Національні інтереси України
5(22) 2026
ISSN 3041-1793 Online
УДК 620.9:004.91:351.862(477)
https://doi.org/10.52058/3041-1793-2026-5(22)-915-931

Остапенко Ольга Павлівна кандидат технічних наук, доцент, Вінницький національний технічний університет, м. Вінниця, https://orcid.org/0000-0001-9682-9419

ЕНЕРГЕТИЧНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ВОЄННОЇ ЗАГРОЗИ: АНАЛІЗ КРИТИЧНОЇ ІНФРАСТРУКТУРИ, ОЦІНКА ВТРАТ І ПОДОЛАННЯ ВРАЗЛИВОСТЕЙ ЧЕРЕЗ ДЕЦЕНТРАЛІЗАЦІЮ І КІБЕРБЕЗПЕКУ

Анотація. Повномасштабна збройна агресія проти України показала критичний рівень вразливості національної енергетичної інфраструктури, яка історично розвивалася як централізована система з великими генерувальними та переробними вузлами. Дослідження встановило, що вразливість енергосистеми формується сукупністю факторів: надмірною централізацією виробництва електроенергії, залежністю від кількох нафтопереробних заводів, лінійною конфігурацією мереж та історичною залежністю від застарілих технологічних стандартів радянського періоду. Дослідження включає комплексний аналіз міжнародної нормативної бази, зокрема Регламентів ЄС: Cybersecurity Act (EU) 2019/881, що встановлює стандарти сертифікації продуктів та послуг; Cyber Resilience Act (EU) 2024/2847, що запроваджує горизонтальні вимоги кібербезпеки для виробів з цифровими елементами та потребує впровадження принципу "security by design"; та AI Act (EU) 2024/1689, що встановлює нормативний режим для систем штучного інтелекту, включаючи вимоги до прозорості, документації та людського контролю. Ці регламенти становлять основу для гармонізації українського законодавства у сфері енергетичної безпеки. Дослідження виокремило три основні напрями підвищення стійкості енергетичної системи: (1) децентралізацію генерації та розвиток локальних енергетичних систем на основі мікромереж та відновлюваних джерел енергії; (2) посилення фізичного захисту критичних об'єктів через інженерне укриття, резервування та просторове розосередження; (3) розбудову інтегрованого кіберзахисту з опорою на спеціалізовані галузеві Security Operation Centers, сегментацію мереж, багатофакторну автентифікацію та AI-системи для виявлення аномалій. Стаття включає рекомендації щодо створення національного центру кібербезпеки енергетики, розроблення технічних стандартів гармонізованих з ЄС, запровадження обов'язкового звітування про кіберінциденти, розвитку

ISSN 3041-1793 Online

кадрового потенціалу та залучення міжнародного фінансування (у тому числі через "Green bonds" для проектів відновлюваної енергетики). Розглядаються практичні приклади успішного впровадження у Естонії, Литві та Польщі, які змогли інвестувати в децентралізовану енергетику при дотриманні європейських стандартів. Запропоновані підходи можуть бути застосовані при плануванні реконструкції енергетичних об'єктів, формуванні регіональних стратегій стійкості та підготовці нормативних документів, що регулюють безпеку критичної інфраструктури. Наукова новизна полягає у поєднанні структурного, просторового, кібернетичного аналізу з врахуванням вимог міжнародних регламентів ЄС, що дало змогу сформувати цілісне бачення вразливості енергетичної системи під час війни та шляхів її трансформації у відповідь на сучасні виклики. Висновки мають практичне значення для органів державної влади, операторів паливно-енергетичного комплексу, аналітичних центрів та міжнародних партнерів, які розробляють програми відновлення та захисту критичної енергетичної інфраструктури в умовах тривалої воєнної загрози та європейської інтеграції України.

Ключові слова: енергетична структура, критична інфраструктура, вразливість енергосистеми, відновлення енергетики, цивільна безпека, децентралізація генерації, кібербезпека, AI Act, Cybersecurity Act, Cyber Resilience Act.

Ostapenko Olha Pavlivna Candidate of Technical Sciences, Associate Professor, Vinnytsia National Technical University, Vinnytsia, ehttps://orcid.org/0000-0001-9682-9419

ENERGY SECURITY OF UKRAINE IN THE CONDITIONS OF MILITARY THREAT: ANALYSIS OF CRITICAL INFRASTRUCTURE, ASSESSMENT OF LOSSES AND OVERCOMING VULNERABILITIES THROUGH DECENTRALIZATION AND CYBERSECURITY

Abstract. The full-scale armed aggression against Ukraine showed a critical level of vulnerability of the national energy infrastructure, which historically developed as a centralized system with large generating and processing nodes. The study found that the vulnerability of the energy system is shaped by a combination of factors: excessive centralization of electricity production, dependence on several oil refineries, linear network configuration, and historical dependence on outdated technological standards from the Soviet period. The study includes a comprehensive analysis of the international regulatory framework, in particular the EU Regulations: Cybersecurity Act (EU) 2019/881, which sets standards for the certification of products and services; Cyber Resilience Act (EU) 2024/2847, which introduces

