

ІННОВАЦІЙНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ БЕЗПЕКИ ТА СТІЙКОСТІ ЕНЕРГЕТИЧНОЇ СИСТЕМИ УКРАЇНИ

Коваль Яна Сергіївна

*кандидат наук з державного управління, доцент,
доцент кафедри міжнародного менеджменту,
Державний торговельно-економічний університет
ORCID: <https://orcid.org/0000-0001-6578-2996>*

Енергетична система України сьогодні перебуває під подвійним тиском – необхідністю цифрової модернізації та зростаючими загрозами в кіберпросторі. Постійні кібератаки, спрямовані на критичну інфраструктуру, а також виклики, пов'язані з воєнними діями, актуалізують потребу у впровадженні інноваційних підходів до захисту енергетичного сектору. Забезпечення цифрової безпеки та стійкості енергосистеми є стратегічним завданням, адже від її надійності залежить безперервність економічних процесів, обороноздатність держави та якість життя населення.

У цьому контексті особливої актуальності набуває пошук інноваційних підходів до забезпечення цифрової безпеки та стійкості енергосистеми. Йдеться не лише про модернізацію технічних засобів захисту, але й про створення комплексної багаторівневої архітектури кіберстійкості, що поєднує технологічні рішення (штучний інтелект, блокчейн, хмарні обчислення), управлінські інструменти (ризик-менеджмент, сценарне планування) та нормативно-правові механізми. Ключовим завданням стає інтеграція цифрових інновацій із системою стратегічного управління енергетичною безпекою, що забезпечить здатність енергетичного сектору протистояти кібератакам, швидко відновлюватися після інцидентів і гарантувати безперебійне енергопостачання [1].

Основна проблема полягає у необхідності поєднання цифрової трансформації з формуванням кіберстійкості енергетичної інфраструктури України, що передбачає розробку та впровадження інноваційних рішень, здатних забезпечити безпеку та стабільність функціонування енергосистеми навіть в умовах кризових викликів.

Серед ключових інноваційних підходів до забезпечення цифрової безпеки енергетичної системи України доцільно виділити [2]:

1. Використання штучного інтелекту та машинного навчання для проактивного виявлення та нейтралізації загроз у режимі реального часу,

що дозволяє оперативно реагувати на аномалії та запобігати масштабним кібератакам.

2. Запровадження концепції Zero Trust Architecture, що передбачає постійну верифікацію доступу до систем незалежно від рівня користувача чи пристрою, мінімізуючи ризики внутрішніх та зовнішніх загроз.

3. Застосування технологій блокчейн для захисту критично важливих транзакцій та підвищення прозорості управління енергетичними процесами.

4. Інтеграція хмарних платформ та edge-computing для децентралізації управління, підвищення гнучкості та швидкого відновлення після інцидентів.

5. Розвиток системи кібер-симуляцій та цифрових двійників енергетичної інфраструктури для прогнозування наслідків атак і тестування ефективності різних сценаріїв захисту.

6. Створення кіберстійких центрів обробки даних (Cyber Resilient Data Centers), які здатні працювати навіть в умовах фізичного чи кібернетичного ураження.

7. Формування культури кібербезпеки через систематичне навчання персоналу та впровадження інноваційних методик кібергігієни на всіх рівнях управління.

Застосування цих підходів дозволяє сформувати багаторівневу систему захисту, яка базується не лише на пасивному протистоянні загрозам, але й на активній адаптації та відновлюваності. Таким чином, інноваційні технології та методології стають фундаментом нової парадигми забезпечення цифрової безпеки енергетичної інфраструктури України.

Для ефективного протистояння сучасним загрозам доцільним є впровадження багаторівневої моделі кіберстійкості, яка інтегрує інноваційні підходи до цифрової безпеки. Доцільно запропонувати модель з п'яти взаємопов'язаних рівнів [3]:

1. Технологічний рівень (базовий захист):

- впровадження архітектури Zero Trust;
- використання блокчейн-рішень для захисту транзакцій;
- застосування цифрових двійників для прогнозування сценаріїв атак;
- створення кіберстійких центрів обробки даних.

2. Аналітичний рівень (проактивне виявлення загроз):

- застосування штучного інтелекту та машинного навчання для моніторингу аномалій;
- використання Big Data та predictive analytics для прогнозування ймовірності атак;
- автоматизація інцидент-менеджменту на основі алгоритмів самонавчання.

3. Організаційний рівень (управління ризиками)
 - впровадження системи cyber risk management;
 - розробка протоколів швидкого відновлення після інцидентів (resilience planning);
 - формування багаторівневої системи реагування на кризові ситуації.
4. Людський рівень (кадрова кіберстійкість):
 - систематичне навчання персоналу принципам кібергігієни;
 - використання симуляцій та кіберполігонів для відпрацювання дій у кризових умовах;
 - формування культури кібербезпеки на рівні держави та енергетичних підприємств.
5. Інституційно-правовий рівень (стратегічна стійкість):
 - гармонізація українського законодавства з європейськими стандартами кібербезпеки (NIS2, GDPR тощо);
 - створення державно-приватних партнерств у сфері кіберзахисту енергетики;
 - залучення міжнародного досвіду та інтеграція у глобальні системи кіберспостереження.

Дана модель формує цілісну архітектуру кіберстійкості, де інноваційні технології поєднуються з управлінськими та правовими механізмами. Її впровадження дозволить підвищити рівень цифрової безпеки енергетичної системи України, забезпечити безперервність її функціонування та зміцнити стратегічну енергетичну безпеку держави в умовах воєнних і гібридних загроз.

Підсумовуючи, варто відмітити, що забезпечення цифрової безпеки та кіберстійкості енергетичної системи України є стратегічним завданням національної безпеки, особливо в умовах воєнних і гібридних загроз. Проведений аналіз свідчить, що традиційні підходи до захисту вже не відповідають сучасним викликам, а отже, потребують інтеграції з інноваційними рішеннями. Запропонована багаторівнева модель кіберстійкості, що включає технологічний, аналітичний, організаційний, людський та інституційно-правовий рівні, створює комплексну архітектуру захисту, здатну адаптуватися до швидкозмінних умов та відновлювати функціонування системи після інцидентів.

Використання штучного інтелекту, блокчейну, цифрових двійників, архітектури Zero Trust та інших інноваційних рішень у поєднанні з розвитком культури кібербезпеки і державно-приватним партнерством забезпечує стійкість енергетичної інфраструктури. Таким чином, інноваційні підходи не лише підвищують ефективність цифрового захисту, але й формують основу для стратегічної енергетичної безпеки України в умовах підвищених ризиків.

Список використаних джерел:

1. Кравець І. В. Енергетична дипломатія як інструмент протидії гібридним загрозам. *Державне будівництво і місцеве самоврядування*. 2023. № 1. С. 58–67. DOI: <https://doi.org/10.32702/dbms2023.1.58>
2. Коваль, Я. Державне управління енергетичною сферою в умовах гібридної війни: стратегічні підходи та інструменти. *Таврійський науковий вісник. Серія: Економіка*. 2025. №24. С. 362–372. DOI : <https://doi.org/10.32782/2708-0366/2025.24.40>.
3. Мазаракі А., Мельник Т. Конкурентоспроможність української економіки в реаліях європейської проблематики. *Зовнішня торгівля: економіка, фінанси, право*. 2025. Том 138. №1. С. 4–22. DOI: [https://doi.org/10.31617/3.2025\(138\)01](https://doi.org/10.31617/3.2025(138)01).