

Ірина ШЕВЧЕНКО,
доктор економічних наук, доцент,
професор кафедри менеджменту та бізнес-адміністрування
Національного аерокосмічного університету
«Харківський авіаційний інститут», Харків, Україна
ORCID: <https://orcid.org/0000-0001-8188-3551>
e-mail: irina_shevchenko@ukr.net

DOI: <https://doi.org/10.32620/pls.2025.67.33>

ЦИФРОВІЗАЦІЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЯК ЧИННИК ЇЇ СТАЛОГО РОЗВИТКУ ТА ЗАХИСТУ

Анотація: у статті розглянуто роль цифровізації як ключового чинника зміцнення захисту та стійкості критичної інфраструктури в умовах сучасних глобальних викликів. Визначено основні цифрові технології, що впроваджуються в інфраструктурні системи, а також окреслено переваги, ризики та напрями підвищення кіберстійкості. Обґрунтовано значення цифрової трансформації для досягнення екологічної, економічної, соціальної та інформаційної стійкості, а також надано рекомендації щодо формування ефективної стратегії цифрового розвитку інфраструктурних об'єктів.

Ключові слова: цифровізація, критична інфраструктура, кібербезпека, стійкість, інновації, штучний інтелект, цифрові технології.

Критична інфраструктура відіграє ключову роль у забезпеченні життєдіяльності суспільства, стабільності економіки та національної безпеки. В умовах глобальних трансформацій, посилення геополітичної напруги та зростання ризиків (зокрема, кіберзагроз), питання її захисту та стійкості стають пріоритетними. У цьому контексті цифровізація виступає не лише як інструмент модернізації, а й як необхідна умова для забезпечення ефективного управління інфраструктурними об'єктами, оптимізації ресурсів, прогнозування ризиків та підвищення загального рівня безпеки. Цифрові технології дають змогу забезпечити прозорість процесів, інтеграцію міжгалузевих систем та оперативне реагування на надзвичайні ситуації. Таким чином, цифровізація стає важливим чинником сталого розвитку критичної інфраструктури. Сучасні цифрові технології стрімко зміню

Відтак, з рис. 1 видно, що до ключових інструментів цифрової трансформації критичної інфраструктури належать Інтернет речей (IoT), великі дані (Big Data), штучний інтелект (AI) та блокчейн. Інтернет речей забезпечує збір і передачу даних у реальному часі, що дозволяє створювати інтелектуальні системи моніторингу інфраструктурних об'єктів. Великі дані використовуються для аналізу значних обсягів інформації, виявлення закономірностей, прогнозування ризиків та оптимізації управлінських процесів. Штучний інтелект дає змогу автоматизувати прийняття рішень, розпізнавати

аномальні ситуації в роботі систем і підвищувати адаптивність інфраструктури до змін. Блокчейн сприяє прозорості, незмінності та захищеності операцій, що особливо актуально у сферах енергетики, логістики та фінансової інфраструктури.

Цифровізація дозволяє істотно підвищити ефективність роботи критичної інфраструктури за рахунок точнішого управління, зменшення витрат на обслуговування, зниження ризику людських помилок та підвищення оперативності реагування на надзвичайні ситуації.

Попри очевидні переваги цифровізації, вона створює нові загрози для функціонування критичної інфраструктури. Високий ступінь автоматизації та підключення до мережі робить інфраструктурні системи вразливими до кіберзлочинності, кібершпигунства, саботажу та кібератак з боку ворожих державних чи недержавних суб'єктів.

Основні виклики цифровізації критичної інфраструктури полягають у зростанні кількості кібератак на її об'єкти, зокрема енергетичні системи, водопостачання, транспорт та охорону здоров'я. Ситуацію ускладнює недостатній рівень кіберзахисту, що проявляється у відсутності сучасних засобів виявлення загроз, використанні застарілого програмного забезпечення та наявності слабких каналів комунікації. Значною проблемою також є дефіцит кваліфікованих фахівців у сфері кібербезпеки, які здатні ефективно реагувати на новітні загрози. Додатково, правова та

