктури; заходи кібербезпеки, включаючи захист систем SCADA й автоматизованих систем управління; навчання персоналу та проведення регулярних тренувань з реагування на надзвичайні ситуації [43].

Захисні інструменти включають фізичний захист об’єктів критичної інфраструктури (огородження, контроль доступу, відеоспостереження), протиповітряну оборону стратегічних енергетичних об'єктів, резервування критичних компонентів та систем, а також диверсифікацію джерел енергопостачання. Законодавство про критичну інфраструктуру зобов’язує операторів розробляти плани захисту й забезпечення безперервності функціонування, що є важливим елементом системи захисту [65].

Відновлювальні інструменти спрямовані на швидке відновлення функціонування енергосистеми після атак або аварій. До них належать аварійні запаси обладнання та матеріалів, мобільні генераторні установки, системи оперативного реагування й координації відновлювальних робіт, а також міжнародні механізми надання допомоги (зокрема Механізм енергетичної підтримки ЄС). Досвід зими 2022-2023 років продемонстрував критичну важливість наявності достатніх запасів обладнання для швидкого відновлення пошкодженої інфраструктури [10].

Адаптаційні інструменти передбачають трансформацію енергетичної системи для підвищення її стійкості до нових типів загроз. До таких інструментів належать децентралізація генерації через розвиток розподілених енергетичних ресурсів, впровадження накопичувачів енергії, розвиток відновлюваних джерел енергії, менш вразливих до централізованих атак, а також перехід на більш гнучкі та адаптивні технології управління мережами [42].

Ефективне публічне управління енергетичною безпекою в умовах гібридних загроз потребує налагодження дієвих механізмів міжвідомчої координації. Традиційна модель галузевого управління, де кожен орган діє переважно в межах своєї компетенції, виявилася недостатньо ефективною для протидії комплексним загрозам, що одночасно охоплюють кілька секторів. За висновками С. М. Бугазіянуса, фрагментація управлінських повноважень є однією з ключових проблем публічного управління енергетичною безпекою в Україні [42].

В умовах повномасштабної російської агресії сформувалися нові

координаційні механізми. На рівні РНБО функціонують ситуаційні центри, що забезпечують оперативний моніторинг загроз і координацію реагування. Створено оперативні штаби на рівні Кабміну та Міненерго для координації відновлювальних робіт після атак на інфраструктуру. Важливим елементом є координація з Міністерством оборони та Збройними Силами України щодо захисту енергетичних об'єктів засобами протиповітряної оборони.

У дослідженні НАТО «Енергетична безпека в епоху гібридної війни» (2023) акцентовано увагу на необхідності інтегрованого підходу до захисту критичної енергетичної інфраструктури [27]. Рекомендації дослідження включають створення спеціалізованих міжвідомчих структур для координації захисту критичної інфраструктури, розвиток системи раннього попередження про загрози, забезпечення резервування критичних функцій, налагодження взаємодії з приватним сектором та міжнародними партнерами. Україна частково імплементувала ці рекомендації, проте потребує подальшого вдосконалення координаційних механізмів [63].

Особливого значення набуває координація з міжнародними партнерами. Синхронізація української енергосистеми з ENTSO-E в березні 2022 року стала історичним досягненням, що суттєво підвищило енергетичну безпеку країни. Цей крок забезпечив можливість імпорту електроенергії з ЄС у періоди дефіциту та зменшив залежність від російської енергосистеми [21]. Подальше поглиблення інтеграції передбачає збільшення пропускної спроможності міждержавних перетинів та гармонізацію правил ринку з вимогами Європейського Союзу.

Науковці М. Гранд та О. Свйонтик у своєму історіографічному дослідженні (2025) систематизували бачення українських і закордонних учених щодо пріоритетних завдань зміцнення енергетичної безпеки України в умовах російсько-української війни. Дослідники визначили такі ключові напрями: збільшення виробництва енергоресурсів з метою імпортозаміщення, створення стратегічних запасів енергоносіїв, диверсифікація джерел постачання, розвиток альтернативної енергетики, забезпечення кібербезпеки енергетичної

інфраструктури та вдосконалення системи державного регулювання і управління енергетичною сферою [48]. Ці пріоритети значною мірою корелюють із завданнями, визначеними у Стратегії національної безпеки України та Енергетичній стратегії України до 2050 року.

Важливий внесок у розуміння перспектив розвитку публічного управління енергетичною безпекою зробив Є. В. Кисельов (2024), який акцентував увагу на необхідності системного вдосконалення механізмів державного регулювання та управління енергетичним сектором в умовах сучасних викликів [53]. Дослідник наголошує на важливості адаптації інституційних механізмів до нових реалій і посилення їх спроможності реагувати на гібридні загрози.

Методологічні засади формування системи управління ризиками енергетичної безпеки розроблено в монографії О. М. Суходолі, Ю. М. Харазішвілі та Г. Л. Рябцева (2023), підготовленій у Національному інституті стратегічних досліджень. Автори обґрунтували комплексний підхід до оцінювання рівня енергетичної безпеки та стратегування, що враховує багатофакторність загроз і необхідність інтеграції різних компонентів системи управління [80]. Ці напрацювання є важливою науковою основою для вдосконалення механізмів публічного управління енергетичною безпекою.

Проведений аналіз засвідчує, що система публічного управління енергетичною безпекою України має багаторівневу структуру, яка включає органи стратегічного планування (РНБО, Кабінет Міністрів України), галузевого управління (Міністерство енергетики), регулювання (НКРЕКП) та операторів критичної інфраструктури (НЕК «Укренерго», НАК «Нафтогаз», оператори систем розподілу). Кожен суб'єкт виконує специфічні функції, що в сукупності забезпечують формування та реалізацію державної політики у сфері енергетичної безпеки.

Механізми публічного управління енергетичною безпекою включають нормативно-правовий, інституційний, економічний, технологічний і міжнародний компоненти. Ці механізми забезпечують правове регулювання, координацію діяльності органів влади, стимулювання інвестицій, впровадження

інновацій та інтеграцію до європейського енергетичного простору.

Повномасштабна російсько-українська війна, що триває з 24 лютого 2022 року, виявила як сильні сторони, так і вразливості системи публічного управління. До сильних сторін належать оперативність реагування на кризові ситуації, здатність до швидкої адаптації регуляторних механізмів, ефективна координація міжнародної допомоги. Водночас виявлено проблеми фрагментації управлінських повноважень, недостатньої міжвідомчої координації та вразливості інституційної незалежності регулятора. Ці проблеми потребують системного вирішення для підвищення ефективності публічного управління енергетичною безпекою, що буде проаналізовано в наступному підрозділі.

2.2 Аналіз ефективності публічного управління у протидії гібридним загрозам в енергетичному секторі України

Повномасштабна російсько-українська війна, що триває з 24 лютого 2022 року, перетворила енергетичний сектор України на один із ключових об'єктів гібридної агресії. Систематичні ракетні та безпілотні удари по об'єктах енергетичної інфраструктури поставили безпрецедентні виклики перед системою публічного управління, вимагаючи миттєвої адаптації механізмів державного регулювання до умов активних бойових дій. Аналіз ефективності цієї системи потребує збалансованої оцінки як позитивних здобутків, так і критичних недоліків, що проявилися в умовах реальної кризи. Методологічною основою такого аналізу є системний підхід, що передбачає дослідження взаємозв’язків між різними суб'єктами управління, оцінку їх функціональної спроможності та виявлення структурних диспропорцій у механізмах реагування на загрози.

Актуальність дослідження ефективності публічного управління енергетичною безпекою в умовах війни визначається не лише масштабами

завданих збитків, а й необхідністю формування теоретичної бази для вдосконалення системи антикризового реагування. Традиційні моделі управління енергетичним сектором, розроблені для мирного часу, виявилися недостатньо адаптованими до умов систематичних цілеспрямованих атак на критичну інфраструктуру. Це актуалізує потребу в критичному переосмисленні існуючих підходів та розробці нових механізмів забезпечення енергетичної стійкості.

Масштаби завданих збитків енергетичній інфраструктурі засвідчують безпрецедентність викликів для системи публічного управління. За даними аналітичного центру DiXi Group, протягом 2022-2024 років Росія здійснила 25 масованих атак на енергетику України, внаслідок яких було втрачено близько 21 гігават генеруючих потужностей, а додаткові удари 2024 року знищили ще 9 гігават [8]. Звіт Моніторингової місії ООН з прав людини зафіксував, що атаки 2024 року завдали втричі більше шкоди генеруючим потужностям порівняно з ударами взимку 2022-2023 років, знищивши близько 9 гігават електрогенерації – еквівалент половини зимових потреб країни [36]. Міжнародне енергетичне агентство констатувало, що станом на середину 2024 року Україна втратила близько двох третин диспетчерської потужності електрогенерації, а 73 відсотки теплових електростанцій було виведено з ладу [22]. Ці дані формують контекст для оцінки ефективності управлінських рішень в умовах екстремального тиску та безперервного руйнування інфраструктурних об'єктів.

Методологія аналізу ефективності публічного управління у сфері енергетичної безпеки базується на зіставленні задекларованих цілей із фактичними результатами діяльності органів влади. При цьому враховуються як кількісні показники – обсяги відновлених потужностей, терміни реагування на кризові ситуації, рівень покриття потреб споживачів, – так і якісні характеристики – ступінь міжвідомчої координації, адаптивність нормативно-правової бази, ефективність комунікації з міжнародними партнерами. Такий комплексний підхід дозволяє уникнути однобічних оцінок та сформувати цілісне уявлення про функціонування системи управління в екстремальних умовах.

Структура аналізу передбачає послідовний розгляд позитивних досягнень та негативних аспектів функціонування системи публічного управління енергетичною безпекою, що забезпечує збалансованість оцінок і дозволяє виявити причинно-наслідкові зв’язки між управлінськими рішеннями та їх результатами. Особлива увага приділяється синтезу наукових підходів вітчизняних і зарубіжних дослідників, що дозволяє врахувати різні перспективи й методологічні традиції в оцінці ефективності державного управління кризовими ситуаціями.

Об'єктивний аналіз результатів антикризового управління енергетичним сектором передбачає насамперед виокремлення тих сфер, де органи публічної влади продемонстрували високу ефективність. Такий підхід дозволяє ідентифікувати успішні практики, які можуть бути масштабовані та застосовані в інших секторах критичної інфраструктури.

Безперечним досягненням стала екстрена синхронізація об'єднаної енергосистеми України з континентальною електромережею ENTSO-E. Це рішення, реалізоване всього за три тижні замість запланованих півтора року, стало одним із найуспішніших прикладів міжінституційної координації в історії української енергетики [12]. Синхронізація відбулася 16 березня 2022 року після екстреного запиту НЕК «Укренерго», підтриманого міністрами енергетики країн ЄС, і стала можливою завдяки попередній підготовчій роботі, розпочатій ще у 2017 році за підтримки USAID [37]. Надзвичайно важливим є той факт, що за три дні до початку повномасштабного вторгнення українська енергосистема успішно пройшла тестове відключення від російської та білоруської мереж, працюючи в ізольованому режимі. У листопаді 2023 року ENTSO-E офіційно підтвердила завершення проєкту синхронізації після виконання «Укренерго» всіх ключових технічних вимог, а з 1 січня 2024 року український оператор системи передачі став повноправним 40-м членом асоціації [13]. Цей успіх демонструє спроможність органів публічного управління до ефективної стратегічної координації за наявності чіткого бачення, професійної підготовки й міжнародної підтримки.