ISSN 3041-1793 Online

horizontal cybersecurity requirements for products with digital elements and requires the implementation of the "security by design" principle; and AI Act (EU) 2024/1689, which establishes a regulatory regime for artificial intelligence systems, including requirements for transparency, documentation and human control. These regulations form the basis for harmonizing Ukrainian legislation in the field of energy security. The study identified three main areas for increasing the resilience of the energy system: (1) decentralization of generation and development of local energy systems based on microgrids and renewable energy sources; (2) strengthening the physical protection of critical facilities through engineering shelter, redundancy and spatial dispersion; (3) building integrated cyber defense based on specialized industry Security Operation Centers, network segmentation, multi-factor authentication, and AI-based anomaly detection. The article includes recommendations for establishing a national energy cybersecurity center, developing technical standards harmonized with the EU, introducing mandatory reporting of cyber incidents, developing human resources, and attracting international financing (including through "Green bonds" for renewable energy projects). Practical examples of successful implementation in Estonia, Lithuania, and Poland are considered, which were able to invest in decentralized energy while adhering to European standards. The proposed approaches can be applied in planning the reconstruction of energy facilities, forming regional resilience strategies and preparing regulatory documents regulating the security of critical infrastructure. The scientific novelty lies in the combination of structural, spatial, cybernetic analysis taking into account the requirements of international EU regulations, which made it possible to form a holistic vision of the vulnerability of the energy system during war and the ways of its transformation in response to modern challenges. The conclusions are of practical importance for state authorities, operators of the fuel and energy complex, analytical centers and international partners who develop programs for the restoration and protection of critical energy infrastructure in the conditions of a prolonged military threat and European integration of Ukraine.

Keywords: energy structure, critical infrastructure, energy system vulnerability, energy restoration, civil security, decentralization of generation, cybersecurity, AI Act, Cybersecurity Act, Cyber Resilience Act.

Постановка проблеми. Енергетична інфраструктура розглядається сучасними дослідниками як один із найважливіших компонентів національної безпеки держави [1]. Енергія є необхідною умовою функціонування всіх секторів економіки, від промислового виробництва до надання основних комунальних послуг населенню. Однак енергетичні системи також належать до найбільш вразливих секторів критичної інфраструктури, особливо в умовах збройного протистояння та в контексті зростаючих цифрових загроз.

ISSN 3041-1793 Online

Повномасштабна воєнна агресія, що розпочалася у лютому 2022 року, продемонструвала критичну залежність України від централізованої енергосистеми з великими генерувальними та переробними об'єктами. Те, що складалося як раціональне рішення у мирний час з точки зору економічної ефективності, виявилося фатальною уразливістю в умовах систематичних атак.

Істотним аспектом, що часто залишається поза увагою національних дослідників, є гармонізація українських стандартів кібербезпеки та управління енергетичною інфраструктурою з міжнародними, зокрема із стандартами Європейського Союзу. У контексті європейської інтеграції України виникає необхідність адаптації національної нормативної бази до вимог Регламентів ЄС, таких як Cybersecurity Act [2], Cyber Resilience Act [3] та AI Act [4].

Аналіз останніх досліджень і публікацій. Дослідження вразливості енергетичної інфраструктури України поступово сформували окремий міждисциплінарний напрям, у якому поєднано безпекові, правові, технологічні та просторові підходи. В українській науковій традиції питання енергетичної безпеки розглядалися переважно крізь призму економічної стабільності та диверсифікації ресурсів. Однак, починаючи з 2014 року, і особливо після 2022 року, акценти змістилися на аналіз військових загроз, системних кібератак і фізичних руйнувань критичних об'єктів. Зокрема, вагоме значення мають дослідження Л. А. Арсеновича [5], присвячені питанням захисту критичних об’єктів у загальній системі національної безпеки України. Питання стратегічного планування та розробки фундаментальних засад політики захисту було ґрунтовно висвітлено у працях Д. С. Бірюкова [6], тоді як специфіку реалізації сучасної державної політики в цій сфері досліджено Я. О. Страхницьким [7]. Крім того, комплексний аналіз нормативно-правових і організаційних аспектів забезпечення безпеки інфраструктурних об’єктів представлений праці С. І. Мельника, П. Я. Пригунова та В. І. Франчука [8]. Попри наявність ґрунтовних напрацювань, динамічна трансформація вітчизняного законодавчого поля актуалізує потребу в подальшому комплексному вивченні механізмів державної політики у сфері захисту критичної інфраструктури з урахуванням новітніх правових реалій. У межах дослідження Б. В. Богдана [9] було здійснено критичний аналіз базових нормативно-правових актів, що регламентують захист критичної інфраструктури. В дослідженні [9] визначено, що кінцевою метою реалізації державної політики на сучасному етапі є розбудова цілісної та функціонально спроможної національної системи захисту критичної інфраструктури, здатної оперативно реагувати на виклики воєнного часу. Метою дослідження С. П. Берсименка [1] було встановлення факторів, що зумовлюють уразливість критичних енергетичних вузлів України до ракетно-дронових та кібернетичних атак, а також обґрунтування напрямів підвищення їхньої стійкості.