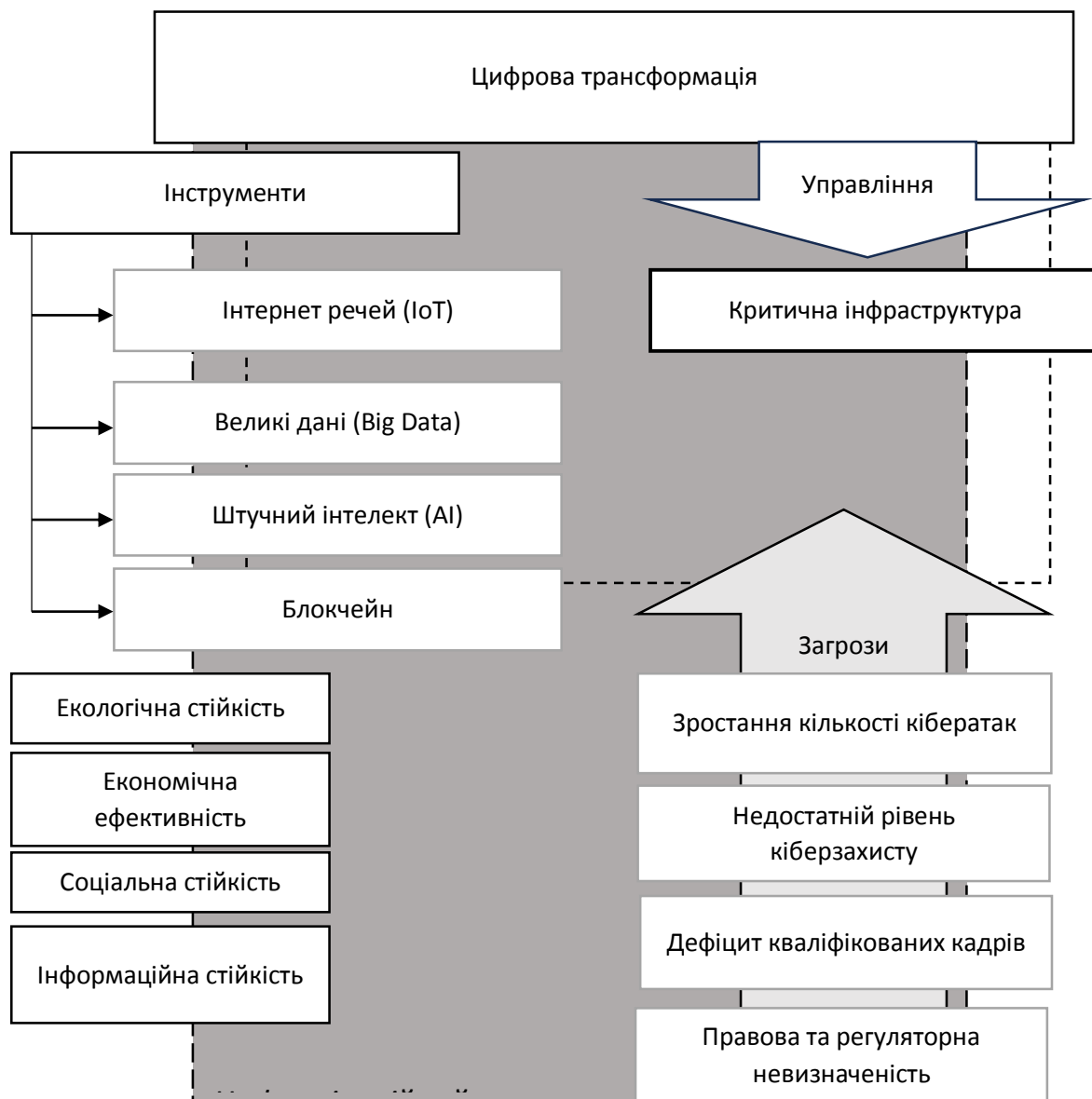


Рис. 1. Цифровізація критичної інфраструктури

регуляторна невизначеність ускладнює впровадження єдиних стандартів захисту, що критично важливо для побудови надійної, стійкої та безпечної цифрової інфраструктури. У цифрову епоху забезпечення безпеки критичної інфраструктури вимагає комплексного, проактивного підходу до кіберзахисту. Ефективна стратегія повинна включати технічні, організаційні та нормативно-правові заходи. Основні компоненти такого підходу:

1. Кіберстійкість як здатність системи протистояти, реагувати та швидко відновлюватися після кібератак або збоїв;

2. Використання сучасних технологій захисту – систем виявлення вторгнень (IDS), багаторівневої аутентифікації, сегментації мереж, шифрування даних;

3. Моніторинг у реальному часі та використання штучного інтелекту для виявлення аномалій;

4. Розробка кризових планів реагування та проведення регулярних тренувань для персоналу;

5. Міжсекторальна взаємодія та обмін інформацією між державними структурами, приватним сектором та міжнародними партнерами.