Інтеграція з європейською енергосистемою забезпечила критично важливу гнучкість у періоди найгострішого дефіциту потужностей. У 2024 році Україна імпортувала рекордні 4 436 гігават-годин електроенергії, що дозволило пом'якшити наслідки масованих атак на генеруючі об'єкти [22]. Улітку 2024 року, коли генеруючі потужності впали більш ніж на 2,3 гігават нижче пікового попиту в 12 гігават, саме імпорт електроенергії від європейських партнерів дозволив уникнути критичних віялових відключень. Водночас у період із червня по вересень 2025 року, коли генеруючі потужності було частково відновлено, країна стала нетто-експортером електроенергії, досягнувши у вересні показника 635 гігават-годин місячного експорту – найвищого рівня з початку повномасштабного вторгнення [22]. Така динаміка засвідчує здатність системи управління не лише реагувати на кризи, а й використовувати можливості для економічного розвитку в умовах війни. З грудня 2024 року потужність імпорту встановлено на рівні 2,1 гігават у зимові місяці та 1,7 гігават улітку, що забезпечує необхідний резерв для стабілізації енергосистеми.

Курс на децентралізацію енергосистеми становить стратегічне досягнення системи публічного управління, що виходить за межі суто антикризового реагування та закладає фундамент для трансформації всієї архітектури енергетичного сектора. За даними Державного агентства з енергоефективності та енергозбереження України (САЕЕ), розподілена генерація стала основою для формування енергетично незалежних громад, дозволяючи знизити залежність від централізованих мереж і забезпечити стабільність у критичних ситуаціях [77]. Фонд декарбонізації України вже реалізував 54 проєкти з розподіленої генерації в 11 регіонах країни, що доводить практичну життєздатність цього підходу навіть в умовах активних бойових дій [77]. Станом на початок 2024 року встановлена потужність споживчих сонячних електростанцій досягла майже 1 500 мегават, продовжуючи стабільно зростати попри воєнні ризики [22].

Стратегія розвитку розподіленої генерації на період до 2035 року, прийнята 18 липня 2024 року, визнала вразливість централізованої побудови

об'єднаної енергетичної системи в умовах збройної агресії та закріпила необхідність прискореного будівництва нової розподіленої генерації [46]. Як зазначають експерти GoLaw, розподілена генерація надає низку вагомих переваг: підвищення надійності та стійкості енергосистеми, зменшення втрат при передачі електроенергії, забезпечення енергетичної незалежності громад та екологічність через використання відновлюваних джерел [46]. Особливо важливим є те, що пошкодження локальних джерел енергії вимагає мінімального часу для відновлення, на відміну від великих централізованих об'єктів, і не призводить до каскадних відключень.

Досвід України у сфері посилення стійкості енергосистеми привернув увагу міжнародної спільноти. За даними DiXi Group, на конференції Міжнародного енергетичного агентства в Парижі (вересень-жовтень 2024 року) українські експерти презентували підходи до функціонування енергетичного сектора в умовах війни та досвід, які можуть бути корисними для інших країн [6]. Модель поєднання децентралізації й модульності викликала інтерес представників Польщі та країн Балтії, що засвідчує формування нового напряму у глобальній дискусії про енергетичну безпеку критичної інфраструктури.

Законодавча підтримка сектора відновлюваної енергетики демонструє адаптивність системи управління до мінливих умов та здатність до проактивного нормотворення. Прийняття Закону України № 3141-IX від 10 червня 2023 року продовжило терміни введення в експлуатацію об’єктів вітрової енергетики та запровадило механізми протидії зловживанням на оптових енергетичних ринках відповідно до Регламенту ЄС REMIT [34]. Закон про «зелену» трансформацію енергетичної системи від 30 червня 2023 року надав можливість отримання відстрочок до 31 грудня 2025 року, враховуючи об’єктивні труднощі з логістикою та постачанням обладнання в умовах порушених ланцюгів постачання [34]. Особливо важливим є те, що перші проєкти у 2023 році отримали страхування політичних ризиків, включаючи воєнні, від міжнародних організацій, зокрема MIGA, що створило передумови для залучення приватних інвестицій навіть у період активних бойових дій [34].

Координація міжнародної допомоги стала критичним фактором виживання енергетичного сектора та водночас продемонструвала здатність українських органів влади до ефективної взаємодії з широким колом міжнародних партнерів. За даними Міністерства енергетики, завдяки партнерству з ПРООН і внескам дев'яти країн-донорів Україна забезпечила постачання та встановлення енергетичного обладнання загальною потужністю понад 450 мегават у Києві, Харкові, Запоріжжі, Одесі, Дніпропетровській та Миколаївській областях [23]. Програма Ukraine Facility передбачає надання 50 мільярдів євро на підтримку України впродовж 2024-2027 років, із яких значна частина спрямовується на відновлення енергетичної інфраструктури [16]. Ефективна інтеграція цієї допомоги в національні програми відновлення, включаючи План відновлення України, свідчить про спроможність органів влади до стратегічної координації з міжнародними партнерами та формування єдиного бачення пріоритетів розвитку енергетичного сектора.

Попри очевидні досягнення, системний аналіз виявляє суттєві недоліки в організації публічного управління енергетичною безпекою, які знижують загальну ефективність системи та створюють передумови для повторення кризових ситуацій. Ці недоліки мають як структурний характер, пов'язаний з архітектурою системи управління, так і функціональний, що стосується якості реалізації окремих управлінських процесів.

Фундаментальною проблемою залишається фрагментація повноважень між органами влади. Дослідження з проблем реалізації державної енергетичної політики (2024) констатує: до семи різних органів дублюють функції моніторингу критичної інфраструктури, що призводить до розмивання відповідальності за кінцеві результати [81]. Кожен із цих органів – Верховна Рада, Кабінет Міністрів, Міністерство енергетики, НКРЕКП, Рада національної безпеки, профільні комітети та регіональні адміністрації – має власне бачення пріоритетів і власні інформаційні системи, що ускладнює формування цілісної картини стану енергетичної безпеки та оперативне реагування на загрози.

Дослідження проблем енергетичної політики з погляду національної

безпеки (2024) виявило додаткові системні недоліки: проблеми енергетичної корупції, яка послаблює регулювання галузі та створює дисбаланс на ринку, недостатній рівень модернізації інфраструктури й обмежене фінансування, низьку інвестиційну привабливість сектора та відсутність довгострокової державної стратегії, адаптованої до воєнних умов [72]. Автор наголошує, що корупційні ризики знижують довіру міжнародних партнерів і ускладнюють залучення необхідних інвестицій у відновлення інфраструктури.

Критичний аналіз Енергетичної стратегії України виявляє відсутність чітких механізмів персональної відповідальності посадовців за невиконання стратегічних завдань та функціонування розрізнених баз даних без інтеграції в єдину інформаційну систему [50]. Ця проблема набуває особливої гостроти в умовах війни, коли швидкість і точність інформаційного обміну є критичними для прийняття ефективних рішень. Стратегічні документи, розроблені до 2022 року, не передбачали сценаріїв систематичних ракетних ударів по енергетичній інфраструктурі, що засвідчує недостатню увагу до сценарного планування на етапі їх розробки та потребу в суттєвому перегляді підходів до стратегічного планування у сфері енергетичної безпеки.

Особливо гострою залишається проблема захисту критичної інфраструктури від повторних ударів, що свідчить про недостатню ефективність превентивних механізмів. Масштабна комбінована атака 26 серпня 2024 року, коли Росія застосувала 127 ракет різних типів та 109 ударних безпілотників, завдала значних руйнувань енергетичній інфраструктурі в 15 областях, змусивши «Укренерго» запровадити екстрені відключення електроенергії по всій країні [18]. Попри значні зусилля з фізичного захисту об'єктів, включаючи будівництво захисних споруд та диверсифікацію точок розташування обладнання, система раннього попередження та інженерного укріплення залишається недостатньою для протидії сучасним високоточним засобам ураження.

Проблема горизонтальної координації між різними рівнями управління проявляється у складнощах взаємодії центральних органів виконавчої влади з

операторами критичної інфраструктури та місцевими органами влади. Особливо гостро ця проблема відчувається у прифронтових регіонах, де локальні особливості ситуації потребують гнучкого реагування, яке не завжди може бути забезпечене централізованими рішеннями. Атаки дедалі частіше призводять до розділення добре забезпечених західних регіонів від східних територій поблизу лінії фронту, які часто відчувають дефіцит електроенергії [22]. Перевантаження міждержавних перетинів та обмежена пропускна здатність внутрішніх мереж створюють ситуацію, коли імпортована електроенергія не може бути доставлена до тих споживачів, які найбільше її потребують.

Важливим аспектом, який часто залишається поза увагою при формуванні державної політики, є соціальний вимір енергетичної кризи. Дослідження «Гендерний вимір енергетичної кризи в Україні: шляхи до стійкості» (2025), проведене Жіночим енергетичним клубом України за підтримки UN Women, засвідчило нерівномірний вплив енергетичної нестабільності на різні групи населення [51]. Зокрема, 90 % опитаних погодилися, що жінкам стало важче піклуватися про дітей і родичів через перебої з електрикою та водопостачанням, а найвразливішими до кризи виявилися жінки з дітьми (65 %), люди з інвалідністю (64 %) та люди літнього віку (63 %) [51]. При цьому лише 5 % опитаних повідомили про отримання підтримки від держави, що засвідчує критичний розрив між потребами населення та спроможністю системи соціального захисту. Особливо важка ситуація склалася на Південному Сході країни – 48 % жінок із цього регіону оцінили вплив кризи як «надзвичайно ускладнювальний» порівняно з 31-33 % в інших регіонах [51].

Окремою проблемою є недостатня прозорість процесів прийняття рішень та комунікація з населенням. Графіки планових відключень часто змінюються без попередження, а інформація про реальний стан енергосистеми залишається фрагментованою й важкодоступною для пересічних громадян. Це підриває довіру населення до системи управління та ускладнює планування економічної діяльності підприємствами й домогосподарствами.

Проблема кадрового забезпечення також заслуговує на окрему увагу.

Мобілізація та міграція населення призвели до значного скорочення кваліфікованих спеціалістів в енергетичному секторі, що обмежує спроможність до оперативного відновлення пошкоджених об’єктів. Система підготовки кадрів і механізми збереження критичного персоналу потребують суттєвого вдосконалення з урахуванням реалій воєнного часу.

Узагальнюючи результати аналізу, можна виділити декілька системних закономірностей функціонування публічного управління енергетичною безпекою в умовах гібридної війни. По-перше, система демонструє високу ефективність у реалізації стратегічних проєктів із чітко визначеними цілями та міжнародною підтримкою, як засвідчує успіх екстреної синхронізації з ENTSO-E. Ключовими факторами успіху в цьому випадку стали багаторічна підготовча робота, чітке розуміння кінцевої мети та наявність компетентних фахівців на всіх рівнях реалізації. По-друге, тактичні антикризові заходи забезпечують базову функціональність інфраструктури, хоча й за високої ціни ресурсних витрат і значного навантаження на операційний персонал енергетичних підприємств. По-третє, децентралізація генерації формує нову архітектуру енергосистеми, більш стійку до точкових ударів та орієнтовану на довгострокові цілі енергетичної трансформації.

Водночас системними проблемами залишаються фрагментація повноважень між органами влади, дублювання функцій моніторингу критичної інфраструктури, відсутність інтегрованого аналітичного забезпечення, недостатнє сценарне планування та реактивний характер більшості управлінських рішень. Аналіз засвідчує, що Енергетична стратегія України на період до 2050 року потребує суттєвого доопрацювання в частині механізмів реагування на воєнні загрози й чіткого розподілу відповідальності між суб'єктами управління. Особливої уваги потребує розробка механізмів превентивного захисту критичної інфраструктури та систем раннього попередження про загрози, а також інтеграція соціального виміру у формування енергетичної політики з урахуванням потреб найвразливіших груп населення.

