https://doi.org/10.12958/1817-3772-2026-1(83)-57-67

УДК 330.341.1:330.101.541:338.45+339.9

Олена Олексіївна Хандій,
д-р екон. наук, професор,
ORCID 0000-0002-7926-9007
e-mail: alkhandiy@ukr.net
Інститут економіки промисловості НАН України, м. Київ

БЕЗПЕКОВІ ТА ЕКОЛОГІЧНІ РИЗИКИ ІННОВАЦІЙНОГО РОЗВИТКУ ПРОМИСЛОВОСТІ УКРАЇНИ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТА ПЕРЕХОДУ ДО ІНДУСТРІЙ 4.0 І 5.0[1]

Вступ. Трансформація промисловості на засадах Індустрій 4.0 та 5.0 є ключовою передумовою довгострокової конкурентоспроможності національних економік, підвищення їхньої стійкості та забезпечення економічної безпеки в умовах глобальних технологічних, безпекових і кліматичних викликів. Для України зазначений процес відбувається в умовах повномасштабної військової агресії, глибоких структурних деформацій промислового комплексу, зростання екологічних загроз та обмеженого доступу до фінансових і технологічних ресурсів, що суттєво ускладнює інноваційний розвиток.

Перехід до цифрових, кіберфізичних та людиноцентричних моделей виробництва супроводжується не лише новими можливостями зростання продуктивності та технологічного оновлення, але й формуванням комплексних безпекових та екологічних ризиків. До них належать загрози технологічного суверенітету, вразливість ланцюгів створення доданої вартості, ризики втрати промислової інтелектуальної власності, зростання енергоспоживання цифрових технологій, екологічний слід дата-центрів і цифрової інфраструктури, а також залежність від критичних сировинних ресурсів. У контексті Індустрії 5.0 ці ризики доповнюються соціально-етичними викликами, пов'язаними з роллю людини у цифровому виробництві, справедливістю трансформацій та відповідністю принципам сталого розвитку.

Європейський Союз розглядає Індустрію 5.0 як нормативно-ціннісну модель, спрямовану на поєднання технологічного прогресу з екологічною відповідальністю, соціальною інклюзивністю та економічною стійкістю. Для України, яка задекларувала курс на європейську інтеграцію, адаптація цієї парадигми потребує глибокого переосмислення взаємозв'язку між інноваційним розвитком промисловості, управлінням ризиками та системою забезпечення економічної безпеки держави. Водночас у наукових дослідженнях недостатньо висвітлено безпекові та екологічні ризики інноваційного розвитку промисловості саме в контексті переходу до Індустрій 4.0 і 5.0 з урахуванням українських реалій та європейських політик.

Аналіз останніх досліджень та публікацій. Еволюція дослідницької парадигми від Індустрії 4.0 до Індустрії 5.0 супроводжується поглибленим аналізом ризиків, що виникають при впровадженні відповідних технологічних рішень. Актуалізація цієї проблематики зумовлена розширенням використання кіберфізичних систем, штучного інтелекту, промислового Інтернету речей та цифрових платформ управління виробництвом, інтегрованих у процеси оперативного менеджменту та стратегічного планування підприємств. Узагальнення результатів 83 досліджень, проведене Д. Фукс, Б. Кейс, Б. Айзенбарт і К. Геріке [1] свідчить, що ризики впровадження зазначених технологій мають чітко виражену багатовимірну структуру, яка охоплює стратегічні, фінансові, операційні, технологічні, екологічні та соціальні компоненти. Найбільш часто акцентується увага в цих роботах на ризиках кібербезпеки промислових систем, фінансовій невизначеності інвестицій у цифрову трансформацію, а також ризиках, пов'язаних з недостатнім рівнем підготовки та адаптації робочої сили до використання нових технологічних рішень, що підтверджує системний характер зазначених загроз для інноваційного розвитку промисловості.

Питання безпеки цифровізації промисловості розглядається в багатьох роботах через призму адаптації робочої сили до автоматизованих систем та ризиків, пов'язаних із новими формами технологічної взаємодії. Так, автори [2] підкреслюють, що впровадження розумних машин, штучного інтелекту та роботизованих систем у виробничі процеси з одного боку створює можливості для підвищення продуктивності, а з іншого – породжує ризики для здоров'я та безпеки працівників, що вимагає розбу-

[1] Дослідження виконано в межах «Комплексного наукового дослідження щодо актуалізації промислової політики України на принципах Індустрій 4.0 та 5.0» Інституту економіки промисловості НАН України за рахунок бюджетних коштів, спрямованих на забезпечення проведення державними науковими установами наукових досліджень і науково-технічних (експериментальних) розробок за результатами державної атестації та бюджетної теми «Забезпечення повоєнної розбудови промисловості України робочою силою»(КПКВК6541030).

дови нових стандартів і нормативних механізмів безпеки в контексті Індустрії 5.0.

Серед наукових публікацій вітчизняних вчених у великій кількості представлені роботи про правові та інституційні аспекти забезпечення економічної безпеки в умовах цифрової трансформації. Наприклад, в дослідженні правового регулювання економічної безпеки [3] робиться акцент на загрозах цифровізації, серед яких виділено недостатній перелік індикаторів для оцінювання наслідків цифрових трансформацій, загрози технологічної та фінансової залежності від розвинених країн, а також потреба вдосконалення методик оцінювання ризиків у сфері цифрової економіки. У роботах [4-6] підкреслюється важливість формування правових механізмів, які б дозволили аналізувати не лише технічні, а й економічні аспекти ризикових ситуацій, що виникають при впровадженні технологій Індустрії 4.0. У роботі [7] класифіковано основні групи ризиків, включно з технологічними, фінансовими, операційними, ризиками людських ресурсів, зв'язків із стейкхолдерами та брендовими ризиками, що виникають у процесі цифровізації підприємств української промисловості. Це підкреслює багатовимірний характер ризиків, що виходять за межі суто технічних чи економічних аспектів. Зарубіжні та українські науковці звертають увагу на важливість інтегрованого підходу до аналізу ризиків у виробничих ланцюгах. Так, в роботі [8] висвітлюються аспекти кіберризиків у промислових мережах Інтернету речей та автоматизованих системах, де високий рівень взаємодії між цифровими компонентами створює уразливості, що потребують комплексних засобів безпеки («Defense-in-Depth», криптографічні рішення тощо) для забезпечення цілісності даних і захисту ланцюгів постачання.