ISSN 3041-1793 Online

Попри значний обсяг наукових напрацювань, залишаються "білі плями", що потребують подальшого опрацювання. Недостатньо дослідженим є розроблення комплексних моделей оцінки стійкості, здатних одночасно враховувати ракетно-дронові атаки, кібератаки та соціально-економічні чинники. Більшість наявних досліджень фокусуються або на фізичних загрозах, або на кібератаках окремо, без врахування їхнього взаємного впливу. Низка досліджень демонструє суперечливі висновки щодо ефективності децентралізації. Частина авторів розглядає децентралізацію як ключовий інструмент стійкості, тоді як інші наголошують на високих видатках та складності інтеграції розподілених систем у традиційну централізовану ОЕС. Недостатньо дослідженою залишається проблема синхронізації роботи різних секторів енергетики (електроенергія, газ, нафта) у умовах тривалого дефіциту потужностей та постійних атак. Такі дослідження мають міжсекторальний характер і потребують координації між різними експертами.

Поки що недостатньо розвинуто питання практичного впровадження стандартів ЄС (Cybersecurity Act, Cyber Resilience Act, AI Act) в контексті української енергетичної інфраструктури. Необхідні детальні дослідження щодо того, як адаптувати європейські стандарти до реалій воєнної України та яким чином найбільш ефективно розподілити видатки.

Слабко дослідженою залишається проблема розвитку кадрового потенціалу для роботи з новими системами кібербезпеки та управління нововведеннями. Україна відчуває гострий дефіцит спеціалістів, які глибоко розуміють як енергетику, так і кібербезпеку, а також мають знання міжнародних стандартів.

Аналіз стану дослідження питань енергетичної безпеки України показує, що: українські дослідження добре охоплюють правові, просторові та економічні аспекти проблеми; міжнародні дослідження демонструють глобальний характер проблеми кібератак на енергетичну інфраструктуру; європейські регламенти (Cybersecurity Act, Cyber Resilience Act, AI Act) встановлюють нову парадигму нормативного регулювання, яка має бути врахована при плануванні відновлення України; залишаються істотні прогалини щодо комплексного аналізу вразливостей та практичної адаптації європейських стандартів до українських умов. Пропоноване дослідження спрямоване на подолання цих прогалин та надання комплексного, науково обґрунтованого бачення проблеми енергетичної безпеки України у сучасному глобальному контексті.

Мета статті полягає в комплексному аналізі структури енергетичної системи України, дослідженні масштабів та характеру втрат енергетичної інфраструктури внаслідок воєнних дій, а також у розгляді міжнародної нормативної бази та практичних напрямів відновлення та підвищення стійкості системи в контексті вимог міжнародного права та стандартів безпеки.

ISSN 3041-1793 Online

Дане дослідження заповнює вищевказані "білі плями" шляхом:

1. Комплексного аналізу структури енергетичної системи України з врахуванням як фізичних, так і кібернетичних вразливостей;
2. Синтезу міжнародної практики щодо впровадження Cybersecurity Act, Cyber Resilience Act та AI Act з українськими реаліями;
3. Розроблення практичних рекомендацій щодо децентралізації генерації, посилення фізичного захисту та розбудови кібербезпеки;
4. Розглядання інституційних аспектів і необхідності створення національного центру кібербезпеки енергетики;
5. Аналізу економічних аспектів відновлення та доступних джерел фінансування, включаючи можливості залучення "Green bonds" та міжнародної допомоги;
6. Вивчення досвіду європейських країн (Естонія, Литва, Польща) у запровадженні децентралізованої енергетики при дотриманні європейських стандартів.

Пропоноване дослідження має практичне значення для органів державної влади, операторів паливно-енергетичного комплексу та аналітичних центрів, які розробляють програми відновлення та захисту інфраструктури в контексті як воєнної загрози, так і європейської інтеграції України.

Виклад основного матеріалу. Енергетична система України, як вона сформувалася до 2022 року, характеризувалася чітко виразною централізацією виробництва електроенергії. За даними Всеукраїнської енергетичної асамблеї [10], у 2021 році розподіл за типами електростанцій мав такий вигляд: атомні електростанції (4 об'єкти) забезпечували понад 55% виробництва електроенергії; теплові електростанції та теплоелектроцентралі (17 ТЕС та 47 ТЕЦ) генерували близько 30%; гідроелектростанції та гідроакумулювальні станції (9 ГЕС та 4 ГАЕС) становили близько 7%; відновлювані джерела енергії та блокстанції забезпечували близько 8% [1]. Така конфігурація демонструє екстремальну концентрацію виробництва у кількох великих об'єктах. Це означало, що вихід з ладу одного або двох великих вузлів призводить до системних порушень у роботі всієї мережі. На практиці, як показало дослідження, навіть короткочасне пошкодження однієї атомної електростанції або кількох теплових станцій викликає розповсюджені дефіцити електроенергії по всій країні.

Поряд з генерацією важливу роль відігравали 103 високовольтні підстанції класу напруги 220–750 кВ, які забезпечували зв'язок між основними центрами виробництва та споживання електроенергії. Ці об'єкти також становили вразливі точки, оскільки їхнє пошкодження порушувало передачу енергії навіть за умови функціонування генерувальних потужностей.