Дедуктивний аналіз свідчить, що ефективність публічного управління

енергетичною безпекою прямо корелює з рівнем міжінституційної координації та якістю стратегічного планування. Успішні кейси, такі як синхронізація з ENTSO-E чи розгортання децентралізованої генерації, характеризуються чітким розподілом ролей, визначеними термінами та міжнародною підтримкою. Натомість сфери з розмитою відповідальністю та дублюванням функцій демонструють значно нижчу результативність, що підтверджує необхідність системних інституційних реформ.

Індуктивне узагальнення окремих випадків антикризового реагування дозволяє сформулювати загальну закономірність: ефективність управлінських рішень зростає пропорційно до ступеня їх координації з міжнародними партнерами та рівня залучення приватного сектора. Це пояснюється тим, що міжнародні партнери привносять не лише фінансові ресурси, а й управлінські компетенції, технічну експертизу й механізми контролю якості, які підвищують загальну ефективність реалізації проєктів.

Перспективним напрямом удосконалення системи публічного управління є створення інтегрованого ситуаційного центру енергетичної безпеки з повноваженнями оперативної координації всіх суб’єктів управління. Такий центр міг би забезпечити єдину інформаційну платформу для моніторингу загроз у режимі реального часу, планування превентивних заходів та координації відновлювальних робіт на основі єдиної методології пріоритезації. Крім того, необхідним є посилення механізмів персональної відповідальності посадовців за досягнення конкретних показників енергетичної безпеки, включаючи KPI щодо термінів відновлення, рівня покриття потреб споживачів та ефективності використання ресурсів. Такий стан речей стимулюватиме проактивний підхід до управління замість реактивного реагування на кризові ситуації.

Важливим напрямом є також розвиток механізмів державно-приватного партнерства у сфері захисту й відновлення енергетичної інфраструктури. Досвід 2022-2024 років засвідчує, що приватні компанії здатні забезпечувати значно вищу швидкість реагування та гнучкість порівняно з державними структурами за умови належного регуляторного середовища й механізмів компенсації

ризиків. Формування гендерно чутливої енергетичної політики, що враховує потреби різних груп населення та забезпечує рівний доступ до енергетичних ресурсів і компенсаційних механізмів, має стати невід'ємною складовою майбутнього відновлення України.

Отже, система публічного управління енергетичною безпекою України в умовах повномасштабної російсько-української війни демонструє змішані результати, що відображають як значний адаптаційний потенціал, так і структурні обмеження існуючої інституційної архітектури. Безперечними досягненнями є екстрена інтеграція з європейською енергосистемою, успішне розгортання децентралізованої генерації, ефективна координація міжнародної допомоги та формування нормативної бази для підтримки відновлюваної енергетики. Водночас критичними проблемами залишаються фрагментація управлінських повноважень, дублювання функцій, корупційні ризики, недостатнє стратегічне планування на випадок ескалації воєнних загроз, реактивний характер більшості управлінських рішень і недостатня увага до соціального виміру енергетичної кризи. Подальше вдосконалення системи потребує комплексних інституційних реформ, спрямованих на посилення горизонтальної координації, впровадження механізмів проактивного управління ризиками, розвиток державно-приватного партнерства та формування інклюзивної енергетичної політики.

РОЗДІЛ 3
НАПРЯМИ ПІДВИЩЕННЯ РОЛІ ПУБЛІЧНОГО УПРАВЛІННЯ В ЗАБЕЗПЕЧЕННІ ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ ЯК СКЛАДОВОЇ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

3.1 Зарубіжний досвід публічного управління енергетичною безпекою в умовах гібридних загроз

Визначені в попередньому підрозділі системні проблеми українського публічного управління енергетичною безпекою – фрагментація повноважень між органами влади, дублювання функцій моніторингу критичної інфраструктури, недостатнє стратегічне планування та реактивний характер управлінських рішень – актуалізують необхідність дослідження зарубіжного досвіду протидії гібридним загрозам в енергетичному секторі. Методологія компаративного аналізу передбачає дослідження конкретних кейсів антикризового реагування, виявлення інституційних механізмів координації та формулювання практичних уроків, придатних для адаптації в українських умовах.

Особливу цінність для України становить досвід країн, що безпосередньо стикаються з аналогічними викликами з боку Російської Федерації або функціонують в умовах перманентної воєнної загрози. Саме тому об’єктами компаративного аналізу обрано країни Балтії, які щойно завершили історичний процес десинхронізації від російської енергосистеми, Польщу як державу, що розгорнула безпрецедентну операцію із захисту критичної інфраструктури, Німеччину, яка продемонструвала здатність до швидкої адаптації енергетичної політики в умовах кризи, та Ізраїль, що має унікальний досвід захисту інфраструктури в умовах постійних ракетних обстрілів. Критерії відбору країн включають: наявність реального досвіду протидії гібридним загрозам в енергетичному секторі, географічну або геополітичну близькість до України, а

також доступність верифікованих джерел інформації про застосовані механізми публічного управління.

Досвід країн Балтії: стратегія виходу з енергетичної залежності

Історичне відключення Литви, Латвії та Естонії від електроенергетичної системи BRELL 8 лютого 2025 року становить один із найбільш показових прикладів успішної реалізації довгострокової стратегії енергетичної незалежності в умовах гібридних загроз. Система BRELL, створена ще у 2001 р. як спадок радянської енергетичної інфраструктури, протягом десятиліть надавала Росії можливість регулювати частоту електромережі та контролювати енергетичну безпеку всього Балтійського регіону [39]. Процес підготовки до десинхронізації тривав близько двадцяти років і охоплював технічний, організаційний та правовий виміри, що свідчить про необхідність довгострокового стратегічного планування при реалізації подібних проєктів [11].

Ключовим елементом успіху балтійської стратегії стала послідовна розбудова альтернативної інфраструктури міждержавних з'єднань. Запуск LitPol Link із Польщею у 2015 році, введення в експлуатацію двох черг Estlink із Фінляндією у 2006 та 2014 роках, а також NordBalt зі Швецією створили технічні передумови для заміщення російських потоків електроенергії та усунення ризиків енергетичного шантажу. Вартість проєкту десинхронізації становила 1,6 мільярда євро, при цьому три чверті витрат було покрито з бюджету Європейського Союзу, що демонструє критичну роль міжнародної фінансової підтримки в реалізації стратегічних інфраструктурних проєктів [39].

Особливої уваги заслуговує механізм координації між державними органами трьох країн напередодні синхронізації. Усвідомлюючи високу ймовірність провокацій з боку Російської Федерації, литовський уряд запровадив додаткові заходи безпеки для захисту критичної енергетичної інфраструктури, включаючи посилення патрулювання об'єктів та активізацію кіберзахисту. Як зазначають експерти, країни Балтії не виключали можливості диверсій, кібератак та інформаційних операцій, спрямованих на дискредитацію процесу десинхронізації [39]. Ця превентивна готовність, що базувалася на реалістичній

оцінці загроз, стала важливим фактором успішного завершення операції без серйозних інцидентів.

Порівняльний аналіз, проведений Секретаріатом Енергетичного Співтовариства, засвідчує, що балтійський досвід має безпосередню релевантність для України, яка здійснила екстрену синхронізацію з ENTSO-E у березні 2022 року за принципово інших обставин – в умовах активних бойових дій [11]. Якщо країни Балтії мали двадцять років на підготовку, Україна була змушена завершити аналогічний процес за три тижні, що, з одного боку, продемонструвало надзвичайну адаптивність української енергосистеми, а з іншого – залишило низку технічних питань невирішеними.

Інцидент із пошкодженням кабелю Estlink-2 у грудні 2024 року, спричинений діями російського танкера Eagle S, додатково підкреслює вразливість критичної інфраструктури до гібридних атак навіть після успішної десинхронізації [5]. Як зазначає Європейська академія наук (EASAC), цей інцидент продемонстрував важливість наявності резервних потужностей та альтернативних маршрутів постачання електроенергії, оскільки балтійські країни змогли компенсувати втрату потужності через інші з’єднання [9]. Ремонт пошкодженого кабелю тривав близько трьох місяців, що актуалізує питання швидкості відновлення критичної інфраструктури після диверсій – проблему, з якою Україна стикається постійно. Урок балтійського досвіду полягає в необхідності поєднання довгострокового стратегічного планування з готовністю до оперативного реагування на непередбачувані загрози, а також у критичній важливості резервування ключових елементів енергетичної інфраструктури.

Досвід Польщі: модель цивільно-військової координації

Запуск операції «Горизонт» у листопаді 2025 року став відповіддю польського уряду на серію диверсій на об'єктах критичної інфраструктури, зокрема на залізничних магістралях, що використовувалися для транспортування допомоги Україні. Прем’єр-міністр Дональд Туск охарактеризував ці інциденти як «безпрецедентний акт саботажу», вказавши на російський слід у їх організації [30]. Масштаб операції – залучення до десяти тисяч

військовослужбовців із технікою, включаючи безпілотники та вертольоти – свідчить про серйозність оцінки загроз польським керівництвом і готовність до рішучих превентивних дій.

Інституційна архітектура операції «Горизонт» передбачає координацію зусиль різних силових структур: підрозділів армії, Військ територіальної оборони, Сил спеціального призначення, поліції, Служби охорони залізниць та підрозділів кібербезпеки. Така міжвідомча взаємодія, що охоплює як військовий, так і цивільний компоненти, забезпечує комплексний підхід до захисту інфраструктури від різних типів загроз – від фізичних диверсій до кібератак [30]. Патрулі військових було розгорнуто на вісімдесяти ключових залізничних ділянках по всій території Польщі, при цьому основна увага зосереджена на районах із найвищим ризиком диверсій.

Важливим елементом польської моделі є превентивний характер операції. Як зазначається в офіційних джерелах, мета полягає не лише в реагуванні на загрози, а й у стримуванні потенційних виконавців диверсій шляхом демонстрації готовності та присутності сил безпеки [30]. Цей підхід суттєво відрізняється від реактивної моделі, характерної для українського публічного управління, де більшість заходів уживається вже після завдання збитків інфраструктурі.

Двостороння співпраця України та Польщі у сфері енергетичної безпеки набуває дедалі більшої інтенсивності. За даними Міністерства енергетики України, країни реалізують спільні проєкти з розбудови газотранспортної інфраструктури та поглиблення інтеграції в рамках ENTSO-E, при цьому Польща розглядається як стратегічний енергетичний хаб для України [60]. Публічна дискусія «Енергетика без кордонів: Україна та Польща разом до Європи», організована Центром Разумкова спільно з DiXi Group, засвідчила спільність викликів та можливостей для обох країн у протидії гібридним загрозам [83]. Польський досвід координації силових структур для захисту критичної інфраструктури становить практичну модель, яка може бути адаптована в українських умовах з урахуванням специфіки воєнного стану.

Варто зазначити, що польська модель передбачає також активне залучення цивільного населення до системи раннього попередження. Уряд анонсував розробку мобільного додатка, який дозволить громадянам повідомляти про підозрілу активність поблизу об’єктів критичної інфраструктури, що має запрацювати наприкінці 2025 року. Такий підхід «всеохоплюючої безпеки», запозичений із скандинавської практики, перетворює кожного громадянина на потенційного учасника системи захисту, що суттєво розширює можливості моніторингу загроз. Крім того, польський досвід свідчить про важливість чіткого розмежування повноважень між різними силовими структурами при збереженні єдиного центру координації – елемент, якого бракує українській системі управління критичною інфраструктурою.