Сучасні дослідження демонструють, що безпекові й екологічні ризики інноваційного розвитку промисловості необхідно розглядати комплексно: вони включають цифрові ризики, інституційні обмеження, екологічні наслідки життєвого циклу технологій, соціальні та етичні виклики, що у свою чергу вимагає інтегрованих стратегій управління ризиками з урахуванням європейських підходів до економічної безпеки та сталого розвитку. Одночасно вітчизняна наукова спільнота вказує на потребу адаптації правових та стратегічних рамок для ефективного реагування на ці виклики в умовах післявоєнної відбудови України.

Метою дослідження є виявлення та системний аналіз безпекових та екологічних викликів інноваційного розвитку промисловості України в контексті переходу до парадигм Індустрій 4.0 та 5.0.

Результати дослідження. Промислова трансформація в рамках парадигм Індустрії 4.0 та 5.0 актуалізує необхідність детального аналізу властивих їм ризиків. Індустрія 4.0 у своїй базовій концепції передбачає створення ***«розумних фабрик»*** за рахунок широкої інтеграції інтелектуальних технологій, таких як кіберфізичні системи (CPS), Інтернет речей та промисловий Інтернет речей (IIoT), штучний інтелект (AI), великі дані, цифрові двійники (Digital Twins), автоматизація та роботизація виробництва. У цій концепції технології виступають ***рушіями*** трансформації, що забезпечують взаємодію між фізичними об'єктами та цифровими системами для оптимізації, прогнозування та адаптації виробничих процесів. CPS, зокрема, визначаються як сукупність фізичних і цифрових компонентів, що функціонують у тісно інтегрованих циклах, де поведінка системи змінюється залежно від контексту середовища, що створює нові вимоги до безпеки та стійкості виробничих ланцюгів.

Індустрія 5.0, що сформувалася як наступний етап еволюції виробництва, розглядається як синтез технологічної ефективності Індустрії 4.0 із ціннісними орієнтирами стійкості, людиноцентричності та соціальної відповідальності, де ключову роль відіграє не лише ефективність технічних рішень, але й людино-машинна взаємодія та резильєнтність дослідницько-виробничих систем у широкому соціально-екологічному контексті. Індустрія 5.0 зосереджує увагу на ***людиноцентричному дизайні та штучному інтелекті, що співпрацює з людиною***, де інтеграція людей у виробничі процеси на рівні цифрових двійників, роботизованих систем і кіберфізичних середовищ є не лише технологічною можливістю, але й середовищем, що формує ризики, пов'язані із взаємодією людини з автоматизованими агентами [9].

У межах Індустрії 4.0 ризики здебільшого мають технологічне походження (***technology-driven security risks***): вони пов'язані з вразливістю цифрових компонентів, конфіденційністю даних, безпекою мереж та захистом кіберфізичних систем від кібератак, що безпосередньо впливають на цілісність виробничих середовищ і здатність систем адекватно реагувати на зовнішні загрози. Зокрема, у межах Індустрії 4.0 масштабна мережева взаємодія в межах промислового Інтернету речей підсилює ризик витоку даних і втручання у виробничі процеси, що, своєю чергою, збільшує навантаження на безпекові політики підприємств.

Новий конфігураційний простір ризиків, який можна умовно назвати ціннісно-орієнтовані ризики стійкості (***value-driven resilience risks),*** формує Індустрія 5.0 — це ризики, що виникають не лише з боку технічних складових, але й з комплексної взаємодії людей, технологій та соціально-екологічних контекстів. Для такої моделі ризики пов'язані з етикою автоматизованих рішень, захистом прав людини і забезпеченням довіри у взаємодії з автономними системами, а також із здатністю організацій адаптуватися до непередбачених змін зовнішнього середовища. Це пов'язано з тим, що фокус Індустрії 5.0 зміщується від суто технологічної оптимізації до створення стійких, інклюзивних і відповідальних виробничих систем, де вразливості можуть виникати через людину як активного агента у техно-

логічних ланцюгах або ж через культурні, етичні й соціальні аспекти використання технологій.

Особливу увагу в Індустрії 5.0 займає роль людино-машинної взаємодії як окремого джерела ризиків і можливостей. Вона включає не лише взаємодію користувача з інтерфейсами, а й глибше поєднання людей і цифрових моделей (***human-centric digital twins***), де поведінка людини впливає на системну адаптацію виробничих процесів і навпаки. Це створює нові вимоги до управління ризиками: безпека вже не обмежується захистом даних і систем, а охоплює аспекти психофізіологічної безпеки, взаємної адаптації людини та автоматизованих агентів, а також узгодження очікувань стейкхолдерів з поведінкою автономних технологій. Такі ризики включають виклики з точки зору довіри, тлумачення рішень штучного інтелекту, адаптації робочих процесів і збереження соціального добробуту працівників у високотехнологічному середовищі [10].

Різниця між ***technology-driven security risks*** Індустрії 4.0 і ***value-driven resilience risks*** Індустрії 5.0 полягає у тому, що перші сфокусовані на забезпеченні технічної цілісності, конфіденційності та доступності цифрових ресурсів, а другі — на здатності систем виробництва залишатися стійкими, адаптивними і безпечними з урахуванням ціннісних аспектів, таких як права працівників, етичні вимоги та соціальна відповідальність. У цьому сенсі Індустрія 5.0 розширює поняття «безпека» за межі технологічних загроз до комплексного розуміння стійкості систем у взаємодії з людьми та суспільством.

Індустрія 5.0 розглядається не як черговий етап техніко-економічної еволюції, а як інструмент реалізації стратегічних цілей ЄС у сфері кліматичної нейтральності, соціальної згуртованості та економічної стійкості. Європейська Комісія прямо пов'язує Індустрію 5.0 з ESG-підходом, представляючи промисловість як ключовий простір інтеграції екологічних (Environmental), соціальних (Social) та управлінських (Governance) критеріїв. У цьому вимірі технологічні інновації мають оцінюватися не лише за показниками продуктивності або економічної віддачі, а й за їх впливом на скорочення вуглецевого сліду, підвищення безпеки праці, інклюзивність робочих місць та дотримання етичних стандартів управління. Таким чином, Індустрія 5.0 виступає інституційним механізмом «вбудовування» ESG-принципів у промислову політику, що принципово відрізняє її від технологічно нейтральних підходів Індустрії 4.0.

Посилення цифрової складової виробництва породжує новий спектр етичних і соціальних ризиків, які у межах Індустрії 5.0 визнаються складовою безпекового порядку денного. До них належать ризики алгоритмічної дискримінації, непрозорості рішень систем штучного інтелекту, надмірного моніторингу працівників, а також загрози деградації професійних навичок у разі неправильно організованої автоматизації. Саме тому ЄС наполягає на необхідності поєднання цифрової трансформації з етичним регулюванням, розвитком соціального діалогу та механізмами участі працівників у процесах прийняття рішень. У цьому сенсі Індустрія 5.0 формує нову логіку промислової безпеки, в якій екологічна стійкість, соціальна відповідальність та технологічна інноваційність розглядаються як взаємопов'язані елементи єдиної системи. Для України, яка перебуває на етапі прогнозування післявоєнного відновлення та поступової інтеграції до європейського економічного простору, врахування Індустрії 5.0 саме як нормативно-ціннісної моделі є критично важливим. Ігнорування цього виміру може призвести до формального впровадження окремих цифрових рішень без досягнення стратегічних цілей сталого розвитку, соціальної згуртованості та довгострокової економічної безпеки.