ISSN 3041-1793 Online

Газотранспортна система України базувалася на 73 компресорних станціях та 1473 газорозподільчих станціях [1]. Система була спрямована на транспортування газу від джерел видобутку та імпорту до центрів споживання. Однак вона мала низку вразливостей: лінійна конфігурація (основні магістралі прокладалися по єдиному маршруту, що робило їх чутливими до локальних пошкоджень); залежність від контрольних точок (несправність кількох ключових компресорних станцій могла паралізувати постачання на цілих регіонів); енергоємність (сама газотранспортна система залежала від електроенергії для функціонування компресорного обладнання, що створювало взаємозалежність з електроенергетичною системою).

Динаміка валового видобутку природного газу у 2016–2021 роках відображала поступове зниження внутрішнього газовидобутку [1]. Ця тенденція формувала критичну вразливість: у разі порушення логістики імпорту або виведення з ладу критичних видобувних об'єктів держава не могла оперативно компенсувати дефіцит виключно внутрішнім видобутком.

Фізичний вимір загроз енергетичній інфраструктурі різко активізувався восени 2022 року. Найбільш вразливими виявилися: великі генерувальні об'єкти (атомні електростанції мали найвищу критичність, оскільки забезпечували понад половину електроенергії); теплові електростанції (особливо станції, побудовані близько населених пунктів та змушені розташуватися у передбачуваних місцях); розподільчі підстанції (великі трансформаторні комплекси, ураження яких паралізувало енергопередачу в регіонах); магістральні мережі (лінійна організація електромереж робила їх чутливими до розосереджених атак). Комбінування фізичних ударів з кібератаками створювало багатофакторний тиск, до якого система була частково не готова. Навіть успішний захист від однієї складової атаки залишав енергетичні об'єкти вразливими до іншої.

Централізована структура енергосистеми, що сформувалася у радянський період, є однією з ключових причин вразливості. Проектування великих генерувальних комплексів виконувалося без урахування можливості систематичних атак на енергетичну інфраструктуру. Коефіцієнт концентрації генерації був екстремально високим. Якщо розглядати розподіл по чотирьох типах генерації, то кожен тип утримував суттєву частину генеруючих потужностей. Це означало, що навіть поточні ремонти одного об'єкта викликали дефіцити, а вихід з ладу кількох об'єктів водночас міг привести до масштабних блекаутів. Значна частина генерувальних об'єктів розташовувалася у передбачуваних місцях, близько до великих центрів споживання енергії. Хоча це було раціональним з точки зору економічної ефективності передачі енергії, але робило об'єкти легкими цілями для ракетно-дронових ударів.

ISSN 3041-1793 Online

Крім того, розташування об'єктів часто не враховувало рівень воєнних ризиків. Дослідження показало, що значна частина українських енергетичних вузлів мала високий ступінь експозиції до воєнних загроз, що ускладнювало можливості адаптації та захисту.

Значна частина енергетичної інфраструктури базувалася на радянських стандартах проєктування та управління, які не передбачали сучасних засобів захисту від кібератак. Системи управління часто були з низькою надмірністю та без резервних каналів управління.

Європейське агентство з кібербезпеки (ENISA – European Union Agency for Cybersecurity) відіграє ключову роль у розробленні та впровадженні загальноєвропейських стандартів кібербезпеки. Регламент (EU) 2019/881[2], прийнятий Європейським парламентом та Радою від 17 квітня 2019 року (Cybersecurity Act), встановив нову нормативну базу для сертифікації кіберзахисту виробів та послуг.

Регламент [2] визначає три основні функції ENISA:

1. Розроблення стандартів сертифікації – ENISA розробляє схеми сертифікації, що встановлюють мінімальні вимоги до рівня безпеки для різних категорій продуктів та послуг;
2. Технічна експертиза – агентство надає технічне консультування органам ЄС щодо питань кібербезпеки;
3. Сприяння обміну інформацією – ENISA координує обмін інформацією про кіберзагрози та інциденти безпеки на рівні ЄС.

Для енергетичної інфраструктури це має принципове значення. Cybersecurity Act передбачає обов'язкову сертифікацію критичних компонентів енергетичних систем, що забезпечує мінімальний рівень гарантій щодо їхньої стійкості до кібератак. Це особливо важливо в контексті використання систем управління на основі промислового інтернету речей та SCADA-систем, які часто є вразливими до інциденів безпеки.

Регламент (EU) 2024/2847 [3], прийнятий Європейським парламентом та Радою від 23 жовтня 2024 року (Cyber Resilience Act), встановлює горизонтальні вимоги до кібербезпеки для виробів з цифровими елементами. Це регламентування застосовується до практично всіх пристроїв, які містять програмне забезпечення або можуть бути оновлені через інтернет.

Для енергетичної інфраструктури Cyber Resilience Act має наступні наслідки.

