УДК 342.951
DOI https://doi.org/10.24144/2788-6018.2025.04.2.61

ОРГАНІЗАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ ВІД КІБЕРАТАК ТА ДРОНОВИХ НЕБЕЗПЕК УКРАЇНИ

Тімашов В.О.,
доктор юридичних наук, професор,
професор кафедри адміністративного, фінансового
та інформаційного права
Державного торговельно-економічного університету
ORCID: 0000-0001-8368-8856

Адамович В.О.,
здобувач магістерського рівня вищої освіти
факультету інформаційних технологій
Державного торговельно-економічного університету

Тімашов В.О., Адамович В.О. організаційно-правове забезпечення енергетичної безпеки від кібератак та дронових небезпек України.

У статті здійснено комплексне дослідження організаційно-правових аспектів забезпечення енергетичної безпеки України в умовах зростаючих гібридних загроз, що охоплюють як кібератаки, так і атаки із застосуванням безпілотних літальних апаратів (БПЛА). Актуальність теми зумовлена високою вразливістю енергетичної інфраструктури до новітніх викликів, що на тлі повномасштабної збройної агресії російської федерації проти України набули системного та загрозливого характеру. Особливу увагу приділено аналізу сучасного стану нормативно-правового забезпечення сфери енергетичної безпеки, виявлено ключові прогалини в національному законодавстві, пов'язані з відсутністю чітко окресленої концепції енергетичної безпеки, недостатньою координацією між уповноваженими органами влади та відсутністю єдиної вертикалі управління.

У роботі доведено, що кіберзагрози та дронові атаки є складовими гібридної війни, що поєднує військові й невійськові засоби дестабілізації держави. У цьому контексті енергетичний сектор України перетворився на мішень системних і високотехнологічних атак, наслідками яких є значні порушення в енергопостачанні, руйнування критичної інфраструктури, економічні збитки та загрози для життя і здоров'я громадян. Проаналізовано найрезонансніші випадки кібератак на енергетичні об'єкти України, зокрема інциденти із застосуванням шкідливого програмного забезпечення BlackEnergy, Industroyer та Industroyer2. Розкрито методи і засоби, які використовуються агресором для здійснення технічно складних атак, що вимагає високого рівня підготовки з боку держави у сфері кіберзахисту.

Здійснено характеристику чинної нормативно-правової бази, зокрема законів України «Про національну безпеку» та «Про критичну інфраструктуру», а також проаналізовано проєкти та пропозиції, спрямовані на реформування системи енергетичної безпеки. Автори обґрунтовують необхідність формування цілісної законодавчої моделі, яка передбачатиме конституційне закріплення статусу незалежних регуляторних органів, чіткий розподіл повноважень між усіма суб'єктами системи безпеки, а також інтеграцію України до європейського енергетичного простору з урахуванням стандартів ЄС. У статті визначено ключові інституційні недоліки, зокрема брак міжвідомчої взаємодії, недостатню участь органів місцевого самоврядування та громадянського суспільства у реалізації заходів енергетичної безпеки, а також низький рівень правового залучення приватного сектору до цієї діяльності.

Особливу увагу приділено пропозиціям щодо удосконалення організаційно-правового механізму протидії загрозам у сфері енергетики. Запропоновано запровадження нових механізмів державно-приватного партнерства, розвиток систем раннього виявлення загроз, цифрової стійкості, а також інвестицій у модернізацію енергетичних об'єктів із метою зниження їх вразливості до атак. Також акцентовано на важливості розвитку відновлюваної енергетики як інструменту територіальної децентралізації постачання, що підвищує гнучкість та адаптивність енергетичної системи.

У підсумку автори доходять висновку, що забезпечення енергетичної безпеки України в умовах сучасних гібридних загроз вимагає не лише оновлення законодавчої бази та реформування державного управління, а й побудови системи, здатної динамічно реагувати на нові виклики, інтегруючись у європейський і світовий безпековий простір.

Ключові слова: енергетична безпека, кібератаки, безпілотні літальні апарати, гібридна війна, критична інфраструктура, організаційно-правове забезпечення, національна безпека, відновлювана енергетика.

Timashov V.O., Adamovych V.O. Organizational and legal support for Ukraine's energy security against cyberattacks and drone threats.