Порівняння траєкторій переходу України та держав – членів Європейського Союзу до Індустрій 4.0 і 5.0 потребує принципового врахування глибокої асиметрії стартових умов, інституційної зрілості та доступу до фінансово-інвестиційних інструментів розвитку. На відміну від України, для якої цифрова та екологічна трансформація промисловості відбувається в умовах повномасштабної війни, втрати виробничих активів і фрагментації інфраструктури, країни ЄС реалізують відповідні процеси в межах стабільних інституційних середовищ, сформованих протягом кількох десятиліть промислової, інноваційної та регіональної політики.

Ключову роль у забезпеченні структурної готовності промисловості ЄС до переходу на засадах Індустрії 5.0 відіграють наднаціональні фінансові та інституційні механізми, насамперед Horizon Europe, Important Projects of Common European Interest (IPCEI) та Recovery and Resilience Facility (RRF). Програма Horizon Europe із загальним бюджетом понад 95,5 млрд євро на 2021–2027 роки забезпечує системне фінансування досліджень і інновацій у сферах штучного інтелекту, кіберфізичних систем, цифрових двійників, чистих технологій та людиноцентричних виробничих рішень, що є базовими напрямами Індустрій 4.0 і 5.0. Водночас Україна має лише асоційований доступ до цієї програми, що обмежує масштаб участі національних промислових підприємств у спільних технологічних платформах та транснаціональних ланцюгах створення доданої вартості.

IPCEI пропонує унікальний інструмент концентрації державної допомоги у стратегічних секторах, зокрема у виробництві мікроелектроніки, акумуляторів, водневих технологій та хмарних інфраструктур. Саме ці проєкти створюють технологічний фундамент для суверенітету ЄС у критичних цифрових і «зелених» технологіях, мінімізуючи зовнішні залежності та підвищуючи безпекову стійкість промисловості. В Україні подібні механізми перебувають лише на етапі концептуального формування, а можливості державної підтримки стратегічних технологій істотно обмежені бюджетними та воєнними факторами.

Recovery and Resilience Facility виступає каталізатором прискореної цифрової та екологічної трансформації економік ЄС після пандемії COVID-19, забезпечуючи синхронізований перехід до кліматично нейтральної та цифровозрілої промисловості. Вимога спрямування не менше 37% коштів на кліматичні цілі та 20% – на цифровізацію створює структурні стимули для впровадження рішень Індустрії 5.0, зокрема у сфері сталого виробництва, енергоефективності та соціальної інклюзивності. Україна ж реалізує процес відновлення без порівнянного за масштабом стабільного фінансового інструменту, що зумовлює значно повільніші темпи накопичення технологічної та екологічної готовності.

Окремої уваги потребує внутрішня асиметрія самого Європейського Союзу, яка проявляється у різних швидкостях переходу до Індустрій 4.0 і 5.0 між «старими» та «новими» індустріальними регіонами. Західноєвропейські промислові кластери, зокрема в Німеччині, Франції та Нідерландах, характеризуються високим рівнем інтеграції цифрових технологій, значними інвестиціями у дослідження та розвиток і сформованими екосистемами взаємодії бізнесу, науки й держави. Водночас країни Центральної та Східної Європи демонструють нижчий рівень технологічної зрілості, вищу енергетичну інтенсивність виробництва та обмежену спроможність до впровадження людиноцентричних і циркулярних моделей, що наближає їхню стартову позицію до української, хоча й за відсутності воєнних ризиків.

Порівняльний аналіз України та ЄС у контексті Індустрій 4.0 і 5.0 має ґрунтуватися не на формальному зіставленні індикаторів, а на врахуванні багаторівневої асиметрії доступу до фінансових ресурсів, інституційної стабільності та політичних інструментів трансформації. Для України це означає необхідність адаптивної, поетапної моделі переходу до Індустрії 5.0, орієнтованої на інтеграцію у європейські програми, поступове нарощування інституційної спроможності та використання післявоєнного відновлення як точки прискореної конвергенції, а не механічного копіювання європейських траєкторій розвитку.

Сучасні дослідження безпекових викликів в контексті цифрової та промислової трансформації дедалі частіше включають в аналіз поняття технологічного суверенітету, яке описує здатність держави та економічної системи контролювати власну цифрову інфраструктуру, програмне забезпечення та технологічні стеки без надмірної залежності від зовнішніх постачальників. Технологічний суверенітет стає ключовим фактором промислової безпеки та конкурентоспроможності: у звіті Європейського парламенту зазначено, що низький рівень власного контролю над цифровою інфраструктурою та технологіями комунікацій створює значну геополітичну вразливість ЄС, зокрема у сегментах оптоволоконних мереж, 5G та супутникового зв'язку, що підсилює ризики для інтегрованих цифрових виробничих систем (***strategic digital infrastructure***) [11].

В контексті української промисловості технологічний суверенітет набуває ще більшої ваги: висока залежність від зовнішніх цифрових платформ, іноземних AI-моделей, хмарних сервісів, програмного забезпечення та обладнання, зокрема пропрієтарних промислових ОС та CAD/CAM-рішень, створює ризики, що виходять за межі традиційних кіберзагроз. Така залежність ускладнює надійну роботу автоматизованих виробничих систем, оскільки будь-які перебої у доступі до міжнародних хмарних сервісів або обмеження доступу до необхідних технологій (через санкції, політичні рішення або технічні збої) здатні привести до зупинки виробничих процесів. Ці проблеми стають очевидними не лише у глобальній практиці – випадки масштабних збоїв у хмарних постачальників демонструють, як зовнішні технічні проблеми можуть паралізувати платформену інфраструктуру, від якої залежить автоматизація виробництва.