Досвід Німеччини: адаптивність енергетичної політики в умовах кризи

Реакція Німеччини на газову кризу 2022 року, спричинену скороченням російських поставок, продемонструвала здатність системи публічного управління до швидкої адаптації стратегічних пріоритетів в умовах зовнішнього тиску. Рішення про реактивацію шістнадцяти вугільних теплоелектростанцій, прийняте урядом у липні 2022 року, суперечило базовим принципам політики Energiewende, спрямованої на декарбонізацію енергетичного сектора [25]. Проте усвідомлення загрози енергетичній безпеці країни змусило політичне керівництво відступити від ідеологічних настанов на користь прагматичних рішень.

Механізм реалізації цього рішення передбачав тимчасовий характер реактивації – станції виводилися з резерву на обмежений період для покриття дефіциту генерації, спричиненого скороченням газових поставок. Згодом було ухвалено рішення про додаткову реактивацію ще одинадцяти станцій, що загалом дозволило компенсувати значну частину втрачених потужностей [25]. Цей досвід засвідчує важливість підтримання стратегічних резервів генеруючих потужностей навіть в умовах енергетичної трансформації, оскільки вони забезпечують гнучкість системи в кризових ситуаціях.

Водночас німецький досвід демонструє й певні обмеження. Тривала

залежність від російського газу, яка формувалася десятиліттями попри численні попередження партнерів зі Східної Європи, свідчить про недостатню увагу до геополітичних ризиків при формуванні енергетичної політики. Як зазначають аналітики Agora Energiewende, вторгнення Росії в Україну посилило аргументацію на користь прискорення енергетичної трансформації, оскільки залежність від імпортованого викопного палива створює системні вразливості [2]. Урок для України полягає в необхідності диверсифікації енергетичного балансу та уникнення критичної залежності від будь-якого зовнішнього постачальника.

Інституційні зміни в німецькій системі управління енергетичною безпекою також заслуговують на увагу. Ухвалення так званого KRITIS umbrella law у листопаді 2024 року надало Федеральному мережевому агентству розширені повноваження з нагляду за захистом критичної інфраструктури в енергетичному секторі. Закон зобов’язує операторів інфраструктури враховувати всі потенційні ризики (від природних катастроф до актів саботажу) та запроваджує значні штрафні санкції за невиконання вимог щодо звітності [3]. Такий підхід до посилення регуляторних вимог може бути використаний при вдосконаленні українського законодавства у сфері захисту критичної інфраструктури. Водночас слід зауважити, що німецька модель передбачає тривалі перехідні періоди для адаптації операторів до нових вимог- розкіш, якої позбавлена Україна в умовах активних бойових дій. Тому імплементація німецького досвіду потребує суттєвої адаптації з урахуванням необхідності негайного впровадження захисних заходів.

Досвід Ізраїлю: захист інфраструктури в умовах перманентної воєнної загрози

Держава Ізраїль функціонує в умовах постійної загрози ракетних обстрілів з боку ворожих сусідніх територій, що робить її досвід захисту критичної інфраструктури особливо релевантним для України. Система протиповітряної оборони «Залізний купол» забезпечує перехоплення близько дев'яноста відсотків ракет, випущених угрупованнями ХАМАС та підтримуваними Іраном силами, що дозволяє мінімізувати збитки цивільній інфраструктурі та населенню [47]. Ця

технологічна спроможність, однак, є лише одним елементом комплексної системи забезпечення стійкості.

Аналітична записка Національного інституту стратегічних досліджень «Життя як в Ізраїлі: висновки з досвіду забезпечення національної безпеки для України» наголошує на схожості безпекового середовища обох держав, що зумовлює подібність стратегічних цілей. До ключових елементів ізраїльської моделі автори відносять: підтримання фізичної та кібернетичної інфраструктури зв'язку для забезпечення функціонування критично важливих систем, розвиток системи протиракетної оборони з огляду на постійну загрозу обстрілів, а також безумовну протидію пропаганді ворога [62]. Ці пріоритети безпосередньо кореспондують із викликами, що стоять перед Україною в умовах повномасштабної війни.

Особливу увагу в ізраїльському досвіді привертає інтеграція заходів фізичного захисту з кіберзахистом критичної інфраструктури. Національна кібербезпекова директорія координує зусилля державних органів та приватного сектора, забезпечуючи цілісний підхід до захисту від комплексних загроз. Секторальні центри реагування на кіберінциденти, зокрема у фінансовому та енергетичному секторах, дозволяють враховувати специфіку кожної галузі при розробці захисних заходів. Такий диференційований підхід контрастує з українською практикою, де кіберзахист енергетичної інфраструктури часто здійснюється без належного врахування галузевої специфіки.

Практичний вимір ізраїльського досвіду для України полягає також у системі цивільного захисту населення. Розгалужена мережа бомбосховищ, система оповіщення та навчання населення правилам поведінки під час обстрілів формують культуру стійкості на рівні суспільства. Як зазначила віцеспікерка Верховної Ради України Олена Кондратюк під час робочого візиту до Ізраїлю, «необхідність постійної адаптації до життя і роботи в небезпечних реаліях- це те, що сьогодні об'єднує Україну та Ізраїль» [62]. Запозичення ізраїльського досвіду облаштування захисних споруд для критичної інфраструктури становить один із перспективних напрямів підвищення стійкості української енергосистеми.

Слід також наголосити на ізраїльському досвіді застосування радарних систем раннього попередження для захисту енергетичних об’єктів. За даними відкритих джерел, ізраїльські радіолокаційні станції RADA RPS-42, що використовуються в Україні з 2023 року, вже продемонстрували свою ефективність під час масованих атак на енергетичну інфраструктуру, забезпечуючи своєчасне попередження та можливість евакуації персоналу. Цей приклад засвідчує, що технологічне співробітництво з Ізраїлем може мати безпосередній вплив на підвищення захищеності українських енергетичних об'єктів, хоча політичні обмеження на поставки деяких категорій озброєнь залишаються стримуючим фактором.

Порівняльний аналіз досвіду чотирьох країн дозволяє виокремити спільні закономірності ефективного публічного управління енергетичною безпекою в умовах гібридних загроз. По-перше, успішні моделі характеризуються довгостроковим стратегічним плануванням у поєднанні з готовністю до оперативної адаптації, як це продемонстрували країни Балтії (двадцятирічна підготовка до десинхронізації) та Німеччина (швидка реактивація вугільних станцій). По-друге, ефективний захист критичної інфраструктури потребує міжвідомчої координації, що охоплює як цивільні, так і військові структури – польська операція «Горизонт» є показовим прикладом такого підходу. По-третє, комплексний характер сучасних загроз вимагає інтеграції фізичного захисту з кіберзахистом, як це реалізовано в ізраїльській моделі.

Критичний аналіз розглянутих моделей дозволяє виявити й певні обмеження їх застосовності в українському контексті. Балтійський досвід формувався в умовах мирного часу, що дозволило здійснити поступову, добре сплановану трансформацію енергетичної системи. Польська модель розрахована на протидію диверсіям обмеженого масштабу, а не систематичним військовим ударам. Німецький досвід стосується насамперед економічних аспектів енергетичної кризи, а не фізичного захисту інфраструктури. Ізраїльська модель, хоча й найбільш релевантна з точки зору воєнного контексту, базується на значно менших географічних масштабах і принципово інших характеристиках

загроз.

Аналітичні матеріали DiXi Group щодо енергетичного виміру війни наголошують на необхідності систематичного вивчення зарубіжного досвіду та його адаптації до українських умов [7].

Водночас слід ураховувати, що жодна з розглянутих країн не стикалася із загрозами такого масштабу й інтенсивності, як Україна, – систематичними масованими ракетними ударами по енергетичній інфраструктурі протягом тривалого періоду.

Це означає, що український досвід протидії гібридним загрозам в енергетичному секторі сам по собі є унікальним і може становити предмет вивчення для інших країн, як це вже відбувається у випадку з країнами Балтії, які орієнтуються на український досвід при посиленні захисту власної критичної інфраструктури.

Узагальнюючи результати компаративного аналізу, можна констатувати, що ключовими напрямами імплементації зарубіжного досвіду в українську практику публічного управління є: розробка довгострокової стратегії енергетичної безпеки з чіткими індикаторами досягнення цілей та механізмами моніторингу виконання (балтійський досвід), створення ефективних механізмів цивільно-військової координації для захисту критичної інфраструктури з чітким розмежуванням повноважень та єдиним центром управління (польський досвід), забезпечення гнучкості енергетичної політики та підтримання стратегічних резервів генерації для швидкого реагування на кризові ситуації (німецький досвід), а також інтеграція фізичного й кібернетичного захисту з урахуванням галузевої специфіки енергетичного сектора та застосування передових технологій раннього попередження (ізраїльський досвід).

Конкретизація цих напрямів у формі практичних рекомендацій щодо посилення ролі публічного управління в забезпеченні енергетичної безпеки України становить предмет аналізу наступного підрозділу.

3.2 Рекомендації щодо посилення ролі публічного управління в забезпеченні енергетичної безпеки України

Визначені в попередньому підрозділі закономірності зарубіжного досвіду захисту критичної інфраструктури вимагають розгляду механізмів їх адаптації до українських реалій, характеризованих безпрецедентним поєднанням воєнних загроз та системних інституційних викликів. Опалювальний період 2024-2025 років, що супроводжувався дев'ятьма масованими ракетно-дроновими атаками на об'єкти енергетичної інфраструктури, найпотужніша з яких 13 грудня 2024 року включала понад триста засобів ураження, виявив як адаптивний потенціал вітчизняної системи публічного управління, так і її структурні вразливості, що потребують невідкладного усунення [61].

Формулювання науково обґрунтованих рекомендацій має базуватися на критичному аналізі існуючих підходів шляхом синтезу позицій різних дослідників і практиків державного управління з урахуванням принципової відмінності українського контексту від зарубіжного досвіду: якщо країни Балтії мали два десятиліття на підготовку десинхронізації від російської енергосистеми [39], Україна функціонує в режимі постійної бойової готовності, де кожне управлінське рішення має давати негайну практичну віддачу.

Аналітичний звіт Міністерства енергетики України констатує, що, попри песимістичні прогнози щодо тривалих системних блекаутів, Об’єднана енергетична система продемонструвала операційну стійкість: починаючи з січня 2025 року обмеження електропостачання для населення не застосовувалися, а відновлення постачання після масованих ударів здійснювалося протягом кількох діб [61].

За період повномасштабної війни внаслідок атак на енергетичну інфраструктуру загинули 160 працівників галузі безпосередньо на робочих місцях, понад 300 осіб отримали поранення [61]. Міністр енергетики України Г. Галущенко констатує, що забезпечення електро- та теплопостачання в

опалювальний період є заслугою енергетиків, які працюють у надзвичайно небезпечних умовах [61]. Проте експерти Центру Разумкова піддають критичному осмисленню зазначений результат, акцентуючи увагу на тому, що станом на осінь 2024 року обсяг доступної генеруючої потужності становив лише чверть від довоєнного рівня, а дефіцит сягнув критичних 9 ГВт [84].

Означена розбіжність оцінок засвідчує методологічну проблему: оцінювання ефективності публічного управління енергетичною безпекою не може обмежуватися констатацією операційних результатів без урахування системних втрат та упущених можливостей розвитку.