Виробники виробів з цифровими елементами повинні [3]:

- проводити оцінку ризиків – здійснювати систематичну оцінку потенційних кіберзагроз для кожного виробу на всіх етапах його життєвого циклу;
- впроваджувати міри кібербезпеки – проектувати та розробляти вироби з врахуванням вимог кібербезпеки з самого початку (принцип "security by design");

ISSN 3041-1793 Online

• забезпечувати тестування на уразливості – проводити комплексне тестування на виявлення вразливостей, включаючи пентести та фаззинг;

• здійснювати управління вразливостями – впровадити процеси виявлення, документування та вирішення вразливостей протягом визначеного періоду.

Ці вимоги мають бути виконані при розробленні критичних компонентів енергетичної інфраструктури, таких як системи управління підстанціями, контролери автоматики та пристрої інтернету речей для моніторингу енергомереж.

Cyber Resilience Act встановлює суворі вимоги до звітування про кіберінциденти [3]:

• виробники та оператори критичної інфраструктури повинні повідомляти про серйозні інциденти безпеки в установлені терміни;

• інформація про інциденти має включати деталі про природу атаки, методи, які були використані, та заходи, які були приняті для мінімізації шкоди;

• ця інформація має бути доступна органам, що відповідають за безпеку критичної інфраструктури.

Регламент (EU) 2024/1689 [4] про штучний інтелект (AI Act), прийнятий Європейським парламентом та Радою від 13 червня 2024 року, встановлює перший у світі комплексний нормативно-правовий режим для застосування штучного інтелекту. Хоча основна мета AI Act полягає в захисті прав людини та безпеки, він також містить конкретні вимоги щодо використання AI у критичних сферах, включаючи енергетику.

AI Act встановлює чотирирівневу класифікацію систем штучного інтелекту за рівнем ризику [4]:

1. Мінімальний ризик – системи, що не створюють значного ризику для безпеки або прав людини;
2. Обмежений ризик – системи, які вимагають певного рівня прозорості та інформування користувачів;
3. Високий ризик – системи, які можуть негативно впливати на здоров'я, безпеку або основні права людей;
4. Неприйнятний ризик – системи, заборонені на території ЄС.

Для енергетичної інфраструктури системи AI використовуються для: прогнозування попиту на енергію; оптимізації розподілу електроенергії; виявлення аномалій у роботі критичних об'єктів; управлінні розподіленою генерацією. В енергетичній інфраструктурі системи AI часто класифікуються як системи високого ступеня ризику, оскільки помилки у їхній роботі можуть привести до значних порушень у постачанні енергії та створити загрозу для безпеки людей.

ISSN 3041-1793 Online

Системи AI високого ризику повинні відповідати наступним вимогам [4]:

- документація та реєстрація – розробники повинні вести детальну документацію про розроблення, тестування та розгортання систем;
- людський нагляд – людина повинна мати можливість втрутитися та переважити рішення системи AI у критичних ситуаціях;
- прозорість та пояснюваність – користувачі та регулятори повинні мати можливість зрозуміти, як система приймає рішення;
- гарантія якості даних – дані, які використовуються для навчання та експлуатації системи, повинні бути якісними та репрезентативними;
- мониторинг та звітування – розробники повинні безперервно моніторити роботу системи та звітувати про виявлені проблеми.

Ці вимоги мають значні наслідки для організації розробки та впровадження AI-системи у енергетичних мережах. Система управління розподіленої генерацією, яка використовує AI для оптимізації потоків енергії, має задовольняти всі ці вимоги, що вимагає значних інвестицій в документацію, тестування та аудит.

Україна знаходиться у процесі адаптації свого законодавства до стандартів ЄС у рамках євроінтеграційного процесу. Однак цей процес стикається з низкою викликів:

1. Ресурсні обмеження – у воєнний час держава має обмежені ресурси для розроблення нового законодавства та створення інституцій для його моніторингу;
2. Технологічне відставання – багато українських компаній у сфері енергетики використовують застарілі технології, які складно привести до стандартів кібербезпеки ЄС;
3. Інституційні слабкості – Україна не має аналога ENISA з повною функціональністю, що ускладнює проведення сертифікацій продуктів та послуг;
4. Кадровий дефіцит – недостатньо спеціалістів, які глибоко розуміють як енергетику, так і кібербезпеку.

Перший та найважливіший напрям відновлення енергетичної системи полягає в її децентралізації. Замість повної залежності від великих генерувальних центрів, система має розвиватися у напрямі розподіленої генерації. Цей підхід узгоджується з енергетичною стратегією ЄС, яка спрямована на перехід до низьковуглецевої економіки та підвищення безпеки енергопостачання. Це включає: розвиток мікромереж у населених пунктах; запровадження малих газових станцій з розосередженим розташуванням; максимально активне використання відновлюваних джерел енергії – сонячних та вітрових установок, які можуть бути розміщені по всій території держави; впровадження систем накопичення енергії (батарей), що дозволяють згладжувати

ISSN 3041-1793 Online

коливання в генерації та споживанні. Економічна раціональність децентралізованої енергетики доведена численними дослідженнями. Хоча початкові інвестиції можуть бути вищими, довгострокові видатки на обслуговування та захист децентралізованої системи значно менші.

Із точки зору Cyber Resilience Act децентралізована система енергетики має суттєву перевагу: розподіленість означає, що одиниця помилки або атаки не може паралізувати всю систему [3]. Крім того, малі генеруючі об'єкти простіше розробляти з урахуванням вимог "security by design", передбачених AI Act та Cybersecurity Act [2, 4].