Питання технологічного суверенітету тісно пов'язане з безпекою ланцюгів створення вартості (supply chain security), яка в моделі Індустрії 4.0 трансформується під впливом цифрової інтеграції: автоматизовані ланцюги постачання, побудовані на основі CPS, IIoT та AI-аналітики, стають надзвичайно складними системами, що вимагають гнучкого управління ризиками. Як зазначено в сучасних дослідженнях, інтегровані цифрові ланцюги створення вартості підвищують ефективність і видимість операцій, але одночасно створюють нові вектори уразливостей: від кібератак на периферійні пристрої до маніпуляцій з даними в хмарних сервісах, що може призвести до катастрофічних наслідків для всього виробничого циклу [12]. У національному контексті це означає, що втручання у будь-яку ланку глобального ланцюга поставок може негативно вплинути на виробничі плани підприємств, позбавляючи їх ресурсів, компонентів або доступу до ринку. Окремої уваги потребує оцінка залежності від критичних компонентів (мікрочипи, сенсори, батареї) та ризиків решорингу / френд-шорингу (reshoring / friend-shoring).

Регуляторна безпека виступає ще одним ключовим чинником, що стримує інвестиції у цифрову трансформацію промисловості. Невизначеність у регуляторному середовищі – включно з відсутністю чітких правил щодо захисту даних, стандартів інтероперабельності, захисту прав інтелектуальної власності та норм щодо обов'язкової кібербезпеки (наприклад у ланцюгах поставок IoT-пристроїв) – створює невпевненість у довгострокових інвестиційних рішеннях. В ЄС, навпаки, розробка та запровадження нормативних актів, таких як Cyber Resilience Act (Закон ЄС про кіберстійкість (CRA)), створюють більш передбачуване регуляторне середовище для виробників та розробників технологій, встановлюючи вимоги безпеки у виробництві цифрових

продуктів протягом їх життєвого циклу. Така практика демонструє, що чіткі правові рамки сприяють зниженню невизначеності і підвищують готовність підприємств вкладати ресурси у передові технології.

Особливої уваги в межах безпекового аналізу потребує безпека даних промислової інтелектуальної власності, яка становить критичний ресурс для конкурентоспроможності у цифрову епоху. Інтелектуальна власність у вигляді алгоритмів, проектної документації, моделей AI, даних Digital Twins та аналітичних моделей є основою для інноваційної діяльності підприємств. Уразливість цих активів у випадку кібератак, витоку даних або неправомірного доступу створює серйозні ризики не лише для окремих компаній, але й для національної економіки взагалі, оскільки втрата унікальних технологій може призвести до зниження інноваційного потенціалу та послаблення позицій у глобальних ринках. Відсутність ефективної системи захисту інтелектуальної власності у цифровому середовищі суттєво послаблює спроможність держав забезпечувати довгострокове технологічне лідерство.

Безпековим викликом, що набуває сили в умовах цифрової трансформації, є зростання кіберзагроз для промислових систем управління та критичної інфраструктури. За даними Державної служби спеціального зв'язку та захисту інформації України у 2024 році кількість кібератак зросла на 70% порівняно з попереднім роком, а в 2025 - вдвічі порівняно з 2022 роком, основні об'єкти кібератак - місцеві органи влади, уряд та урядові організації, сектор безпеки та оборони, енергетичний сектор, комерційні організації, телекомунікації, що свідчить про цілеспрямоване використання кіберінструментів як складової гібридної війни[1]. В умовах Індустрії 4.0, де виробничі процеси базуються на взаємодії кіберфізичних систем, промислового інтернету речей та хмарних сервісів, такі загрози здатні паралізувати виробництво та спричинити втрату даних. Порушення цілісності цифрових систем негативно впливає на готовність працівників і суспільства до прийняття нових технологій. У цьому контексті відставання України у формуванні комплексної системи кіберстійкості промисловості посилює загальний розрив із країнами ЄС, де кібербезпека вже інтегрована у промислову та цифрову політику. Виклики, які стримують розвиток національної промисловості в контексті Індустрій 4.0 та 5.0, подано в табл. 1.

Таблиця 1. **Безпекові виклики, що стримують розвиток національної промисловості в контексті Індустрій 4.0 та 5.0**

Безпекові виклики (Індустрія 4.0)	Безпекові виклики (Індустрія 5.0)
Кіберуразливість кіберфізичних систем (CPS), IIoT, цифрових двійників	Недостатня людиноцентрична кіберстійкість (human-in-the-loop security)
Залежність від іноземних цифрових платформ і промислового ПЗ	Відсутність технологічного суверенітету та цифрової автономії
Вразливість промислових даних і виробничих алгоритмів	Недостатній захист промислової інтелектуальної власності в цифровому середовищі
Низька безпека цифрових ланцюгів постачання	Відсутність стійких та етичних ланцюгів створення вартості
Регуляторна невизначеність у сфері кібербезпеки та цифрових технологій	Інституційна слабкість у впровадженні ESG-орієнтованих норм безпеки
Недостатня інтеграція вимог директиви NIS2, стандартів ISO/IEC та настанов ENISA	Невідповідність національних практик ціннісній моделі безпеки ЄС
Орієнтація на реактивне управління ризиками	Потреба у превентивній, резильєнтній та соціально відповідальній безпеці
Фрагментованість архітектури промислової кібербезпеки між підприємствами та секторами	Відсутність інтеграції безпеки у корпоративне управління та стратегії сталого розвитку
Низький рівень підготовки інженерно-технічного персоналу до управління цифровими загрозами	Дефіцит компетенцій із управління соціально-технологічними ризиками та соціально-психологічними ризиками цифровізації
Висока залежність безпеки виробництва від стабільності енергетичної та телеком-інфраструктури	Недостатня інституалізація безпеки як елементу соціальної стійкості та довіри
Ризики стандартизаційної фрагментації	Ризики ерозії довіри між людиною та автономними системами
Залежність промислової безпеки від зовнішніх хмарних та edge-інфраструктур	Відсутність механізмів ethical governance AI у промисловості, асиметрія відповідальності за безпекові рішення

Джерело: складено автором

Узагальнюючи, сучасні безпекові виклики Індустрій 4.0 та 5.0 виходять далеко за межі традиційної кібербезпеки. Вони включають структурну залежність від зовнішніх цифрових платформ, що зумовлює технологічну вразливість, складність і динамічність цифрових ланцюгів створення вартості, невизначеність у регуляторному полі як фактор стримування інвестицій у інновації та ризики втрати даних інтелектуальної власності як основи промислових конкурентних переваг. Такий розширений аналіз безпекових аспектів дозволяє краще зрозуміти, чому національна промислова політика має орієнтуватися на комплексне управління ризиками, що включає не лише технологічні, але й правові,

[1] CERT-UA минулого року опрацювала 4315 кіберінцидентів. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (дата звернення: 10.01.2026)

економічні та стратегічні компоненти, особливо в умовах інтеграції у європейський технологічний простір.

Крім безпекових, на шляху інноваційної трансформації промисловості постають не менш гострі екологічні виклики. Вони не лише поглиблюють існуючі ризики, а й формують нові обмеження для інтеграції України в європейський технологічний і економічний простір. Важливо розглядати ці дві групи загроз у їхній синергії.