Окрему увагу слід приділити формуванню ефективного нормативного середовища. Важливо, щоб законодавча база враховувала сучасні виклики цифровізації та забезпечувала належний рівень контролю, відповідальності й підтримки інновацій.

Вплив цифровізації на стійкість і сталий розвиток:

Цифрові технології суттєво розширюють можливості для досягнення стійкості критичної

інфраструктури та сприяють реалізації принципів сталого розвитку. Застосування інтелектуальних систем управління дає змогу підвищити адаптивність інфраструктури до зовнішніх загроз, зменшити вплив надзвичайних ситуацій і скоротити час на відновлення.

Ключові напрями впливу цифровізації:

1. Екологічна стійкість: оптимізація споживання енергії, зменшення викидів, інтелектуальні енергосистеми (smart grids), цифровий моніторинг стану довкілля;

2. Економічна ефективність: зниження витрат на обслуговування інфраструктури, оптимізація логістики, зменшення простоїв;

3. Соціальна стійкість: покращення доступу до базових послуг (вода, енергія, транспорт), підвищення рівня безпеки та якості життя населення;

4. Інформаційна стійкість: здатність систем зберігати функціональність під час криз, підтримка безперервності державних сервісів і цифрового управління.

Таким чином, цифровізація не лише посилює безпеку, але й виступає каталізатором довготривалих позитивних змін у функціонуванні критичної інфраструктури.

Цифровізація критичної інфраструктури є необхідною умовою її адаптації до сучасних викликів, підвищення стійкості та сприяння сталому розвитку. Однак вона супроводжується зростанням цифрових ризиків, що вимагає чіткої та скоординованої відповіді з боку держави, бізнесу та наукової спільноти.

У підсумку можна сформулювати такі ключові рекомендації:

1. Розробка та впровадження національної стратегії цифрової трансформації критичної інфраструктури, що враховує безпекові та екологічні аспекти;

2. Посилення кадрового потенціалу у сфері кібербезпеки та цифрових технологій;

3. Інвестиції у дослідження і розробки інноваційних рішень, спрямованих на моніторинг, прогнозування ризиків та управління кризами;

4. Підвищення рівня міжвідомчої та міжнародної співпраці для обміну досвідом, стандартами та кращими практиками;

5. Створення гнучкої нормативно-правової бази, яка підтримує цифрові інновації та одночасно

гарантує безпеку і стійкість інфраструктурних систем.

Успішна цифрова трансформація критичної інфраструктури можлива лише за умови інтеграції технологічних інновацій з ефективними механізмами управління ризиками та забезпеченням загальнодержавного підходу до безпеки.

Бібліографічні посилання

1. Assessment of Spatial Challenges of the Economic Security System of Industrial Enterprises/ I. Shevchenko et al. International Journal of Safety and Security Engineering. August, 2022. Vol. 12, no. 4, P. 421-428. DOI: <https://doi.org/10.18280/ijssse.120402>

2. Shevchenko I.O. Factors influencing the investment activity of enterprises in the field of digitalization Вчені записки Збірник наукових праць Київський національний економічний університет імені Вадима Гетьмана 38 (1) 2025 р. 275-289

3. Shevchenko I.O. Trading Digital Twin as an Innovative Technology for Ensuring Digital Trade in Sustainable Development Conditions Vol. 1 No. 161 (2024): Actual problems of International Relations DOI: <https://doi.org/10.17721/apmv.2024.161.1.190-199>

I. Shevchenko

Digitalization of critical infrastructure as a factor of sustainable development and protection.

Abstract: the paper examines digitalization as a key factor in strengthening the protection and resilience of critical infrastructure under current global challenges. It outlines the main digital technologies implemented in infrastructure systems and analyzes their benefits, risks, and strategies for enhancing cyber resilience. The importance of digital transformation for achieving ecological, economic, social, and informational sustainability is substantiated, along with recommendations for shaping an effective digital development strategy for infrastructure objects.

Keywords: digitalization, critical infrastructure, cybersecurity, resilience, innovation, artificial intelligence, digital technologies.

Зразок для цитування:

Шевченко І. Цифровізація критичної інфраструктури як чинник її сталого розвитку та захисту. Пропілеї права та безпеки: наук, 2025. №6-7. С. 117-119. DOI: <https://doi.org/10.32620/pls.2025.67.33>.