Другий напрям стосується посилення фізичного захисту найбільш критичних об'єктів енергетичної системи. Це включає:

1. Інженерне укриття – розташування критичних компонентів під захистом залізобетонних або земляних укриттів;
2. Резервування критичних ліній – створення альтернативних маршрутів передачі електроенергії, щоб пошкодження однієї лінії не паралізувало постачання;
3. Розосередження складів пального – замість кількох великих сховищ, розробка мережі середніх та малих сховищ, розміщених у різних місцях;
4. Мобільні резервні генератори – готовність швидко розгортати генеруючі потужності в місцях пошкоджень.

У контексті мінімізації впливу кібератак фізичний захист має доповнюватися мікросегментацією критичних систем управління. Це означає, що управління окремих підстанцій не повинне бути об'єднане в єдину мережу, як це часто буває у централізованих системах. Замість цього кожна підстанція або невелика група підстанцій повинні мати автономну систему управління, яка може функціонувати навіть при втраті зв'язку з центральною диспетчерською.

Третій напрям спрямований на захист енергетичних систем від кібератак. В контексті вимог Cybersecurity Act [2]. та Cyber Resilience Act [3], це включає:

1. Розбудову галузевих Security Operation Centers (SOC) – спеціалізованих центрів, які будуть моніторити кіберзагрози у реальному часі та відповідати на інциденти в установлені терміни, як вимагається Cyber Resilience Act;
2. Сегментація мереж – розділення інформаційних систем на кілька ізольованих сегментів, щоб компрометація одного не призвела до компрометації всієї системи. Ця практика узгоджується з вимогою "security by design" у Cybersecurity Act;
3. Багатофакторна автентифікація – впровадження сучасних систем контролю доступу, включаючи біометричні методи та криптографічні ключі;
4. AI-системи для виявлення аномалій – використання машинного навчання для виявлення незвичайної активності в енергомережах. Такі

ISSN 3041-1793 Online

системи повинні задовольняти вимоги AI Act щодо прозорості, документації та людського нагляду;

5. Спільні навчання з операторами – розвиток свідомості про кіберзагрози та навичок реагування на інциденти. Це включає регулярні навчання з симуляціями кібератак.

Одним з найперспективніших напрямів підвищення стійкості енергетичної інфраструктури є застосування штучного інтелекту для виявлення та запобігання кібератакам. AI-системи можуть: проводити аналіз поведінки (вивчати нормальні картини роботи енергомереж і виявляти відхилення, які можуть вказувати на атаку); прогнозувати атаки (на основі даних про попередні атаки й тренди передбачати можливі майбутні загрози); автоматизувати реагування (швидко відреагувати на виявлені загрози, ізолюючи компрометовані системи).

Однак впровадження таких систем повинно виконуватися у повній відповідності до вимог AI Act [4]. Зокрема: розробник системи повинен вести детальну документацію про те, як система розробляється та тестується; система повинна бути прозорою – оператор енергосистеми повинен розуміти, чому система вирішила ізолювати той чи інший сегмент мережі; людина (оператор) завжди повинна мати можливість переважити рішення системи у критичних ситуаціях; дані, які використовуються для навчання системи, повинні бути якісними та відповідати вимогам Регламенту про захист даних (GDPR) [11].

Однак важливо зазначити, що у контексті європейської інтеграції та адаптації до стандартів Cybersecurity Act та Cyber Resilience Act додаткові витрати на впровадження сучасних систем кібербезпеки можуть становити 10–15% від загальної вартості проектів. Це включає витрати на: проведення оцінок уразливості та сертифікаційних перевірок; встановлення обладнання для моніторингу безпеки; навчання персоналу з питань кібербезпеки; розроблення та впровадження нових нормативних документів.

Вартість відновлення енергетичної інфраструктури України є надзвичайно високою. Фінансування відновлення має йти з кількох джерел:

1. Державний бюджет – визначена частина видатків на оборону та реконструкцію;

2. Міжнародна технічна допомога – гранти та позики від міжнародних фінансових організацій, включаючи Європейський банк реконструкції та розвитку (EBRD) та Міжнародний банк реконструкції та розвитку (IBRD);

3. Приватні інвестиції – залучення приватного капіталу у децентралізовані проекти генерації. Дані проекти можуть отримувати податкові пільги на основі Директив ЄС про енергетику;

4. Фонди відновлення – міжнародні фонди, створені для постконфліктної реконструкції, такі як Фонд відновлення України;

ISSN 3041-1793 Online

5. "Green bonds" – зелені облігації, які інвестори готові купувати для проектів, які мають позитивний вплив на навколишнє середовище та кліматичні цілі.

Європейський Союз активно сприяє використанню "Green bonds" для проектів у країнах, що розвиваються, включаючи Україну. Проекти енергетичної інфраструктури на основі відновлюваних джерел енергії можуть залучати значні обсяги таких інвестицій.