Одним із ключових екологічних викликів залишається високий рівень викидів парникових газів та низькі темпи декарбонізації промисловості. Попри скорочення абсолютних обсягів виробництва внаслідок війни, структура української промисловості зберігає домінування енергоємних та ресурсомістких галузей, що зумовлює значно вищі викиди CO_2 у перерахунку на одиницю валової доданої вартості порівняно з країнами ЄС. Для порівняння, у 2024 році економіка Європейського Союзу продемонструвала послідовне зниження викидів парникових газів, зокрема до 894 млн т CO_2-екв. у першому кварталі[1] та 767 млн т CO_2-екв. у третьому кварталі року[2], що відображає ефективність реалізації Європейського зеленого курсу та промислової політики декарбонізації. В Україні ж загальні викиди CO_2 у 2024 році зросли на 30% і сягнули 230 млн т CO_2-екв. з початку повномасштабного вторгнення 24 лютого 2022 року[3], що є значним показником з огляду на масштаб економіки та обмеженість виробничої бази.

Ці відмінності формують фундаментальний екологічний бар'єр для інтеграції української промисловості до європейських ланцюгів доданої вартості, оскільки механізм вуглецевого коригування на кордоні (Carbon Border Adjustment Mechanism (CBAM)) прямо пов'язує доступ до ринку ЄС з екологічними характеристиками виробництва. У контексті Індустрії 4.0 це означає зростання трансакційних витрат для підприємств, які не мають можливості оперативно модернізувати виробничі процеси за допомогою цифрових систем управління ресурсами та енергоефективності. Для Індустрії 5.0 ситуація є ще більш критичною, оскільки ця модель передбачає не лише технологічну ефективність, а й відповідність принципам кліматичної нейтральності, соціальної відповідальності та екологічної безпеки.

Вагомим екологічним і водночас безпековим викликом є структура енергоспоживання промисловості України, яка характеризується високою часткою викопних джерел енергії та низьким рівнем диверсифікації. Частка промисловості у кінцевому енергоспоживанні країни в 2023 р. становила близько 21,6%, що не суттєво відрізнялось від середніх показників країн ЄС 23,1%. Така енергоємність робить промислові підприємства надзвичайно вразливими до руйнування енергетичної інфраструктури, коливань цін на енергоносії та перебоїв у постачанні, які стали системним явищем у воєнний період. Проте слід враховувати, що для Європи така структура енергоспоживання є результатом незначного зниження за останні 23 роки, а для України досягнутий рівень енергоспоживання є рух від 1 372 364 ТДж в 2000 р. до 287 484 ТДж в 2023 р.[4]

Для Індустрії 4.0 висока енергоємність означає зниження економічної доцільності впровадження цифрових виробничих систем, робототехніки та промислового інтернету речей, які потребують стабільного енергопостачання. В умовах Індустрії 5.0 ця проблема трансформується у структурний конфлікт між задекларованими цілями сталого розвитку та реальними можливостями підприємств забезпечити екологічно відповідальне виробництво.

Порівняння ролі промисловості в економіках України та країн ЄС додатково підкреслює структурні обмеження трансформації. У Німеччині (27,29%), Польщі (29,39%) та Словаччині (29,14%) частка промислової доданої вартості у ВВП в 2023 році перевищувала середнє значення за даними 178 країн світу - 26,19%[5], що дозволяє цим країнам використовувати промисловість як основу для розвитку цифрових та інноваційних екосистем. В Україні ж цей показник становив 19,09% в 2023 році і 19,03% в 2024 р., що відображає тривалу тенденцію деіндустріалізації та втрати виробничого потенціалу[6].

Крім традиційних екологічних викликів, пов'язаних із викидами, забрудненням та руйнуванням довкілля внаслідок війн або техногенних аварій, сучасна промислова трансформація з використанням цифрових технологій вимагає розгляду повного життєвого циклу технологій, що є ключовим для оцінювання екологічного впливу моделей Індустрії 4.0 та Індустрії 5.0. Цей життєвий цикл включає

[1] EU greenhouse gas emissions down 4.0% in Q1 2024. *Green Forum*. 2024. URL: https://www.green-forum.eu/environment/20240819/eu-greenhouse-gas-emissions-down-40-in-q1-2024-1348 (дата звернення: 10.01.2026)

[2] В ЄС на 5 млн тонн скоротилися викиди парникових газів. *ЕкоПолітика.* 2025. 17 лютого. URL: https://ecopolitic.com.ua/ua/news/v-ies-na-5-mln-tonn-skorotilisya-vikidi-parnikovih-gaziv/ (дата звернення: 10.01.2026)

[3] Кліматична ціна агресії РФ в Україні: викиди парникових газів за рік зросли на 30%. *Укрінформ*. 2025. 25 лютого. URL: https://www.ukrinform.ua/rubric-society/3964311-klimaticna-cina-agresii-rf-v-ukraini-vikidi-parnikovih-gaziv-za-rik-zroslina-30.html.(дата звернення: 15.01.2026)

[4] Україна. Енергетичний баланс. URL: https://www.iea.org/countries/ukraine/energy-mix (дата звернення: 12.01.2026); Європа. Енергетичний баланс. URL: https://www.iea.org/regions/europe/energy-mix (дата звернення: 12.01.2026)

[5] Частка галузі – рейтинг країн. URL: https://www.theglobaleconomy.com/rankings/Share_of_industry/ (дата звернення: 10.01.2026)

[6] Україна: Частка промисловості. URL: https://www.theglobaleconomy.com/Ukraine/share_of_industry/ (дата звернення: 10.01.2026)

не лише експлуатаційну фазу, а й всі етапи створення, обслуговування та виведення з експлуатації цифрових компонентів і інфраструктур, що становлять основу цифрової трансформації.

Одним із найсуттєвіших компонентів цього циклу є енергоспоживання дата-центрів та хмарних інфраструктур, які є фізичною базою для обробки великих даних, штучного інтелекту (AI) та аналітики. За оцінками Міжнародного енергетичного агентства (IEA), на 2024 рік дата-центри споживали близько 415 терават-годин (ТВт·год) електроенергії, що становить приблизно 1,5% світового споживання електроенергії[1], а до 2030 року їх прогнозоване споживання може подвоїтися до 945 ТВт·год, що відповідає майже річному енергоспоживанню великих країн. Такі обсяги споживання створюють значний енергетичний і вугільний слід, особливо якщо джерела електроенергії залишаються частково залежними від викопних палив.