This article presents a comprehensive study of the organisational and legal aspects of ensuring Ukraine's energy security in the context of escalating hybrid threats, which encompass both cyberattacks and assaults involving unmanned aerial vehicles (UAVs). The relevance of the topic is driven by the heightened vulnerability of energy infrastructure to emerging challenges that have acquired a systemic and critical nature amidst the full-scale military aggression of the Russian Federation against Ukraine. Particular attention is given to the analysis of the current state of Ukraine's regulatory and legal framework in the field of energy security, with an emphasis on identifying key shortcomings in the national legislation. These include the absence of a clearly defined concept of energy security, insufficient coordination among authorised government institutions, and the lack of a unified administrative structure.

The study substantiates that cyber threats and drone attacks are integral components of hybrid warfare, which combines military and non-military methods of destabilisation. In this context, Ukraine's energy sector has become a prime target for systematic and technologically sophisticated attacks, resulting in severe disruptions to energy supply, the destruction of critical infrastructure, significant economic damage, and increased risks to public safety. The article analyses prominent cases of cyberattacks against Ukrainian energy infrastructure, particularly those involving malicious software such as BlackEnergy, Industroyer, and Industroyer2. These incidents underscore the adversary's technical preparedness and access to industrial control system protocols, which necessitates a high level of cybersecurity readiness on the part of the state.

The paper provides an overview of the existing legal framework, including the Laws of Ukraine «On National Security» and «On Critical Infrastructure», and reviews current legislative initiatives aimed at reforming the energy security system. The authors argue for the development of a unified legislative model that includes the constitutional recognition of the status of independent regulatory authorities, a clear delineation of competences among all relevant actors, and the alignment of national legislation with European Union standards. Institutional weaknesses are also discussed, particularly the lack of effective interagency collaboration, limited involvement of local self-government bodies and civil society in ensuring energy security, and the insufficient legal inclusion of private sector entities.

The article proposes several measures to strengthen the organisational and legal mechanisms for countering threats to the energy sector. These include the development of public-private partnerships, the implementation of early threat detection systems, the enhancement of digital resilience, and investment in the modernisation of energy facilities to mitigate vulnerabilities. The promotion of renewable energy is also emphasised, not only for environmental considerations but as a means of achieving territorial decentralisation and improving the flexibility and sustainability of the energy system.

In conclusion, the authors argue that safeguarding Ukraine's energy security in the face of hybrid threats requires a comprehensive transformation of the organisational and legal infrastructure. This transformation must be grounded in modern legislative reforms, strategic governance restructuring, and the integration of Ukraine into the broader European energy and security landscape. The findings of this research may serve as a basis for shaping effective public policy in the energy sector, particularly with regard to legal reform, institutional development, and strategic planning.

Key words: energy security, cyberattacks, unmanned aerial vehicles, hybrid warfare, critical infrastructure, organisational and legal framework, national security, renewable energy.

Постановка проблеми. Питання енергетичної безпеки постає як один із ключових пріоритетів національної безпеки в умовах сучасних геополітичних викликів і трансформацій глобального безпекового середовища. Енергетична інфраструктура відіграє стратегічну роль у забезпеченні стабільного функціонування державних інституцій, підприємств, об'єктів критичної інфраструктури та життєдіяльності населення. Водночас її вразливість до новітніх загроз, зокрема кібератак та атак із використанням безпілотних літальних апаратів, зростає пропорційно до рівня технологічного розвитку і цифровізації енергетичних систем. В умовах збройної агресії росії проти України саме енергетичний сектор став однією з головних цілей скоординованих деструктивних дій, що включають як фізичне ураження об'єктів за допомогою дронів, так і руйнування цифрової інфраструктури шляхом кібератак.

Наявні організаційно-правові механізми протидії зазначеним загрозам демонструють низку системних вад, серед яких – нормативна фрагментарність, відсутність ефективного міжвідомчого механізму координації, недостатній рівень технічного та кадрового забезпечення сфер кібербезпеки й захисту об'єктів критичної інфраструктури. Більшість законодавчих ініціатив, що регламентують захист енергетичного сектору, не враховують повною мірою специфіку новітніх викликів, зокрема синергію кібер- та дронових загроз у межах гібридної війни. Крім того, впровадження інструментів цифрового захисту, включаючи системи раннього виявлення атак, штучний інтелект та автоматизоване управління ризиками, потребує належного правового підґрунтя та ресурсної підтримки з боку держави.