Дослідники Центру Разумкова формулюють принципово важливий висновок: унаслідок небажання уряду впровадити європейську модель енергетичного ринку Україна втратила можливість за період війни збудувати щонайменше 7 ГВт відновлюваної генерації та до 2 ГВт балансуючих потужностей [84]. Критично осмислюючи цю позицію, слід зазначити, що вона акцентує увагу переважно на регуляторних чинниках, недостатньо враховуючи об'єктивні обмеження воєнного часу: високі інвестиційні ризики, логістичні перешкоди для імпорту обладнання та кадровий дефіцит. Водночас сам факт існування альтернативної траєкторії розвитку підтверджує тезу про системний характер проблем публічного управління, які не зводяться виключно до наслідків збройної агресії.

Інституційна координація антикризового реагування залишається найбільш проблемним напрямом, що потребує невідкладного вдосконалення. Колишній секретар Ради національної безпеки і оборони України О. Литвиненко ще восени 2024 року артикулював необхідність посилення координації між енергетичним сектором та силами протиповітряної оборони, прогнозуючи масовані удари по інфраструктурі з початком опалювального сезону [75]. Справдження цього прогнозу при одночасній відсутності системних змін у механізмах міжвідомчої взаємодії засвідчує розрив між аналітичним забезпеченням прийняття рішень і їх практичною імплементацією, що є характерною ознакою інституційної дисфункції.

Указом Президента України № 695/2023 від 17 жовтня 2023 року введено в дію рішення Ради національної безпеки і оборони України «Про організацію захисту та забезпечення безпеки функціонування об’єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій», яким на Кабінет Міністрів України покладено обов'язок забезпечити посилений інженерний та фізичний захист об’єктів у десятиденний строк, збільшити кількість мобільних вогневих груп Збройних Сил України та Національної гвардії України для протиповітряного прикриття, а також затвердити у тримісячний строк план заходів з відновлення пошкоджених об’єктів [82]. Аналіз практичної реалізації зазначеного рішення дозволяє констатувати, що правова основа координаційних механізмів сформована, проте її операціоналізація залишається фрагментарною, потребуючи конкретизації процедур міжвідомчої взаємодії та визначення персональної відповідальності посадових осіб.

Адаптація досвіду польської операції «Горизонт» до українських умов [30] передбачає трансформацію Антикризового енергетичного штабу при Кабінеті Міністрів України з консультативно-дорадчого органу на повноцінний оперативний центр, наділений правом прийняття обов’язкових рішень для всіх учасників енергетичного ринку в умовах надзвичайних ситуацій. Ефективність польської моделі обумовлена саме концентрацією повноважень щодо залучення ресурсів різних відомств під єдиним командуванням, що забезпечує оперативність реагування на комплексні загрози. В українському контексті це вимагає нормативного закріплення механізму, за якого Штаб отримує тимчасові повноваження координувати розподіл ресурсів протиповітряної оборони для захисту критичних об'єктів, узгоджувати графіки обмеження електропостачання з урахуванням регіональної специфіки та мобілізувати резерви приватних операторів.

Децентралізація енергетичної генерації становить напрям, де вітчизняна практика демонструє найбільш переконливі результати, водночас виявляючи системні бар'єри масштабування успішних ініціатив. Чортківська територіальна

громада Тернопільської області, що першою серед малих міст України набула членства в Європейській асоціації місцевих органів влади у сфері енергетичного переходу Energy Cities, реалізувала проєкт установлення сонячної електростанції потужністю 22 кВт для районної лікарні, забезпечивши річну економію бюджетних коштів у розмірі 178 тисяч гривень [49]. Міський голова Чорткова В. Шматько акцентує увагу на тому, що громада орієнтується на розвиток власної енергетики, яка вже забезпечує реальну економію, проте для масштабування необхідні кваліфіковані фахівці, яких громада активно залучає, пропонуючи конкурентну заробітну плату та житло [49].

Долинська територіальна громада Івано-Франківської області демонструє більш амбітний підхід до формування енергетичної автономії. У грудні 2023 року тут введено в експлуатацію сонячну електростанцію потужністю 120 кВт для очисних споруд комунального підприємства «Водоканал», на фінансування якої з місцевого бюджету спрямовано 4,7 мільйона гривень. За підсумками 2024 року станція згенерувала близько 147 тисяч кіловат-годин електроенергії, що забезпечило економію понад мільйона гривень; починаючи з липня 2024 року надлишок електроенергії реалізується в загальну мережу [78].

Концепція сотової енергомережі, розроблювана головою громади І. Дирівим, передбачає формування локальної системи, що інтегрує різнотипні об'єкти генерації на основі технологій розумних мереж та механізмів управління попитом, з енергетичним кооперативом у ролі агрегатора [78]. Зазначена модель кореспондує з ізраїльським досвідом секторальних центрів реагування та балтійською практикою резервування критичних елементів інфраструктури, адаптованими до специфіки української територіальної громади.

Бориславська територіальна громада Львівської області ілюструє потенціал залучення приватних інвестицій у децентралізовану енергетику. Міська рада ухвалила рішення про виділення 45 гектарів землі в охоронній зоні сміттєзвалища під будівництво сонячних електростанцій приватним інвестором, трансформуючи проблемну територію на джерело відновлюваної енергії та додаткових надходжень до місцевого бюджету [49].

Місто Харків демонструє специфічну модель забезпечення енергетичної стійкості в умовах прифронтового міста, що зазнає систематичних ударів по енергетичній інфраструктурі. За ініціативи міського голови І. Терехова з липня 2023 року реалізується програма встановлення сонячних електростанцій на об'єктах критичної інфраструктури: першу станцію потужністю близько 52 кВт, що складається з 96 сонячних панелей, було встановлено на даху Міської клінічної багатопрофільної лікарні № 17, яка надає допомогу військовослужбовцям та цивільному населенню [79].

У липні 2024 року аналогічну станцію потужністю 30 кВт з системою резервного живлення ємністю 42,6 кВт·год встановлено в дитячій лікарні, що забезпечує безперебійну роботу паліативного, реабілітаційного відділень та неврологічного стаціонару навіть під час тривалих знеструмлень. Проєкти реалізовано за підтримки благодійного фонду RePower Ukraine та міжнародних партнерів із Німеччини, Великобританії й Шотландії. За оцінкою міської влади, дві станції забезпечують економію мільйонів гривень щорічно [79].

Досвід Харкова засвідчує, що навіть в умовах постійної воєнної загрози децентралізація енергопостачання критичних об’єктів є реалізованим завданням, що потребує координації між місцевою владою та міжнародними донорами.

Узагальнюючи досвід зазначених громад, слід констатувати формування нової парадигми місцевого самоврядування в енергетичній сфері, що базується на принципах енергетичної автономії, диверсифікації джерел генерації й активного залучення приватного капіталу.

Водночас масштабування успішних практик окремих громад на понад тисячу територіальних громад України стикається з низкою системних бар’єрів. Учасники публічного діалогу «Децентралізація на зв'язку» ідентифікували дві ключові проблеми: дефіцит кваліфікованих фахівців з енергоменеджменту на місцевому рівні та недостатнє фінансування проєктів енергетичної автономії [49]. Всеукраїнська асоціація об'єднаних територіальних громад створила фахову мережу, що нараховує 95 енергоменеджерів, проте зазначена кількість є критично недостатньою для забезпечення потреб усіх громад [49].

Державне агентство з енергоефективності та енергозбереження України розгортає мережу регіональних офісів декарбонізації та енергоефективності для надання консультаційної підтримки громадам, проте ця ініціатива потребує доповнення системними заходами щодо підготовки кадрів – запровадження спеціалізованих освітніх програм на базі закладів вищої та професійно-технічної освіти.

Фінансові бар'єри частково долаються новими урядовими ініціативами. Міністерство енергетики України анонсувало програму підтримки безвідсоткових кредитів для побутових споживачів при встановленні до 10 кВт потужностей сонячної генерації разом із системами накопичення енергії [49]. Міністерство економіки України та Міністерство енергетики України спільно працюють над розширенням кредитної програми «Доступні кредити 5-7-9» для підтримки суб'єктів господарювання у встановленні відновлюваних джерел енергії та газових генеруючих установок.

Критично осмислюючи зазначені ініціативи, слід зауважити, що для об'єктів критичної інфраструктури територіальних громад (закладів охорони здоров'я, підприємств водопостачання та водовідведення) необхідним є не кредитне, а цільове грантове фінансування, що може бути мобілізоване через механізми міжнародної підтримки. За даними Міністерства енергетики України, обсяг внесків до Фонду підтримки енергетики України перевищив 1,2 мільярда євро [61], і частина цих коштів має спрямовуватися саме на децентралізовані проєкти, а не виключно на відновлення централізованих генеруючих потужностей.

Законом України № 3220-IX «Про внесення змін до деяких законів України щодо відновлення та «зеленої» трансформації енергетичної системи України» від 30 червня 2023 року, що набрав чинності 27 липня 2023 року, запроваджено поняття «активний споживач» та сформовано правове підґрунтя для участі громадян та організацій в енергетичному ринку [52]. Голова Комітету Верховної Ради України з питань енергетики та житлово-комунальних послуг А. Герус наводить як приклад Хмельницьку обласну лікарню, яка не лише забезпечує

власні потреби електроенергією від сонячної станції, а й реалізує надлишок у мережу, отримуючи додатковий дохід [49].

Поширення цієї практики стримується регуляторними бар'єрами: процедури технологічного приєднання до мережі та погодження технічних умов залишаються надмірно складними, особливо для невеликих об’єктів генерації. Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг, та Міністерство енергетики України працюють над спрощенням зазначених процедур, проте темпи цієї роботи недостатні для забезпечення енергетичної безпеки в умовах воєнного стану.

Кіберзахист енергетичної інфраструктури становить окремий критичний напрям, що характеризується поєднанням позитивних зрушень і глибоких системних вразливостей. Річний аналітичний огляд Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України за період жовтень 2023 – вересень 2024 року фіксує суттєве зростання інтенсивності атак на критичну інфраструктуру, констатуючи еволюцію технологій противника та активне використання угруповань UAC-0010 та UAC-0006 для цілеспрямованих атак на об'єкти енергетичного сектора [74]. Державна служба спеціального зв’язку та захисту інформації України зафіксувала сотні інцидентів, спрямованих проти енергетичної інфраструктури, що підтверджує системний характер кібероперацій як складової гібридної війни.

Адаптація ізраїльського досвіду інтеграції фізичного та кіберзахисту через Національну кібербезпекову директорію, проаналізованого в попередньому підрозділі [62], є релевантною для України з огляду на подібність безпекового середовища. Секторальний підхід, за якого енергетичний сектор має власний центр реагування на кіберінциденти з урахуванням галузевої специфіки, забезпечує більш таргетований захист порівняно з універсальними рішеннями. Формування такого секторального центру реагування на комп'ютерні надзвичайні події на базі структур Міністерства енергетики України, інтегрованого в національну систему кіберзахисту під координацією CERT-UA, є пріоритетним завданням.

При цьому, на відміну від німецького законодавства KRITIS umbrella law [3], що передбачає тривалі перехідні періоди для адаптації операторів, українські заходи кіберзахисту мають упроваджуватися в режимі постійної бойової готовності.

Законодавче забезпечення енергетичної безпеки демонструє позитивну динаміку, хоча темпи прийняття критично важливих рішень залишаються недостатніми для умов воєнного стану. Верховна Рада України 4 листопада 2025 року прийняла за основу проєкт Закону України «Про інфраструктурні проєкти у сфері енергетики, які становлять суспільний інтерес» (реєстраційний № 13450), що імплементує Регламент Європейського Союзу 2022/869 щодо транс'європейської енергетичної інфраструктури та скорочує терміни реалізації стратегічних проєктів до 3,5 років через спрощення дозвільних процедур [44].