У рамках застосування AI додаткові навантаження на енергетичні системи обумовлені як навчанням моделей, що потребує величезних обчислювальних ресурсів, так і реальним використанням, що зростає за рахунок кількості запитів та інтеграції моделей у бізнес-процеси та продукти. Наприклад, моделі генеративного штучного інтелекту можуть у майбутньому значно збільшити споживання електроенергії дата-центрів шляхом інтенсивної обробки даних, створюючи додатковий екологічний тиск на енергетичні мережі.

Крім енергетичного сліду, цифрові технології мають водний слід, оскільки дата-центри використовують величезні обсяги води для охолодження обладнання, а це особливо критично в регіонах із обмеженими водними ресурсами. Потужні дата-центри можуть споживати до декількох мільйонів літрів води щоденно для безперервного охолодження, що створює додаткові навантаження на водні ресурси та може конфліктувати з потребами інших секторів[2].

Проблема електронних відходів (e-waste) також є невід'ємною складовою життєвого циклу цифрових технологій. Активне оновлення обладнання дата-центрів, серверів, мережевих пристроїв та IoT-елементів спричинює значні обсяги відходів електроніки, які містять токсичні речовини (свинець, ртуть, кадмій) та цінні метали (золото, срібло, платиноїди). Незважаючи на важливість даного аспекту, лише близько 22% електронних відходів у світі формально збирається і переробляється, що призводить до серйозних екологічних і соціальних наслідків у країнах, де ці відходи звозяться для утилізації[3].

Ще одним значущим викликом є залежність від критичних мінералів, які використовуються у виробництві цифрових технологій і компонентів. Серверні платформи, пам'ять, графічні процесори та інше обладнання містять літій, кобальт, рідкоземельні метали та інші стратегічні матеріали, видобуток та переробка яких пов'язані з високими екологічними витратами й соціальними ризиками. Такі мінерали рідкісні, а їх видобуток часто пов'язаний з порушенням екологічної рівноваги, деградацією ландшафтів та значними соціальними витратами у регіонах видобутку, що підсилює загальний екологічний тиск цифрового виробництва.

Важливо також зазначити, що екологічний слід цифровізації не обмежується лише дата-центрами та e-waste, а включає екологічний вплив великих технологічних платформ (Big Tech), що створюють і підтримують цифрові сервіси. Сектор ІКТ становив близько 1,4% світових викидів CO_2 через велику кількість споживаної ними енергії, яка часто є вуглецевомісткою [13], а частина цієї активності пов'язана саме із підтримкою великих обчислювальних центрів і серверних парків. За різними прогнозами[4] викиди CO_2, пов'язані з виробництвом електроенергії для центрів обробки даних, впродовж 2020-2035 рр. до 2028 року будуть тільки зростати.

Отже, повний життєвий цикл цифрових технологій – від видобутку сировини до утилізації обладнання – має суттєві екологічні наслідки, які мають бути включені до комплексних оцінок впливу Індустрії 4.0 і 5.0 на довкілля. Такий підхід дозволяє не лише оцінити операційні викиди, а й виявити приховані екологічні витрати, пов'язані з енергоспоживанням, водокористуванням, виробництвом і утилізацією електроніки, що має важливе значення для побудови ефективних екологічних стратегій та політик підтримки сталого промислового розвитку. Безпековий вимір промислового розвитку суттєво загострюється через руйнування виробничої та енергетичної інфраструктури. Масштабні втрати генеруючих потужностей та мереж електропередачі призвели до різкого скорочення виробництва та споживання електроенергії в Україні[5], що обмежує мож-ливості масштабної цифровізації виробничих процесів.

У країнах ЄС ці процеси компенсуються швидким переходом до відновлюваних джерел енергії, частка яких у виробництві електроенергії у 2024 ро-

[1] Energy demand from AI. *International Energy Agency*. URL: https://www.iea.org/reports/energy-and-ai/energy-demand-from-ai (дата звернення: 10.01.2026)

[2] Вода для даних: як дата-центри впливають на розподіл ресурсів. *GigaCenter*. URL: https://gigacenter.ua/ua/news/p-dvodn-volokonno-optichn-kabel-mozhut-chuti-divers (дата звернення: 10.01.2026)

[3] Рестле Б. Ремонт, а не утилізація! Нові правила ЄС для електросміття. *Deutsche Welle*. URL: https://www.dw.com/uk/remont-a-ne-utilizacia-novi-pravila-es-dla-elektrosmitta/a-69370368 (дата звернення: 12.01.2026)

[4] Штучний інтелект та зміна клімату. *International Energy Agency*. URL: https://www.iea.org/reports/energy-and-ai/ai-and-climate-change (дата звернення: 15.01.2026)

[5] За війну Україна втратила третину споживання електроенергії, – «Укренерго». *Finance.ua*. URL: https://news.finance.ua/ua/za-viynu-ukraina-vtratyla-tretynu-spozhyvannya-elektroenerhii-ukrenerho (дата звернення: 10.01.2026)

ці досягла 47,5%[1]. Це створює потужну основу для розвитку «зеленої» Індустрії 4.0 та людиноцентричної Індустрії 5.0, тоді як в Україні низька частка ВДЕ (11%) формує додаткові ризики відставання.

Узагальнюючи результати аналізу (табл. 2), можна констатувати, що безпекові та екологічні виклики розвитку національної промисловості України формують системні обмеження для впровадження як технологічних рішень Індустрії 4.0, так і ціннісно орієнтованих підходів Індустрії 5.0. Подолання цих викликів потребує не фрагментарних рішень, а комплексної політики, що поєднує післявоєнне відновлення інфраструктури, екологічну реабілітацію, декарбонізацію виробництва та глибоку інтеграцію до європейського промислового та нормативного простору.

Таблиця 2. **Екологічні виклики, що стримують розвиток національної промисловості в контексті Індустрій 4.0 та 5.0**

Екологічні виклики (Індустрія 4.0)	Екологічні виклики (Індустрія 5.0)
Зростання енергоспоживання цифрової інфраструктури (дата-центри, AI)	Неврахування повного життєвого циклу цифрових технологій, відсутність системного Life Cycle Assessment (LCA) у промисловій цифровізації
Вуглецевий слід цифрової автоматизації	Недостатня інтеграція принципів кліматичної нейтральності
Накопичення електронних відходів (e-waste)	Повільний перехід до кліматично нейтральної промисловості
Недостатнє застосування вимог Директиви про промислові викиди (IED) та найкращих доступних технологій (BAT) на підприємствах, що проходять цифрову трансформацію	Низький рівень промислової екологічної резильєнтності
Залежність від викопних джерел енергії	Низька готовність до впровадження принципів climate-resilient manufacturing
Обмежена екологічна оцінка цифрових інновацій	Недостатня інтеграція екологічних та соціальних критеріїв
Фрагментарне управління відходами	Нереалізований потенціал circular manufacturing
Зростання матеріалоємності цифрових технологій (сервери, сенсори, мережеве обладнання)	Недостатня інтеграція кліматичної адаптації у промислові стратегії
Обмежений контроль екологічних параметрів цифрово керованих виробничих процесів	Відсутність циркулярних моделей цифрового виробництва

Джерело: складено автором

Воєнні дії істотно посилили довгострокові екологічні загрози, зокрема через руйнування промислових об'єктів, складів небезпечних речовин, очисних споруд та гідротехнічної інфраструктури. За оцінками Міністерства захисту довкілля та природних ресурсів України, станом на 2024 рік площа територій, потенційно забруднених внаслідок бойових дій, перевищує 139 тис. км², а кількість зафіксованих випадків шкоди довкіллю обчислюється тисячами[2]. Такі масштаби екологічного ураження формують тривалі обмеження для відновлення промислової діяльності, оскільки потребують значних фінансових ресурсів на рекультивацію, очищення та екологічний моніторинг.