В умовах війни загрози такого типу не лише набувають більшої інтенсивності, а й ускладнюються непередбачуваністю, високою технологічністю та прихованістю. Фактичне застосування дронів-камікадзе проти трансформаторних підстанцій, ТЕЦ, ГЕС та інших ключових елементів енергетичної системи України, а також масові кібератаки, що мали на меті дестабілізацію енергопостачання, свідчать про необхідність переосмислення існуючих підходів до захисту цієї галузі. Забезпечення надійного правового фундаменту для захисту енергетичного сектору, впровадження комплексних механізмів кібер- і фізичної безпеки, а також підвищення здатності держави реагувати на високотехнологічні загрози виступають передумовами збереження функціональності ключових систем держави в умовах тривалої воєнної дестабілізації.

Метою статті є всебічний аналіз організаційно-правового забезпечення енергетичної безпеки України в умовах загострення загроз, пов'язаних із кібератаками та застосуванням безпілотних літальних апаратів, а також обґрунтування напрямів удосконалення нормативно-правових та інституційних механізмів захисту енергетичної інфраструктури в контексті сучасної гібридної війни та глобальних викликів безпеки.

Виклад основного матеріалу. У науковій праці О.М. Павлової, В.К. Павлова, О.В. Новосад та Л.П. Матійчук [1, с. 86] підкреслюється відсутність чіткої методології щодо конкретизації сфери діяльності, впливу та структурних елементів енергетичної безпеки. Автори здійснили ґрунтовний аналіз наукових підходів і тлумачень поняття «енергетична безпека», запропонованих різними дослідниками та науковими установами. На основі узагальнення наявних теоретичних підходів, вони сформулювали висновок, згідно з яким енергетична безпека розглядається як здатність держави забезпечувати потреби суспільства в енергетичних ресурсах на економічно та технічно обґрунтованому рівні, з метою гарантування стабільного, якісного та безпечного енергоспоживання, водночас забезпечуючи захист національних інтересів енергетичного сектору від потенційних внутрішніх і зовнішніх загроз [1, с. 87].

Концептуалізація енергетичної безпеки характеризується динамічністю, що зумовлена впливом технологічного прогресу, трансформацією способів виробництва й споживання енергії, а також виникненням нових загроз у міжнародному середовищі. На ранніх етапах розвитку цивілізації під енергетичною безпекою розуміли, передусім, забезпечення доступу до джерел енергії, зокрема легкозаймистих матеріалів, таких як деревина, з мінімальними ризиками та витратами. Упродовж XX ст. домінуючим аспектом енергетичної безпеки була стабільність постачання енергетичної сировини. Натомість у XXI ст. цей аспект становить лише один із компонентів більш комплексного уявлення про енергетичну безпеку. З огляду на стрімке зростання енергетичних потреб сучасного суспільства, енергетична безпека набула статусу критично важливого елементу системи національної безпеки [2, с. 38]. Зростаюча вразливість енергетичної сфери потребує постійного моніторингу, ефективних захисних заходів та системного аналізу у взаємозв'язку з екологічною, геополітичною, економічною та іншими складовими безпеки. Отже, трактування енергетичної безпеки має контекстуальний характер і змінюється відповідно до нових викликів і умов функціонування [2, с. 40].

Від початку XXI ст. енергетична безпека набула статусу одного з пріоритетних стратегічних напрямів, що знаходить відображення у військових доктринах та стратегіях національної безпеки. Аналіз подій останніх років свідчить про те, що енергетична безпека стала однією з найактуальніших і водночас найуразливіших сфер як для України, так і для держав – членів НАТО в умовах ескалації гібридних загроз [3, с. 143].

Поняття «гібридна загроза» трактується як сукупність дій, що здійснюються державними або недержавними суб'єктами з метою дестабілізації сталого розвитку або заподіяння шкоди шляхом застосування відкритих та/або прихованих військових і невійськових засобів. У цьому контексті гібридна війна становить суттєву загрозу для енергетичного сектору, оскільки її наслідки можуть мати деструктивний вплив на політичну, соціальну та військову стабільність, а також порушувати узгодженість дій в межах Північноатлантичного альянсу. З огляду на ключову роль енергетичного сектору у забезпеченні функціонування держав і міжнародних організацій, актуалізується необхід-

ність його адаптації до умов посилення гібридних загроз. В умовах триваючої агресії проти України держава-агресор здійснює цілеспрямовані гібридні атаки на об'єкти енергетичної інфраструктури, зокрема на об'єкти критичної інфраструктури загальнодержавного значення [3, с. 144].