Гармонізація українських стандартів з європейськими стандартами Cybersecurity Act та Cyber Resilience Act може здаватися додатковою бюрократичною вимогою. Однак насправді це відкриває нові економічні можливості, а саме:

1. Вихід на європейський ринок – українські виробники енергетичного обладнання, які отримають сертифікацію за стандартами ЄС, зможуть експортувати свої продукти на весь європейський ринок;
2. Залучення іноземних інвесторів – компанії, які розвивають проекти на основі стандартів ЄС, приваблять більше іноземних інвестицій;
3. Підвищення якості та стійкості – дотримання міжнародних стандартів гарантує, що розроблювані об'єкти будуть мати вищу якість та стійкість до сучасних загроз.

Успішне відновлення енергетичної інфраструктури залежить не лише від технічних рішень, але й від інституційних та законодавчих змін. На основі аналізу вимог Cybersecurity Act, Cyber Resilience Act та AI Act можна запропонувати наступні інституційні реформи.

Необхідно створити спеціалізовану державну установу, яка буде відповідати за координацію питань кібербезпеки у енергетичному секторі. Ця установа повинна мати наступні функції:

- розроблення стандартів – розробка технічних та нормативних вимог для операторів енергетики;
- сертифікація та аудит – проведення сертифікаційних перевірок продуктів та послуг, а також аудиту операторів;
- реагування на інциденти – координація реагування на серйозні кібер-інциденти, включаючи обмін інформацією з міжнародними партнерами;
- дослідження та розвиток – фінансування досліджень у галузі кібербезпеки та розроблення нових методів захисту.

Ця установа повинна мати статус, подібний до ENISA в ЄС, з достатньою політичною та фінансовою незалежністю для ефективної діяльності.

Потребує також розроблення детального плану гармонізації українського законодавства з вимогами ЄС. План повинен включати:

- фази впровадження – поступові етапи впровадження нових вимог, враховуючи ресурсні обмеження у воєнний час;

ISSN 3041-1793 Online

• перехідні положення – часові рамки, протягом яких оператори мають привести свої системи до нових вимог;

• фінансову підтримку – державні та міжнародні гранти для допомоги операторам у впровадженні нових вимог;

• навчання та капацитет-білдинг – програми підготовки кадрів для роботи з новими системами.

Для того щоб розробити ефективну стратегію для України, варто розглянути досвід європейських країн, які також стикаються з викликами енергетичної безпеки в контексті гібридної загрози.

Приклад 1: Естонія – ця країна стала піонером у використанні цифрових технологій для управління критичною інфраструктурою. У своїй енергетичній системі Естонія широко використовує AI-системи для моніторингу та оптимізації, але при цьому дотримується найвищих стандартів прозорості та контролю, передбачених AI Act.

Приклад 2: Литва активно інвестує в децентралізовану генерацію та відновлювані джерела енергії, при цьому впроваджуючи сучасні системи кібербезпеки відповідно до стандартів ЄС.

Приклад 3: Польща – ця країна розвиває гібридний підхід до енергетичної безпеки, поєднуючи традиційні джерела енергії з відновлюваними. Польщі вдалося залучити значні інвестиції Євросоюзу на основі своєї відповідності європейським стандартам кібербезпеки.

Спільною рисою всіх цих країн є твердий намір дотримуватися європейських стандартів, незважаючи на вищі початкові видатки. Це дозволило їм отримати доступ до технологій, інвестицій та знань, що сприяло їхній енергетичній безпеці.

Висновки. Дослідження структури, втрат та шляхів відновлення енергетичної інфраструктури України, розглянуте через призму міжнародних стандартів та вимог ЄС, дозволяє зробити такі висновки:

1. Централізована структура енергосистеми сформувала критичні вразливості, які були виявлені в умовах воєнного стану. Однак, ці вразливості не є невідворотними – децентралізація та розвиток розподіленої генерації можуть принципово змінити ситуацію.

2. Масштаби втрат енергетичної інфраструктури в 2022–2025 роках демонструють використання стратегії системного руйнування енергосистеми. Однак той факт, що система частково зберегла функціональність навіть при масових руйнуваннях, показує потенціал для відновлення.

3. Міжнародні стандарти, особливо Cybersecurity Act, Cyber Resilience Act та AI Act, встановлюють чіткі рамки для розроблення стійкої енергетичної інфраструктури. Гармонізація українського законодавства з цими стандартами є не просто нормативною вимогою, але й стратегічною можливістю для залучення інвестицій та технологій.

ISSN 3041-1793 Online

4. Децентралізація генерації – це не лише технічне рішення, але й стратегічний вибір, який робить систему стійкою як до військових атак, так і до кібератак. Розповсюджена генерація на основі відновлюваних джерел енергії узгоджується як з європейськими стандартами, так і з довгостроковими цілями України щодо енергетичної незалежності.

5. AI-системи для кібербезпеки мають величезний потенціал для підвищення стійкості енергетичної системи, але їхнє впровадження повинно виконуватися з дотриманням вимог AI Act щодо прозорості, документації та людського контролю.

6. Інституційні реформи є критично важливими. Створення національного центру кібербезпеки енергетики та розроблення плану гармонізації законодавства повинні розпочатися якнайшвидше.

7. Фінансування відновлення є можливим через комбінацію державних видатків, міжнародної допомоги та приватних інвестицій, особливо у формі "Green bonds" для проектів відновлюваної енергетики.