Ухвалення цього закону створить умови для залучення європейських інвестицій у відновлення та розвиток енергетичної інфраструктури, сприяючи інтеграції України до енергетичного простору Європейського Союзу. Паралельно в Комітеті Верховної Ради України з питань організації державної влади, місцевого самоврядування, регіонального розвитку та містобудування розглядається законопроєкт № 14115 про внесення змін до законодавства щодо реконструкції, капітального ремонту та інженерно-технічних заходів із захисту об'єктів критичної інфраструктури паливно-енергетичного сектора, спрямований на усунення регуляторних бар’єрів при проведенні невідкладних робіт [45].

Проблема, яку адресує цей законопроєкт, гостро постала після масованих атак, коли відновлювальні роботи затримувалися через необхідність проходження стандартних дозвільних процедур, неадаптованих до умов воєнного часу. Комітет Верховної Ради України з питань енергетики та житлово-комунальних послуг підтримав законопроєкти щодо митних і податкових стимулів для відновлення енергетики, що передбачають преференції для імпорту обладнання та розвитку відновлюваних джерел енергії [54]. Прискорене ухвалення зазначеного пакету законів у другому читанні та їх негайна

імплементація є критичною передумовою для підготовки до наступного опалювального періоду.

Публічно-приватне партнерство у сфері захисту енергетичної інфраструктури залишається недостатньо формалізованим, попри високий рівень фактичної співпраці. За даними Міністерства енергетики України, енергетичні компанії з початку повномасштабного вторгнення спрямували близько 15 мільярдів гривень на підтримку Збройних Сил України, включаючи закупівлю техніки, обладнання та системи радіоелектронної боротьби [61].

Зазначене засвідчує високий рівень соціальної відповідальності приватного сектора, проте системне партнерство у сфері захисту критичної інфраструктури потребує нормативного оформлення через механізми концесії та державно-приватного партнерства. Досвід групи компаній ДТЕК щодо інвестування у фізичний захист енергетичних об'єктів може бути масштабований через державні програми співфінансування захисних заходів для всіх операторів критичної інфраструктури з визначенням чітких критеріїв відшкодування витрат та забезпеченням доступу до розвідувальної інформації про потенційні загрози.

Адаптація польського досвіду залучення громадян до системи раннього попередження передбачає створення функціоналу мобільного додатка для повідомлення про підозрілу активність поблизу об’єктів критичної інфраструктури. Зважаючи на високий рівень цифровізації українського суспільства, підтверджений успішним функціонуванням додатків «Повітряна тривога» та «Дія», створення аналогічного інструмента є технічно реалізованим завданням.

Такий підхід «всеохоплюючої безпеки», запозичений зі скандинавської практики та адаптований Польщею в рамках операції «Горизонт» [30], інтегрує громадян у систему захисту критичної інфраструктури, що є особливо актуальним для протидії диверсійним загрозам. Реалізація цього підходу потребує розроблення відповідної нормативно-правової бази, що регламентуватиме порядок обробки повідомлень громадян та їх інтеграцію в систему реагування на загрози.

Кадрове забезпечення енергетичного сектора становить критичний виклик, масштаб якого недооцінюється в дискусіях про енергетичну безпеку. Тисячі спеціалістів мобілізовані до Збройних Сил України, і ця тенденція продовжується. Критично осмислюючи оцінку Міністерства енергетики України щодо героїзму працівників галузі, слід зазначити, що вона засвідчує залежність системи від екстраординарних зусиль персоналу, а не від ефективності інституційних механізмів -модель, яка не може бути стійкою в довгостроковій перспективі.

Вирішення кадрової проблеми потребує комплексного підходу, що включає збереження критично важливих фахівців через механізми бронювання, прискорену підготовку нових спеціалістів і залучення професіоналів з-за кордону. Питання бронювання працівників енергетичного сектора від мобілізації залишається предметом дискусій, де зіштовхуються потреби Збройних Сил України та необхідність забезпечення функціонування критичної інфраструктури.

Оптимальним є диференційований підхід, за якого бронювання поширюється на вузькопрофільних спеціалістів з унікальними компетенціями, підготовка яких потребує тривалого часу, тоді як для інших категорій працівників забезпечується ротація та прискорена підготовка заміни. Для підготовки нового покоління енергоменеджерів необхідним є запровадження спеціалізованих освітніх програм на базі закладів вищої та професійно-технічної освіти, орієнтованих на децентралізовану енергетику, відновлювані джерела енергії та управління в умовах кризи.

Синтезуючи результати проведеного аналізу, слід констатувати, що система публічного управління енергетичною безпекою України характеризується суперечливим поєднанням операційної стійкості та структурних дисфункцій. До позитивних чинників належать: продемонстрована адаптивність енергетичної системи в умовах безпрецедентних руйнувань, наявність успішних практик децентралізації на рівні територіальних громад (Чортків, Долина, Борислав, Харків), активізація законодавчої роботи та високий

рівень міжнародної підтримки, засвідчений обсягом внесків до Фонду підтримки енергетики України, що перевищує 1,2 мільярда євро. Негативними залишаються: фрагментованість координаційних механізмів між центральними та регіональними органами влади, недостатні темпи впровадження ринкових реформ, що призвело до втрати можливості розбудови 7 ГВт відновлюваної генерації, критичний кадровий дефіцит та нерозв'язані суперечності між централізованим і децентралізованим підходами до управління енергетичною безпекою.

Ключовий висновок полягає в тому, що результати опалювального періоду 2024-2025 років не можуть екстраполюватися на майбутнє без системних змін, оскільки вони досягнуті ціною екстраординарних зусиль працівників галузі, 160 з яких загинули на робочих місцях, а понад 300 отримали поранення. Модель управління, що базується на героїзмі персоналу, а не на ефективності інституційних механізмів, не може бути стійкою в довгостроковій перспективі. Перехід від реактивного до проактивного управління, від фрагментованих ініціатив до системної політики, від консультативно-дорадчих органів до повноцінних оперативних центрів прийняття рішень становить головний напрям трансформації публічного управління енергетичною безпекою України, що визначає необхідність формування цілісної стратегії, окресленої у висновках до третього розділу.

ВИСНОВКИ

У магістерській роботі здійснено комплексне дослідження ролі публічного управління в забезпеченні енергетичної безпеки України як складової протидії гібридним загрозам. За результатами проведеного дослідження сформульовано такі висновки:

1. Дослідження сутності, типології та механізмів впливу гібридних загроз на національну безпеку дозволило встановити, що гібридні загрози є комплексним багатовимірним явищем, яке характеризується синхронним застосуванням воєнних, економічних, енергетичних, інформаційних та кібернетичних інструментів впливу без формального оголошення війни.

Еволюція концепції гібридних загроз від вузького воєнно-тактичного розуміння Ф. Гоффмана до сучасних комплексних підходів Європейського центру передового досвіду з протидії гібридним загрозам (Hybrid CoE) відображає ускладнення безпекового середовища. Енергетичний домен займає центральне місце у структурі гібридних загроз, оскільки виступає водночас самостійним інструментом тиску та каталізатором загроз в інших сферах, від кібератаки BlackEnergy на українські енергомережі у 2015 році до систематичних ракетних ударів 2022-2025 років.

Механізми впливу гібридних загроз (синергетичний, каскадний, асиметричний та дестабілізаційний) потребують відповідних механізмів протидії з боку системи публічного управління.

2. Аналіз поняття, місця та взаємозв'язків енергетичної безпеки в системі протидії гібридним загрозам засвідчив, що концепція енергетичної безпеки еволюціонувала через три етапи: від фокуса на фізичній доступності енергоресурсів (1970-ті – 2000-ні), через увагу до диверсифікації та енергоефективності (2006-2022), до сучасної концепції енергетичної стійкості (resilience), що передбачає здатність енергосистеми протистояти загрозам, швидко відновлюватися й адаптуватися до нових викликів.

В умовах гібридної війни енергетична безпека набуває статусу системоутворюючого елемента національної безпеки через двосторонні взаємозв'язки з економічною, воєнною, кібернетичною безпекою та соціальною стабільністю. Досвід України 2022–2025 років підтвердив, що каскадні ефекти від атак на енергетичну інфраструктуру поширюються на всі сектори: транспорт, комунікації, охорону здоров'я, промисловість, при цьому зимові blackout'и 2022-2023 років, усупереч очікуванням агресора, консолідували суспільство замість підриву підтримки курсу на опір.

3. Дослідження суб'єктів, механізмів та інструментів публічного управління енергетичною безпекою в Україні виявило, що система має багаторівневу структуру, яка включає органи стратегічного планування (РНБО, Кабінет Міністрів України), галузевого управління (Міністерство енергетики), регулювання (НКРЕКП) та операторів критичної інфраструктури (НЕК «Укренерго», НАК «Нафтогаз», оператори систем розподілу).

Механізми управління охоплюють нормативно-правовий, інституційний, економічний, технологічний і міжнародний компоненти, зокрема інтеграцію до європейського енергетичного простору через членство «Укренерго» в ENTSO-E з 1 січня 2024 року. Водночас виявлено системні проблеми: фрагментацію управлінських повноважень між Міненерго, НКРЕКП та іншими органами, недостатню міжвідомчу координацію в кризових ситуаціях, вразливість інституційної незалежності регулятора до політичного тиску щодо тарифних рішень.

4. Оцінка ефективності публічного управління у протидії гібридним загрозам в енергетичному секторі України засвідчила змішані результати. Безперечними досягненнями є: екстрена синхронізація з ENTSO-E за три тижні замість запланованих півтора року (16 березня 2022 року); збереження 80 % розподільних мереж попри руйнування понад 21 ГВт генеруючих потужностей унаслідок 25 масованих атак; зростання встановленої потужності споживчих сонячних електростанцій до майже 1500 МВт; рекордний імпорт електроенергії у 2024 році (4436 ГВт·год) та перетворення на нетто-експортера у вересні 2025

року (635 ГВт·год місячного експорту); ефективна координація міжнародної допомоги – внески до Фонду підтримки енергетики України перевищили 1,2 млрд євро. Критичними проблемами залишаються: реактивний характер управлінських рішень, відсутність інтегрованого моніторингу ефективності, недостатнє сценарне планування на випадок ескалації загроз, нездатність запобігти значним руйнуванням під час масованих атак (зокрема удар 26 серпня 2024 року залишив без електропостачання близько 8 млн домогосподарств).

5. Вивчення зарубіжного досвіду публічного управління енергетичною безпекою в умовах гібридних загроз дозволило виокремити ключові закономірності ефективного управління. Балтійський досвід (Литва, Латвія, Естонія) продемонстрував необхідність довгострокового стратегічного планування: двадцятирічна підготовка до десинхронізації від системи BRELL завершилася успішним відключенням 8 лютого 2025 року, при цьому вартість проєкту (1,6 млрд євро) на три чверті покрито з бюджету ЄС.

Польська операція «Горизонт» (листопад 2025 року) із залученням до 10 тис. військовослужбовців засвідчила ефективність міжвідомчої цивільно-військової координації та превентивного підходу до захисту критичної інфраструктури.

Німецький досвід реактивації 16 вугільних електростанцій у 2022 році підтвердив важливість підтримання стратегічних резервів генерації. Ізраїльська модель Національної кібербезпекової директорії продемонструвала переваги інтеграції фізичного та кібернетичного захисту з урахуванням галузевої специфіки.