Особливістю гібридної війни є те, що енергетичні об'єкти піддаються не лише фізичним атакам (саботажу, збройним нападам), але й кіберзагрозам, дезінформаційним кампаніям, маніпулюванню енергоринками, дипломатичному та економічному тиску. Такі акти значно ускладнюють виявлення джерела загрози та формування ефективної відповіді, адже межа між воєнними та невоєнними методами впливу є розмитою.

У контексті зростання інтенсивності гібридної агресії, особливу загрозу для енергетичної сфери становлять кібератаки та атаки із застосуванням безпілотних літальних апаратів (БПЛА). Успішні реалізації таких атак спричиняють суттєві операційні збої, призводять до зупинки виробництва, руйнування елементів інфраструктури, порушення безперебійного енергопостачання, а також завдають значних фінансових втрат як окремим енергетичним компаніям, так і економіці держави в цілому.

Україна, перебуваючи в епіцентрі повномасштабної військової агресії, фактично перетворилася на експериментальний полігон для випробування новітніх інструментів кібервійни. Така ситуація, хоча й є вкрай загрозливою, водночас створює унікальні умови для накопичення практичного досвіду, що є надзвичайно цінним для розуміння трансформації кіберзагроз та удосконалення механізмів протидії. В умовах стрімкої еволюції форм кібератак – від втручання в диспетчерські системи до масових атак на мережі постачання – критично важливо забезпечити надійний захист інформаційних систем енергетичних об'єктів, зокрема об'єктів критичної інфраструктури [4, с. 188].

Паралельно з кіберзагрозами, дедалі більш системного характеру набувають дронові атаки, які завдяки високій мобільності та точності ураження дозволяють агресору завдавати шкоди енергетичним об'єктам навіть на значній глибині оборони. Масове застосування БПЛА актуалізувало необхідність стратегічного перегляду підходів до побудови енергетичної системи. Зокрема, все більшої ваги набуває розвиток відновлюваних джерел енергії не лише з міркувань екологічної безпеки, а й через їхню територіальну розосередженість, здатність функціонувати автономно та забезпечувати локальні потреби в енергопостачанні. Така децентралізація енергетичних потужностей дозволяє знизити вразливість національної енергосистеми до масованих атак і сприяє підвищенню енергетичної стійкості держави [5, с. 109].

Енергетична безпека становить один із ключових об'єктів національної безпеки України, що набуває особливої актуальності в умовах дії воєнного стану. Попри визначення її значущості у Законі України «Про національну безпеку України» [6], спеціальне законодавче регулювання в цій сфері досі відсутнє, що зумовлює потребу у створенні додаткових правових механізмів для реалізації державної політики в енергетичному секторі [7, с. 61].

Організаційно-правове забезпечення енергетичної безпеки включає два взаємопов'язані компоненти: нормативно-правовий та інституційно-правовий. Перший передбачає створення нормативної бази для стабільного функціонування енергетичних ринків, узгодження повноважень органів влади, наближення українського законодавства до права ЄС, а також запровадження податкових пільг та посилення відповідальності за посягання на об'єкти енергетичної інфраструктури [7, с. 62].

Інституційно-правовий компонент охоплює діяльність уповноважених органів, зокрема Кабінету Міністрів України, Міністерства енергетики та інших суб'єктів, які забезпечують координацію та реалізацію енергетичної політики. Важливими напрямами інституційної діяльності є забезпечення сталого розвитку енергетики, диверсифікація джерел енергопостачання, підвищення енергоефективності, інтеграція в європейські енергетичні ринки, а також розвиток відновлюваних джерел енергії [7, с. 61-62].

З урахуванням збройної агресії проти України, держава змушена адаптувати чинне правове поле до умов воєнного стану. Зокрема, було запроваджено низку тимчасових регуляторних рішень: продаж електроенергії на аукціонах, податкові пільги на ввезення обладнання, підтримка державних енергетичних підприємств та звільнення від митних зборів на критичні товари для енергетичного сектору [7, с. 63].

Окрему увагу в умовах війни приділено захисту критичної інфраструктури. Відповідно до Закону України «Про критичну інфраструктуру» [8], об'єкти енергетики визнаються стратегічно важливими. Організаційно-правові механізми захисту передбачають функціонування розгалуженої системи суб'єктів, до яких належать як державні органи, так і приватні оператори інфраструктури. У перспективі передбачено створення спеціалізованого органу – Державної служби захисту критичної інфраструктури, проте на період дії воєнного стану відповідні повноваження покладено на Державну службу спеціального зв'язку та захисту інформації [7, с. 64].