Для промисловості, орієнтованої на впровадження Індустрії 4.0, деградація довкілля означає необхідність інтеграції складних цифрових систем контролю екологічних параметрів, управління ризиками та відповідності регуляторним вимогам ЄС. Проте за відсутності належної інституційної підтримки та доступу до інвестицій такі системи залишаються фрагментарними і не забезпечують системного ефекту. У контексті Індустрії 5.0 екологічні наслідки війни мають ще глибший вплив, оскільки ця модель виходить за межі суто технологічної ефективності та розглядає промисловість як частину соціально-екологічної системи, де безпека людини і довкілля є базовими цінностями.

Окремої уваги потребує проблема втрати людського та інтелектуального капіталу, яка має безпосередній безпековий та екологічний вимір. Масова міграція кваліфікованих кадрів, зокрема інженерів, IT-фахівців та науковців, суттєво знижує спроможність промислових підприємств до впровадження складних технологічних рішень. Для Індустрії 4.0 це означає дефіцит компетенцій у сфері автоматизації, аналізу великих даних та управління цифровими платформами. Для Індустрії 5.0 – неможливість реалізувати людиноцентричний підхід, який передбачає активну участь персоналу у процесах інноваційного розвитку та екологічної модернізації.

У сукупності зазначені безпекові та екологічні виклики формують замкнене коло, в якому структурна слабкість промисловості посилює вразливість до зовнішніх і внутрішніх загроз, а ці загрози, своєю чергою, унеможливлюють прискорену модернізацію (табл. 3).

Водночас порівняльний аналіз з країнами ЄС свідчить, що саме системне поєднання промислової, екологічної та безпекової політики дозволяє європейським економікам не лише знижувати ризики, а й використовувати трансформацію як джерело довгострокового зростання.

[1] 2024: nearly 50% of EU electricity came from renewables. *Eurostat.* 2025. 14 January. URL: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20260114-1 (дата звернення: 10.01.2026)

[2] 71 млрд доларів збитків та 180 млн тонн викидів: на COP29 Україна назвала масштаб шкоди природі за 1000 днів війни. *Урядовий портал.* URL: https://www.kmu.gov.ua/news/71-mlrd-dolariv-zbytkiv-ta-180-mln-tonn-vykydiv-na-sor29-ukraina-nazvala-masshtab-shkody-pryrodi-za-1000-dniv-viiny (дата звернення: 15.01.2026)

Таблиця 3. **Загальні системні виклики розвитку промисловості в контексті Індустрій 4.0 та 5.0**

Системні виклики (Індустрія 4.0)	Системні виклики (Індустрія 5.0)
Фокус на технологічній ефективності без урахування соціальних наслідків	Обмежена готовність до ціннісно-орієнтованої промислової політики
Недостатня інституційна спроможність управління трансформаціями	Неузгодженість економічних, екологічних і соціальних стратегій
Обмежений доступ до фінансування інновацій	Асиметричний доступ до європейських фінансових інструментів
Кадровий дефіцит цифрових компетенцій	Дефіцит компетенцій сталого та етичного іннова-ційного управління
Низька довіра між державою та бізнесом	Потреба у партнерських і співтворчих моделях розвитку
Орієнтація на короткострокову ефективність	Необхідність довгострокової промислової резильєнтності
Недостатня інтеграція управління ризиками в систему промислової політики та стратегічного планування	Відсутність системної інтеграції безпекових, екологічних та соціальних ризиків у промислове управління
Домінування проєктного підходу над програмно-системною трансформацією промисловості	Потреба в екосистемному підході до інноваційного розвитку з участю держави, бізнесу та суспільства
Відсутність єдиної національної системи моніторингу цифрової та екологічної трансформації промисловості	Недостатній розвиток індикативного управління резильєнтністю та сталим розвитком
Низький рівень інтеграції науки, промисловості та цифрових інновацій	Обмежена спроможність до співтворення інновацій (co-creation) між людиною, технологіями та інституціями
Фокус на імпорті технологій без розвитку власної інноваційної та виробничої бази	Неузгодженість інноваційного розвитку з цілями стратегічної автономії та економічної безпеки
Недостатня координація між національними та регіональними рівнями промислової політики	Асиметричний розвиток регіонів у процесі людиноцентричної та зеленої трансформації
Відсутність системи оцінювання готовності промисловості до Індустрії 4.0	Недостатня інституціоналізація оцінювання готовності до Індустрії 5.0 та резильєнтності
Воєнно зумовлена деградація промислового та екологічного простору, що ускладнює розгортання цифрових виробничих систем, екологічного моніторингу та відповідність вимогам ЄС	Тривале порушення соціально-екологічної цілісності територій, що обмежує формування резильєнтних, людиноцентричних і сталих промислових екосистем
Скорочення людського та інтелектуального капіталу, зокрема дефіцит інженерних, IT та аналітичних компетенцій, необхідних для автоматизації та цифровізації	Втрата соціального та інноваційного потенціалу працівників, що ускладнює реалізацію співтворчих, етичних і людиноцентричних моделей Індустрії 5.0

Джерело: складено автором

Висновки. Проведений аналіз свідчить, що безпекові та екологічні виклики розвитку національної промисловості України мають системний і багатовимірний характер та істотно стримують її трансформацію на засадах Індустрій 4.0 та 5.0. Висока енергоємність виробництва, значний рівень викидів парникових газів, деградація довкілля внаслідок воєнних дій, руйнування енергетичної та промислової інфраструктури, а також зростання кіберзагроз формують сукупність обмежень, які не можуть бути подолані виключно за рахунок технологічних інновацій.