6. Розробка практичних рекомендацій щодо посилення ролі публічного управління в забезпеченні енергетичної безпеки як складової протидії гібридним загрозам базується на результатах проведеного дослідження. В інституційній площині необхідна трансформація Антикризового енергетичного штабу при Кабінеті Міністрів України на повноцінний оперативний центр із правом прийняття обов'язкових рішень для всіх учасників енергетичного ринку в умовах надзвичайних ситуацій. У сфері децентралізації енергетики доцільним є

масштабування успішних практик територіальних громад: Чортківська громада (СЕС 22 кВт для лікарні, економія 178 тис. грн/рік), Долинська громада (СЕС 120 кВт, економія понад 1 млн грн/рік, концепція «енергоострова»), Бориславська громада (залучення приватних інвестицій), місто Харків (програма встановлення СЕС у лікарнях в умовах прифронтового міста). У кіберзахисті рекомендовано формування секторального центру реагування на комп'ютерні надзвичайні події на базі Міністерства енергетики, інтегрованого в національну систему під координацією CERT-UA.

У законодавчій площині пріоритетним є прискорене ухвалення законопроєктів № 13450 про інфраструктурні проєкти у сфері енергетики та № 14115 про захист об'єктів критичної інфраструктури. Кадрова проблема потребує диференційованого підходу до бронювання вузькопрофільних спеціалістів і запровадження спеціалізованих освітніх програм з децентралізованої енергетики. Ключовим є перехід від реактивного до проактивного управління, оскільки модель, що базується на героїзмі персоналу (160 загиблих та понад 300 поранених енергетиків за період повномасштабної війни), не може бути стійкою в довгостроковій перспективі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ACAPS. Ukraine: Energy Infrastructure Attacks – Impact Overview. Thematic Report. Geneva, 2025. 24 p. URL: https://www.acaps.org/fileadmin/Data_Product/Main_media/20250310_acaps_thematic_report_ukraine_energy_attacks.pdf (last accessed: 29.11.2025).

2. Agora Energiewende. Germany's Energy Transition: Ensuring Supply Security. 2024. URL: https://www.agora-energiewende.org/about-us/the-german-energiewende/how-can-germany-ensure-a-secure-energy-transition (last accessed: 29.11.2025).

3. Agora Energiewende. The German Energiewende. 2024. URL: https://www.agora-energiewende.org/about-us/the-german-energiewende (last accessed: 29.11.2025).

4. Butrimas V., Hajek J., Sukhodolia O. Hybrid warfare against Critical Energy Infrastructure: The Case of Ukraine. *Energy Highlights*. Vilnius: NATO ENSEC COE, 2024. № 18. P. 1-12. URL: https://www.enseccoe.org/publications/hybrid-warfare-against-critical-energy-infrastructure-the-case-of-ukraine/ (last accessed: 29.11.2025).

5. CE Energy News. EstLink 2 failure: security of supply intact. 2024. URL: https://ceenergynews.com/electricity/estlink2-failure-security-prices/ (last accessed: 29.11.2025).

6. DiXi Group. Countries interested in learning from Ukraine's experience in strengthening energy system resilience. 2024. URL: https://dixigroup.org/en/countries-interested-in-learning-from-ukraines-experience-in-strengthening-energy-system-resilience/ (last accessed: 29.11.2025).

7. DiXi Group. Аналітичні продукти: енергетичний вимір війни. 2025. URL: https://dixigroup.org/analytical-products/ (дата звернення: 29.11.2025).

8. DiXi Group. За два роки РФ здійснила 25 масованих атак на енергетику України. 2024. URL: https://dixigroup.org/za-dva-roky-rf-zdijsnyla-25-

masovanyh-atak-na-energetyku-ukrayiny/ (дата звернення: 29.11.2025).

9. EASAC. Europe's Energy Security and the Estlink-2 incident amid winter demands. 2025. URL: http://easac.eu/news/details/europes-energy-security-and-the-estlink-2-incident-amid-winter-demands (last accessed: 29.11.2025).

10. Energy Charter Secretariat. Ukrainian Energy Sector: Damage Assessment. Brussels, 2023. 45 p. URL: https://www.energycharter.org/fileadmin/DocumentsMedia/Occasional/2023_05_24_UA_sectoral_evaluation_and_damage_assessment_Version2.pdf (last accessed: 29.11.2025).

11. Energy Community Secretariat. Ukraine: Energy Security Comparative Analysis. 2023. URL: https://www.energy-community.org/ukraine.html (last accessed: 29.11.2025).

12. ENTSO-E. Continental Europe successful synchronisation with Ukraine and Moldova power systems. 16 March 2022. URL: https://www.entsoe.eu/news/2022/03/16/continental-europe-successful-synchronisation-with-ukraine-and-moldova-power-systems/ (last accessed: 29.11.2025).

13. ENTSO-E. Ukrainian Transmission System Operator, NPC Ukrenergo, joins ENTSO-E as new member. 14 December 2023. URL: https://www.entsoe.eu/news/2023/12/14/ukrainian-transmission-system-operator-npc-ukrenergo-joins-entso-e-as-new-member/ (last accessed: 29.11.2025).

14. European Commission. European Energy Security Strategy. COM(2014) 330 final. Brussels, 2014. URL: https://ec.europa.eu/energy/topics/security-of-supply/energy-security-strategy_en (last accessed: 29.11.2025).

15. European Commission. Joint Framework on countering Hybrid Threats: a European Union response. SWD(2016) 227 final. Brussels, 2016. 19 p. URL: https://data.consilium.europa.eu/doc/document/ST-11034-2016-INIT/en/pdf (last accessed: 29.11.2025).

16. European Commission. The Ukraine Facility. 2024. URL: https://commission.europa.eu/topics/eu-solidarity-ukraine/eu-assistance-ukraine/ukraine-facility_en (last accessed: 29.11.2025).

17. F. G. Conflict in the 21st Century: The Rise of Hybrid Wars.

Arlington: Potomac Institute for Policy Studies, 2007. 72 p. URL: https://potomacinstitute.us/reports/19-reports/1163-conflict-in-the-21st-century-the-rise-of-hybrid-wars (last accessed: 29.11.2025).

18. Forbes.ua. Понад 100 ракет і майже сотня дронів. Наслідки удару РФ по українській енергетиці 26 серпня 2024. URL: https://forbes.ua/news/rosiya-vchergove-atakue-ukrainu-raketami-i-dronami-e-problemi-z-energopostachannyam-onovlyuetsya-26082024-23228 (дата звернення: 29.11.2025).

19. Galeotti M. The Weaponisation of Everything: A Field Guide to the New Way of War. New Haven: Yale University Press, 2022. 256 p.

20. Hybrid CoE. The Landscape of Hybrid Threats: A Conceptual Model. Hybrid CoE Paper 1. Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2021. 15 p. URL: https://www.hybridcoe.fi/publications/hybrid-coe-paper-1-the-landscape-of-hybrid-threats-a-conceptual-model/ (last accessed: 29.11.2025).

21. International Energy Agency. IEA and Ukraine deepen bilateral cooperation with new joint work programme. Paris: IEA, 2024. URL: https://www.iea.org/news/iea-and-ukraine-deepen-bilateral-cooperation-with-new-joint-work-programme (last accessed: 29.11.2025).

22. IEA. Ukraine’s Energy Security and the Coming Winter. Paris: IEA, 2024. URL: https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter (last accessed: 29.11.2025).

23. Interfax-Україна. Завдяки допомозі ПРООН в Україні встановлено понад 450 МВт додаткової генерації. 23 травня 2025. URL: https://en.interfax.com.ua/news/economic/1074247.html (дата звернення: 29.11.2025).

24. International Energy Agency. Energy Security. Paris: IEA, 2022. URL: https://www.iea.org/topics/energy-security (last accessed: 29.11.2025).

25. LB.ua. Німеччина запускає 16 ТЕС на вугіллі для компенсації скорочення постачання газу з РФ. 2022. URL: https://lb.ua/economics/2022/07/17/523381_nimechchina_zapuskaie_16.html (дата звернення: 29.11.2025).

26. Murray W., Mansoor P. R. Hybrid Warfare: Fighting Complex Opponents

from the Ancient World to the Present. New York: Cambridge University Press, 2012. 320 p.

27. NATO STO. Energy Security in the Era of Hybrid Warfare. STO Technical Report SAS-163. Brussels, 2023. URL: https://www.google.com/search?q=https://publications.sto.nato.int/publications/STO%2520Technical%2520Reports/STO-TR-SAS-163/$$TR-SAS-163-ALL.pdf (last accessed: 29.11.2025).

28. NATO. Countering hybrid threats. *NATO Topics*. 2024. URL: https://www.nato.int/cps/en/natohq/topics_156338.htm (last accessed: 29.11.2025).

29. NATO. Energy Security. *NATO Topics*. 2024. URL: https://www.nato.int/cps/en/natohq/topics_49208.htm (last accessed: 29.11.2025).

30. RBC-Україна. Польща розпочала операцію із захисту критичної інфраструктури після НП із залізницею. 2025. URL: https://www.rbc.ua/rus/news/polshcha-rozpochala-operatsiyu-iz-zahistu-1763791690.html (дата звернення: 29.11.2025).

31. Rühle M. Energy as a Tool of Hybrid Warfare. *NATO Defense College Research Paper*. Rome, 2023. No. 8. 12 p. URL: https://www.ndc.nato.int/research/research.php?icode=0 (last accessed: 29.11.2025).

32. Rühle M., Grubliauskas J. Energy as a Tool of Hybrid Warfare. *NATO Defense College Research Paper*. 2015. № 113. URL: http://www.ndc.nato.int/news/news.php?icode=803 (last accessed: 29.11.2025).

33. Sweijs T., Zilincik S., Bekkers F., Meessen R. A Framework for Cross-Domain Strategies Against Hybrid Threats. The Hague: Hague Centre for Strategic Studies, 2021. 56 p. URL: https://euhybnet.eu/wp-content/uploads/2021/06/Framework-for-Cross-Domain-Strategies-against-Hybrid-Threats.pdf (last accessed: 29.11.2025).

34. The adoption of the law for prevention of abuse in wholesale energy markets (REMIT). *CMS Law-Now*. 2023. URL: https://cms-lawnow.com/en/ealerts/2023/09/the-adoption-of-the-law-for-prevention-of-abuse-in-wholesale-energy-markets-remit (last accessed: 29.11.2025).

35. Ukrainian Energy Security Dialogue 2024: Towards Resilience. Kyiv:

DiXi Group, 2024. 36 p. URL: https://dixigroup.org/storage/files/2024-12-19/uesd-2024-towards-resilience.pdf (last accessed: 29.11.2025).

36. UN Human Rights Monitoring Mission. Attacks On Ukraine's Electricity Infrastructure Threaten Key Aspects of Life As Winter Approaches. September 2024. URL: https://ukraine.ohchr.org/en/Attacks-On-Ukraines-Electricity-Infrastructure (last accessed: 29.11.2025).

37. USAID Energy Security Project. How did Ukraine synchronize with the EU's power system, and why is it important for the country's energy security? March 2023. URL: https://energysecurityua.org/news/how-did-ukraine-synchronize-with-the-eu-s-power-system/ (last accessed: 29.11.2025).

38. VoxUkraine. Біла книга реформ 2025. Розділ 7: Реформи енергетичного сектору. Київ, 2025. URL: https://voxukraine.org/bila-knyga-reform-2025-rozdil-7-reformy-energetychnogo-sektoru (дата звернення: 29.11.2025).

39. WeUkraine. Країни Балтії не виключають провокацій з боку РФ напередодні від'єднання від російської енергосистеми. 2025. URL: https://weukraine.tv/ekonomika/krajini-baltiji-ne-vikljuchajut-provokatsij-z-boku-rf-naperedodni-vidjednannja-vid-rosijskoji-enerhosistemi/ (дата звернення: 29.11.2025).