Аналіз законодавчих ініціатив демонструє наявність спрямування на посилення державного контролю та координації у сфері енергетики, однак практична реалізація багатьох проектів залишається на початковому етапі. На цьому фоні необхідним є забезпечення безперервного правового моніторингу, розробка довгострокової енергетичної стратегії, а також впровадження механізмів державно-приватного партнерства для модернізації енергетичної інфраструктури [7, с. 65]. Організаційно-правове регулювання енергетичної безпеки України перебуває на етапі трансформації, що спричинено як воєнними загрозами, так і загальною потребою в структурних реформах. Забезпечення енергетичної незалежності та стабільності функціонування енергетичного сектору потребує подальшої розробки цілісної законодавчої бази, поглиблення міжвідомчої координації та інтеграції в європейську енергетичну систему [7, с. 66].

Кібератаки на енергетичний сектор України є складовою системної гібридної війни, яку росія веде проти України з 2014 р. Одним із найвідоміших інцидентів стала атака із застосуванням шкідливого програмного забезпечення BlackEnergy, що у грудні 2015 р. призвела до тимчасового відключення електропостачання для близько 230 тис. споживачів у трьох областях – Івано-Франківській, Чернігівській та Київській [9]. Відповідальність за атаку була покладена на угруповання Sandworm, пов'язане зі спецслужбами рф.

У 2016 р. зафіксовано ще одну кібератаку на ПАТ «Укренерго», під час якої було використано більш складний зразок шкідливого ПЗ – Industroyer (CrashOverride). Цей інструмент безпосередньо взаємодіє з промисловими протоколами, що керують об'єктами енергетики. Він дозволяє не тільки виводити з ладу обладнання, але й створювати затримки у відновленні систем шляхом модифікації налаштувань керування [10]. У 2022 р. було виявлено нову модифікацію – Industroyer2, яка знову націлювалася на українську енергетику під час війни, але була нейтралізована до моменту розгортання [11].

Вищезгадані атаки свідчать про глибоку технічну підготовку противника, наявність доступу до специфікацій промислових протоколів, а також можливість тривалого прихованого проникнення у внутрішні мережі енергетичних компаній.

У період з осені 2022 р. до весни 2023 р. росія здійснювала масовані удари по об'єктах енергетичної інфраструктури із застосуванням дронів-камікадзе типу Shahed-136 і ракет великої дальності. Напади були спрямовані на електростанції, високовольтні підстанції, об'єкти розподільчої інфраструктури та системи резервного живлення. Наприклад, внаслідок атак 10 жовтня 2022 р., було уражено понад 30% генеруючих потужностей України, що призвело до віялових відключень по всій країні [12].

У грудні 2022 р. дрони атакували підстанції «Укренерго» у Київській, Одеській та Дніпропетровській областях, у результаті чого відбулися тривалі перебої з електропостачанням, а також пошкоджено критичне обладнання, відновлення якого потребувало значних технічних ресурсів. Спостерігалася чітка координація між кібератаками на системи моніторингу та фізичними ударами безпілотників, що посилювало ефект дестабілізації.

Українська енергетична інфраструктура – це складна технічна система, що включає старі радянські елементи, а також сучасні цифрові технології, інтегровані з європейськими мережами. Її вразливість зумовлена:

– застарілою архітектурою окремих технологічних вузлів;

– недостатнім рівнем сегментації внутрішніх мереж автоматизації;

– недостатньою кількістю засобів захисту від безпілотних літальних апаратів;

– обмеженими ресурсами для резервного живлення та швидкого технічного відновлення після уражень.

За даними Держспецзв'язку, тільки у першому півріччі 2023 р. на об'єкти критичної інфраструктури було зафіксовано понад 762 кібератак, з яких значна частина спрямовувалася саме на енергетичний сектор [13]. В умовах постійної воєнної загрози забезпечення енергетичної безпеки потребує глибокої модернізації систем захисту SCADA, впровадження багаторівневого моніторингу, а також активного розвитку контрдій проти дронів.