Трансформація енергетичної системи України у відповідь на виклики 2022–2025 років та у контексті європейської інтеграції є складною, але здійсненною. Вона вимагає як технічних інновацій, так і політичної волі. Однак результат цих зусиль буде не лише енергетично стійка система, яка стане на рівень із європейськими стандартами, а й система, яка буде прикладом для інших країн, що стикаються з подібними загрозами.

Література:

1. Берсименко, С. П. (2026). Вразливість енергетичної інфраструктури України до атак та руйнувань. *Національні інтереси України*, 2(19), 42–59.

2. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15–69.

3. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act), OJ L 2024/2847, 11.12.2024.

4. European Data Protection Supervisor, (2025) AI Act Regulation (EU) 2024/1689 : Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). Publications Office of the European Union. https://data.europa.eu/doi/10.2804/4225375.

5. Арсенович Л. А. (2024). Парадигма захисту критичної інфраструктури в системі національної безпеки України. *Державне управління: удосконалення та розвиток*. № 8. DOI: http://doi.org/10.32702/2307-2156.2024.8.7.

6. Бірюков Д. С. (2015). Захист критичної інфраструктури в Україні: від наукового осмислення до розробки засад політики. *Науково-інформаційний вісник Академії національної безпеки*. Випуск 3-4 (7-8). С. 155-170.

ISSN 3041-1793 Online

7. Страхніцький Я. О. (2023). Особливості сучасної державної політики у сфері захисту критичної інфраструктури в умовах війни в Україні. *Modernization of the system of public management and administration in Ukraine : the experience of the Republic of Latvia : Scientific monograph*. Riga. Latvia : «Baltija Publishing». С. 115-142. DOI: https://doi.org/10.30525/978-9934-26-279-1-5.

8. Франчук В. І., Пригунов П. Я., Мельник С. І. (2021). Безпека об'єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. *Соціально-правові студії*. Випуск 3 (13). С. 142-148. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3984/1/19.pdf.

9. Богдан Б. В. (2025). Державна політика у сфері захисту критичної інфраструктури під час дії воєнного стану. *Юридичний науковий електронний журнал*. № 1. С. 828 – 830.

10. Всеукраїнська енергетична асамблея (2022). *Виробництво електроенергії в Україні у 2021 році*. URL: https://uaea.com.ua/news/pek-news/power-generation-202112.html.

11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 1–88 (2016). europa.eu.

References:

1. Bersymenko, S. P. (2026). Vrazlyvist enerhetychnoi infrastruktury Ukrainy do atak ta ruinuvan. Natsionalni interesy Ukrainy, 2(19), 42–59. [in Ukrainian]

2. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15–69.

3. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act), OJ L 2024/2847, 11.12.2024.

4. European Data Protection Supervisor, (2025) AI Act Regulation (EU) 2024/1689 : Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). Publications Office of the European Union. https://data.europa.eu/doi/10.2804/4225375.

5. Arsenovych L. A. (2024). Paradyhma zakhystu krytychnoi infrastruktury v systemi natsionalnoi bezpeky Ukrainy. Derzhavne upravlinnia: udoskonalennia ta rozvytok. № 8. DOI: http://doi.org/10.32702/2307-2156.2024.8.7. [in Ukrainian]

6. Biriukov D. S. (2015). Zakhyst krytychnoi infrastruktury v Ukraini: vid naukovoho osmyslennia do rozrobky zasad polityky. Naukovo-informatsiinyi visnyk Akademii natsionalnoi bezpeky. Vypusk 3-4 (7-8). S. 155-170. [in Ukrainian]

7. Strakhnitskyi Ya. O. (2023). Osoblyvosti suchasnoi derzhavnoi polityky u sferi zakhystu krytychnoi infrastruktury v umovakh viiny v Ukraini. Modernization of the system of public management and administration in Ukraine : the experience of the Republic of Latvia : Scientific monograph. Riga. Latvia : «Baltija Publishing». S. 115-142. DOI: https://doi.org/10.30525/978-9934-26-279-1-5. [in Ukrainian]

ISSN 3041-1793 Online

8. Franchuk V. I., Pryhunov P. Ya., Melnyk S. I. (2021). Bezpeka obiektiv krytychnoi infrastruktury v Ukraini: orhanizatsiino-normatyvni problemy ta pidkhody. Sotsialno-pravovi studii. Vypusk 3 (13). S. 142-148. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3984/1/19.pdf. [in Ukrainian]

9. Bohdan B. V. (2025). Derzhavna polityka u sferi zakhystu krytychnoi infrastruktury pid chas dii voiennoho stanu. Yurydychnyi naukovyi elektronnyi zhurnal. № 1. S. 828 – 830. [in Ukrainian]

10. Vseukrainska enerhetychna asambleia (2022). Vyrobnytstvo elektroenerhii v Ukraini u 2021 rotsi. URL: https://uaea.com.ua/news/pek-news/power-generation-202112.html. [in Ukrainian]

11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 1–88 (2016). europa.eu.

Дата першого надходження статті до видання: 25.04.2026
Дата прийняття статті до друку після рецензування: 09.05.2026