40. Бартлов А. «Доктрина Герасимова» та її роль у забезпеченні національної безпеки України. *Доктрини і політики*. 2018. № 79. С. 163-170. URL: http://jnas.nbuv.gov.ua/j-pdf/drpn_2018_79_17.pdf (дата звернення: 29.11.2025).

41. Бобко А. Енергетична безпека України: екологічні та військові загрози. *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки*. 2024. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2024/oct/36038/9_0.pdf (дата звернення: 29.11.2025).

42. Бугазіянус С. М. Механізми публічного управління: основні поняття, різновиди та приклад формування організаційно-правового механізму в контексті smart grid аналізу. *Економічний простір*. 2025. № 203. С. 23-34. DOI: 10.30838/EP.203.23-34.

43. Величко Л. Ю., Білоконь М. В. Гібридні загрози транспортній

інфраструктурі: виклики для державного регулювання та національної безпеки. *Теорія та практика державного управління*. 2024. № 2 (65). С. 10-20. URL: https://periodicals.karazin.ua/tpdu/article/download/25830/23207 (дата звернення: 29.11.2025).

44. Верховна Рада України. Верховна Рада України прийняла за основу проєкт Закону про інфраструктурні проєкти у сфері енергетики, які становлять суспільний інтерес (реєстр. № 13450). 2025. URL: https://www.rada.gov.ua/news/razom/267768.html (дата звернення: 30.11.2025).

45. Верховна Рада України. Законопроект № 14115: Про внесення змін до деяких законодавчих актів України щодо реконструкції, капітального ремонту, ремонту та інших інженерно-технічних заходів із захисту об'єктів критичної інфраструктури паливно-енергетичного сектору. 2025. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/57674 (дата звернення: 30.11.2025).

46. Гвоздій В. Чому Україні варто розвивати розподілену генерацію. *GoLaw*. 2025. URL: https://golaw.ua/ua/insights/energy-alert/chomu-ukrayini-varto-rozvivati-rozpodilenu-generacziyu/ (дата звернення: 29.11.2025).

47. Голос Америки. Залізний купол: як працює ізраїльська система протиповітряної оборони. 2024. URL: https://www.holosameryky.com/a/ppo-isreal/7806819.html (дата звернення: 29.11.2025).

48. Гранд М., Свйонтик О. Енергетична безпека України в умовах російсько-української війни (2014-2024): візії, концепції, пріоритети. *Axis Europae*. 2025. Вип. 6. С. 89-107. DOI: 10.69550/3041-1467.6.326259.

49. Децентралізація. Децентралізація енергетики та енергоефективність: як громади можуть забезпечити людей світлом, водою і теплом. 2024. URL: https://decentralization.ua/news/18206 (дата звернення: 30.11.2025).

50. Енергетична стратегія України: критичний аналіз. *Ділова економіка*. 2024. URL: http://www.dy.nayka.com.ua/?op=1&z=863 (дата звернення: 29.11.2025).

51. Жіночий енергетичний клуб України, UN Women. Гендерний вимір енергетичної кризи в Україні: шляхи до стійкості. 2025.

URL: https://ukraine.unwomen.org/en/digital-library/publications/2025/04/doslidzhennya-hendernyy-vymir-enerhetychnoyi-kryzy-v-ukrayini-shlyakhy-do-stiykosti (дата звернення: 29.11.2025).

52. Закон України № 3220-IX від 30 червня 2023 року «Про внесення змін до деяких законів України щодо відновлення та «зеленої» трансформації енергетичної системи України». URL: https://zakon.rada.gov.ua/laws/show/3220-IX (дата звернення: 30.11.2025).

53. Кисельов Є. В. Перспективи розвитку механізмів публічного управління забезпечення енергетичної безпеки. *Інвестиції: практика та досвід*. 2024. № 2. С. 216-218.

54. Комітет Верховної Ради України з питань енергетики та житлово-комунальних послуг. Офіційний вебсайт. 2025. URL: https://kompek.rada.gov.ua/ (дата звернення: 30.11.2025).

55. Концепція гібридної війни: 12 складових сучасного протистояння. Центр досліджень національної безпеки та стратегічних комунікацій (ЦЕНСС). 2024. URL: https://censs.org/concept-of-hybrid-warfare-and-its-components/ (дата звернення: 29.11.2025).

56. Кравчук О. В. Економічна безпека України в умовах гібридних загроз. *Економіка та держава*. 2024. № 5. С. 12-20. URL: https://journals.dpu.kyiv.ua/index.php/economy/article/view/442 (дата звернення: 29.11.2025).

57. Ксендзук В. В., Покотило М. Ю. Енергетична безпека України та світу: оцінка наслідків впливу російсько-української війни та прогнози трансформації ринку. *Економіка, менеджмент та аудит*. 2025. № 2 (112). С. 46-53. DOI: 10.26642/ema-2025-2(112)-46-53. URL: https://ema.ztu.edu.ua/article/view/335558 (дата звернення: 29.11.2025).

58. Магда Є. Гібридна війна: вижити і перемогти. Київ: Наш Формат, 2015. 304 с.

59. Матеріали VII Міжнародної конференції «NucNext-2025: Перспективи впровадження інновацій у атомну енергетику». Київ: ІПБ АЕС

НАН України, 2025. URL: https://www.nas.gov.ua/news/golovni-pidsumki-vii-mizhnarodno-konferenci-nucnext-2025 (дата звернення: 29.11.2025).

60. Міністерство енергетики України. Ukraine and Poland unite efforts to strengthen energy security. 2025. URL: https://www.mev.gov.ua/en/news/ukraine-and-poland-unite-efforts-strengthen-energy-security (last accessed: 29.11.2025).

61. Міністерство енергетики України. Стабільне проходження минулої зими – перемога для всієї енергетичної галузі. 2025. URL: https://mev.gov.ua/novyna/stabilne-prokhodzhennya-mynuloyi-zymy-peremoha-dlya-vsiyeyi-enerhetychnoyi-haluzi (дата звернення: 30.11.2025).

62. Національний інститут стратегічних досліджень. «Життя як в Ізраїлі»: висновки з досвіду забезпечення національної безпеки для України. 2023. URL: https://niss.gov.ua/news/komentari-ekspertiv/zhyttya-yak-v-izrayili-vysnovky-z-dosvidu-zabezpechennya-natsionalnoyi (дата звернення: 29.11.2025).

63. Помаза-Пономаренко А. Л., Тарадуда Д. В. Світовий досвід протистояння впливу гібридної війни на національну й енергетичну безпеку та її об’єкти. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2024. Вип. 9. С. 142-150. DOI: 10.31470/2786-6246-2024-9-142-150.

64. Про затвердження Тимчасового порядку врегулювання відносин на ринку електричної енергії: Постанова Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг від 12 квітня 2022 р. № 386. URL: https://www.nerc.gov.ua (дата звернення: 29.11.2025).

65. Про критичну інфраструктуру: Закон України від 16 листопада 2021 р. № 1882-IX (із змінами, редакція від 21 вересня 2024 р.). URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 29.11.2025).

66. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII (в редакції 2022 р.). URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 29.11.2025).

67. Про Національну комісію, що здійснює державне регулювання у сферах енергетики та комунальних послуг: Закон України від 22 вересня 2016 р. № 1540-VIII (із змінами, редакція від 28 серпня 2025 р.). URL:

https://zakon.rada.gov.ua/laws/show/1540-19 (дата звернення: 29.11.2025).

68. Про ринок електричної енергії: Закон України від 13 квітня 2017 р. № 2019-VIII (із змінами, редакція від 28 серпня 2025 р.). URL: https://zakon.rada.gov.ua/laws/show/2019-19 (дата звернення: 29.11.2025).

69. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037 (дата звернення: 29.11.2025).

70. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020 (дата звернення: 29.11.2025).

71. Про схвалення Енергетичної стратегії України на період до 2050 року: Розпорядження Кабінету Міністрів України від 21.04.2023 № 373-р. URL: https://zakon.rada.gov.ua/laws/show/373-2023-р (дата звернення: 29.11.2025).

72. Проблеми й перспективи енергетичної політики в Україні з погляду національної безпеки. *Літопис Волині*. 2024. URL: http://www.litopys.volyn.ua/index.php/litopys/article/view/623 (дата звернення: 29.11.2025).

73. Проект Плану відновлення України: Енергетична безпека. Кабінет Міністрів України. 2022. URL: https://www.kmu.gov.ua/storage/app/sites/1/recoveryrada/ua/energy-security.pdf (дата звернення: 29.11.2025).

74. Рада національної безпеки і оборони України. Річний аналітичний огляд: ключові події, тенденції та виклики у сфері кібербезпеки у 2024 році. 2025. URL: https://www.rnbo.gov.ua/ua/Diialnist/7095.html (дата звернення: 30.11.2025).

75. РБК-Україна. Росія найближчим часом може відновити масовані обстріли енергетики – Литвиненко. 2024. URL: https://www.rbc.ua/ukr/news/rosiya-nayblizhchim-chasom-mozhe-vidnoviti-1728982744.html (дата звернення: 30.11.2025).

76. Рябченко О. П. Деякі правові засади розуміння енергетичної безпеки. *Вісник Ужгородського національного університету. Серія: Право*. 2025. № 89,

ч. 3. DOI: 10.24144/2307-3322.2025.89.3.11. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/336475 (дата звернення: 29.11.2025).

77. CAEE. Розподілена генерація – основа енергетично незалежних громад. 2025. URL: https://saee.gov.ua/news/rozpodilena-heneratsiia-osnova-enerhetychno-nezalezhnykh-hromad (дата звернення: 29.11.2025).

78. Суспільне Івано-Франківськ. Енергоострів у Долині: як на Франківщині громада створює енергетичну автономію. 2025. URL: https://suspilne.media/ivano-frankivsk/1137364-u-dolini-na-frankivsini-hocut-stvorit i-energoostriv-so-ce-oznacae/ (дата звернення: 30.11.2025).

79. Суспільне Харків. Сонячні панелі встановили на даху лікарні у Харкові: це альтернативне живлення. 2024. URL: https://suspilne.media/kharkiv/794607-u-harkovi-likarnu-obladnali-sonacnou-elektrostancieu-ak-vona-dopomoze-pid-cas-znestrumlen/ (дата звернення: 30.11.2025).

80. Суходоля О. М., Харазішвілі Ю. М., Рябцев Г. Л. Енергетична безпека України: перспективна модель управління ризиками: монографія. Київ: НІСД, 2023. 168 с. ISBN 978-966-554-361-9. DOI: 10.53679/NISS-book.2023.01.

81. Сучасні проблеми та суперечності реалізації державної енергетичної політики. *Public Administration*. 2024. URL: https://journals.politehnica.dp.ua/index.php/public/article/view/227 (дата звернення: 29.11.2025).

82. Указ Президента України № 695/2023 від 17 жовтня 2023 року «Про рішення Ради національної безпеки і оборони України від 17 жовтня 2023 року «Про організацію захисту та забезпечення безпеки функціонування об’єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій»». URL: https://zakon.rada.gov.ua/laws/show/695/2023 (дата звернення: 30.11.2025).

83. Центр Разумкова, DiXi Group. Публічна дискусія «Енергетика без кордонів: Україна та Польща разом до Європи». 2024. URL: https://razumkov.org.ua/novyny/uchast-u-publichnii-dyskusii-energetyka-bez-kordoniv-ukraina-ta-polshcha-razom-do-yevropy (дата звернення: 29.11.2025).

84. Центр Разумкова. Енергетика України 2024-2025 років у тумані

невизначеності. 2024. URL: https://razumkov.org.ua/statti/energetyka-ukrainy-20242025-rokiv-u-tumani-nevyznachenosti (дата звернення: 30.11.2025).