Опираючись на розглянуті публікації та аналізуючи роботу А.А. Цибка [14, с. 70–73] бачимо, що сьогодні в системі суб'єктів забезпечення енергетичної безпеки України існує ряд невирішених проблем, що заважають її ефективному функціонуванню. Найбільш гостро стоїть питання відсутності в законодавстві України розуміння єдиної системи забезпечення енергетичної безпеки України. Для системи енергетичної безпеки важливо приділити особливу увагу правовому статусу та місцю в цій системі центрального органу виконавчої влади. Іншою проблемою є відсутність положень у Конституції України, які б закріплювали основні засади правового статусу незалежних регуляторних органів, зокрема Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг. Існують проблеми з використанням потенціалу та залученням до

вирішення проблем енергетичної безпеки активного громадянського суспільства, а також органів місцевого самоврядування. Невирішеним залишається питання щодо включення до системи суб'єктів, які здійснюють забезпечення енергетичної безпеки України, окремих юридичних осіб.

Опираючись на публікації розглянуті вище та дослідження А.А. Цибка [14, с. 70–73], у системі організаційно-правового забезпечення енергетичної безпеки України виявляється низка суттєвих проблем і викликів, які суттєво ускладнюють ефективне функціонування відповідної системи. Однією з ключових проблем є відсутність у чинному законодавстві єдиного, чіткого визначення концепції та структури системи енергетичної безпеки держави. Дана проблема породжує розпорошеність повноважень і неузгодженість між суб'єктами, відповідальними за реалізацію енергетичної політики та захист національних інтересів у енергетичній сфері.

Також залишається неврегульованим питання включення до системи суб'єктів енергетичної безпеки окремих юридичних осіб, що могли б забезпечити більш гнучке та оперативне реагування на загрози в енергетичній сфері.

До того ж, сучасні виклики вимагають адаптації організаційно-правового механізму до швидкозмінних геополітичних умов, розвитку технологій та інтеграції з європейськими та світовими стандартами. Відсутність системного підходу і затверджених стратегічних документів у цій сфері створює додаткові ризики, знижуючи здатність держави ефективно реагувати на зовнішні та внутрішні загрози енергетичній безпеці.

Для вдосконалення організаційно-правового механізму захисту енергетичної сфери України доцільно запропонувати комплекс заходів, спрямованих на підвищення ефективності управління та забезпечення стабільності енергетичної безпеки, серед яких наступні:

– необхідно законодавчо закріпити єдину систему організаційного забезпечення енергетичної безпеки, що включатиме чітке визначення ролей, повноважень та відповідальності суб'єктів цієї системи, що сприятиме усуненню розпорошеності функцій та покращенню координації між центральними органами виконавчої влади, регуляторними структурами та іншими учасниками процесу;

– конституційне закріплення правового статусу незалежних регуляторних органів, зокрема Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг, що забезпечить стабільність функціонування регуляторів, підвищить рівень їхньої автономії та сприятиме формуванню прозорого та прогнозованого регуляторного середовища;

– слід розробити та впровадити механізми активного залучення органів місцевого самоврядування і громадянського суспільства до процесів планування, контролю та реалізації заходів із забезпечення енергетичної безпеки, що сприятиме формуванню більш гнучкої та адаптивної системи, здатної оперативно реагувати на регіональні виклики та зміни.

– необхідно врегулювати включення окремих юридичних осіб до системи суб'єктів, відповідальних за захист енергетичної сфери, що дозволить підвищити оперативність та ефективність реагування на потенційні загрози, а також розширить інструментарій протидії кризовим ситуаціям;

– необхідно оновити нормативно-правову базу з урахуванням сучасних викликів, зокрема геополітичних загроз, цифровізації енергетичних систем та інтеграції з європейськими стандартами, що сприятиме зміцненню енергетичної безпеки як національного пріоритету.

Висновки. Отже, енергетичний сектор, як складова критичної інфраструктури, став однією з головних цілей гібридної агресії російської федерації, яка поєднує ураження об'єктів фізичної інфраструктури та руйнування цифрових систем управління. Встановлено, що чинна нормативно-правова база не відповідає повною мірою сучасним викликам, що виявляється у фрагментарності законодавства, нечітко визначених повноваженнях органів державної влади та недостатньому рівні координації між суб'єктами, відповідальними за реалізацію політики у сфері енергетичної безпеки.

Гібридна війна виявила значну вразливість енергетичної інфраструктури до кібератак і дронових загроз, які ускладнюють своєчасне виявлення джерел атак і потребують нового підходу до захисту об'єктів енергетики. В роботі проведено аналіз законодавчих ініціатив, які покликані модернізувати систему енергетичної безпеки, однак більшість із них поки що перебувають на етапі розробки або не мають практичного втілення.

З огляду на воєнний стан, доцільним є залучення органів місцевого самоврядування, інститутів громадянського суспільства та окремих юридичних осіб до процесів забезпечення енергетичної безпеки. Важливим також є модернізація технічної інфраструктури, впровадження інноваційних засобів захисту, розвитку відновлюваних джерел енергії як інструменту підвищення стійкості енергосистеми. Таким чином, організаційно-правовий механізм забезпечення енергетичної безпеки України потребує системного оновлення відповідно до вимог цифрової трансформації, умов гібридної війни та стратегічного курсу на європейську інтеграцію.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Павлова О.М., Павлов К.В., Новосад О.В., Матійчук Л.П. Сутність енергетичної безпеки України в умовах трансформаційних змін. *Актуальні проблеми інноваційної економіки*. 2021. № 2. С. 84–91. URL: https://repo.btu.kharkov.ua//handle/123456789/24993.
2. Горбатенко В.П., Кукуруз О.В. Енергетична безпека: зміна підходів до розуміння. *Політикус*. 2023. № 4. С. 37–42. URL: http://dspace.pdpu.edu.ua/handle/123456789/18636.
3. Помаза-Пономаренко А., Тарадуда Д. Світовий досвід протистояння впливу гібридної війни на національну й енергетичну безпеку та її об'єкти. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2024. № 9. С. 142–150. DOI: https://doi.org/10.31470/2786-6246-2024-9-142-150.
4. Фесенко О.Д. та ін. Аналіз динаміки кібератак на об'єкти критичної інфраструктури в умовах геополітичної напруженості. *Системи і технології зв'язку, інформатизації та кібербезпеки*. 2025. № 7. С. 187–201. DOI: https://doi.org/10.58254/viti.7.2025.17.187.
5. Мацерук А.А. Забезпечення сталого розвитку громад в умовах війни: проблеми та інструменти їх вирішення. *Київський економічний науковий журнал*. 2024. № 7. С. 105–111. DOI: https://doi.org/10.32782/2786-765X/2024-7-15.
6. Про національну безпеку. Закон України від 21.06.2018 № 2469-VIII // Офіційний вебпортал парламенту України: [Веб-сайт]. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 29.05.2025).
7. Муза О. Організаційно-правові засади забезпечення енергетичної безпеки України в умовах воєнного стану. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2023. № 1(122). С. 60–66. DOI: https://doi.org/10.31733/2078-3566-2023-1-60-66.
8. Про критичну інфраструктуру. Закон України від 16.11.2021 № 1882-IX / Офіційний вебпортал парламенту України: [Веб-сайт]. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 29.05.2025).
9. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid // WIRED: [Website]. 2016. URL: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (viewed on: 29.05.2025).
10. CRASH OVERRIDE: Analysis of the Threat to Electric Grid Operations // The National Security Archive. URL: https://nsarchive.gwu.edu/sites/default/files/documents/3869008/Dragos-CRASHOVERRIDE-Analyzing-the-Threat-to.pdf (viewed on: 29.05.2025).
11. Ukraine energy grid hit by Russian Industroyer2 malware // Search Security: [Website]. 2022. URL: https://www.techtarget.com/searchsecurity/news/252515899/Ukraine-energy-grid-hit-by-Russian-Indestroyer2-malware (viewed on: 29.05.2025).
12. Russian Strikes Leave Millions Without Power // Dawn: [Website]. 2024. URL: https://www.dawn.com/news/1875441 (viewed on: 29.05.2025).
13. Кількість зареєстрованих кіберінцидентів у першому півріччі 2023 року зросла більше ніж удвічі // Державна служба спеціального зв'язку та захисту інформації України: [Веб-сайт]. 2023. URL: https://cip.gov.ua/ua/news/kilkist-zareyestrovanikh-kiberincidentiv-u-pershomu-pivrichchi-2023-roku-zrosla-bilshe-nizh-udvichi (дата звернення: 29.05.2025).
14. Цибка А.А. Щодо актуальних проблем системи забезпечення енергетичної безпеки України: інституційний аспект. *Науковий вісник УжНУ*. Серія: Право. 2018., Вип. 51 Т. 1. С. 70–73. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/30992.