Порівняння з країнами Європейського Союзу демонструє наявність істотного розриву не лише у рівні технологічного розвитку, але й у здатності інтегрувати екологічні та безпекові вимоги у промислову політику. У той час як у ЄС цифрова трансформація промисловості відбувається паралельно з декарбонізацією, розвитком відновлюваної енергетики та посиленням кіберстійкості, в Україні ці процеси залишаються фрагментованими та значною мірою реактивними.

Результати дослідження підтверджують, що перехід до моделей Індустрії 4.0 та 5.0 в українських умовах можливий лише за умови комплексного підходу, який враховує безпековий та екологічний контекст як ключовий елемент стратегічного планування промислового розвитку. Доцільним є формування інтегрованої державної політики розвитку промисловості, яка поєднувала б завдання післявоєнного відновлення, екологічної реабілітації та цифрової трансформації. Пріоритетним напрямом має стати модернізація енергетичної інфраструктури з орієнтацією на відновлювані джерела енергії та підвищення енергоефективності промислових підприємств, що створить базові умови для впровадження технологій Індустрії 4.0. Важливим є також посилення інституційної спроможності у сфері екологічної політики та екологічного моніторингу з використанням цифрових інструментів, сумісних із європейськими системами даних. Це дозволить не лише знизити екологічні ризики, але й забезпечити відповідність української продукції вимогам ЄС. Окремої уваги потребує розвиток системи промислової та кібербезпеки, інтегрованої у цифрову трансформацію виробництва. Формування кіберстійких промислових екосистем є необхідною умовою як для Індустрії 4.0, так і для людиноцентричної моделі Індустрії 5.0.

Нарешті, стратегічним завданням має стати відновлення та розвиток людського й інтелектуального капіталу через інвестиції в освіту, наукові дослідження та інноваційну інфраструктуру. Саме поєднання технологічних, екологічних і соціальних компонентів дозволить сформувати стійку модель промислового розвитку України, здатну забезпечити її інтеграцію до європейського економічного простору у середньо- та довгостроковій перспективі.

ЛІТЕРАТУРА

1. Fuchs D., Kuys B., Eisenbart B., Gericke K. A systematic literature review on emerging technology risks in Industry 4.0/5.0: identification, clustering and developing mitigation strategies. *Proceedings of the Design Society*. 2025. Vol. 5. P. 299–308. https://doi.org/10.1017/pds.2025.10044

2. Hassan M. A., Zardari S., Farooq M. U., Alansari M. M., Nagro S. A. Systematic Analysis of Risks in Industry 5.0 Architecture. *Applied Sciences*. 2024. Vol. 14, Iss. 4. Art. 1466. https://doi.org/10.3390/app14041466

3. Білоусов Є. М., Корват О. В. Правове регулювання економічної безпеки України в умовах становлення Індустрії 4.0. *Право та інновації*. 2023. № 4 (44). С. 88–94. https://doi.org/10.37772/2518-1718-2023-4(44)-13

4. Копитко М. І., Заверуха Д. А. Ключові аспекти впливу Індустрії 4.0 на економічну безпеку держави. *Соціально-правові студії.* 2021. Вип. 4. С. 117–122. https://doi.org/10.32518/2617-4162-2021-4-117-122

5. Мігус І. Основні тенденції розвитку Індустрії 4.0 та її вплив на економічну безпеку держави: міжнародний аспект. *Вчені записки Університету «КРОК»*. 2023. № 1. С. 52–59. https://doi.org/10.31732/2663-2209-2022-69-52-59

6. Пушак Я. Я., Трушкіна Н. В. Правове забезпечення економічної безпеки держави в умовах Індустрії 4.0. *Цифрова економіка та економічна безпека.* 2022. Вип. 1. С. 135–142. https://doi.org/10.32782/dees.1-22

7. Черніков Д., Гришко С. Сучасні тенденції та стратегічні ризики впровадження технологій Індустрії 4.0 та Індустрії 5.0. *Економіка та суспільство*. 2023. № 54. https://doi.org/10.32782/2524-0072/2023-54-68

8. Mosteiro-Sanchez A. et al. Securing IIoT using defence-in-depth: towards an end-to-end secure Industry 4.0. *Journal of Manufacturing Systems*. 2020. Vol. 57. P. 367–378. https://doi.org/10.1016/j.jmsy.2020.10.011

9. Isaza Domínguez L. G. Digital Twins in Industry 5.0 – a systematic literatura review. *European Public & Social Innovation Review*. 2024. Vol. 9. P. 1–21. https://doi.org/10.31637/epsir-2024-641

10. Davila-Gonzalez S., Martin S. Human Digital Twin in Industry 5.0: A Holistic Approach to Worker Safety and Well-Being through Advanced AI and Emotional Analytics. Sensors. 2024. Vol. 24, Iss. 2. Art. 655. https://doi.org/10.3390/s24020655

11. Knafo S. REPORT on European technological sovereignty and digital infrastructure. 2025. URL: https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html (дата звернення: 10.01.2026).

12. Sobb T., Turnbull B., Moustafa N. Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions. *Electronics.* 2020. Vol. 9, Iss. 11. Art. 1864. https://doi.org/10.3390/electronics9111864

13. Al Kez D., Foley A. M., Laverty D., Furszyfer Del Rio D., Sovacool B. Exploring the sustainability challenges facing digitalization and internet data centers. *Journal of Cleaner Production*. 2022. Vol. 371. Art. 133633. https://doi.org/10.1016/j.jclepro.2022.133633

Надійшла до редакції 19.01.2026
Прийнята до друку 20.02.2026
Опублікована 20.03.2026

REFERENCES

1. Fuchs, D., Kuys, B., Eisenbart, B., & Gericke, K. (2025). A systematic literature review on emerging technology risks in Industry 4.0/5.0: identification, clustering and developing mitigation strategies. *Proceedings of the Design Society*, *5*, 299–308. https://doi.org/10.1017/pds.2025.10044

2. Hassan, M. A., Zardari, S., Farooq, M. U., Alansari, M. M., & Nagro, S. A. (2024). Systematic analysis of risks in Industry 5.0 architecture. *Applied Sciences*, *14*(4), 1466. https://doi.org/10.3390/app14041466

3. Bielousov, Ye. M., & Korvat, O. V. (2023). Legal regulation of Ukraine's economic security in the context of the formation of Industry 4.0. *Pravo ta innovatsii*, *4*, 88–94. https://doi.org/10.37772/2518-1718-2023-4(44)-13 [in Ukrainian].

4. Kopytko, M. I., & Zaverukha, D. A. (2021). Key aspects of the influence of Industry 4.0 on the economic security of the state. *Sotsialno-pravovi studii*, *4*, 117–122. https://doi.org/10.32518/2617-4162-2021-4-117-122 [in Ukrainian].

5. Mihus, I. (2023). Main trends in the development of Industry 4.0 and its impact on the economic security of the state: international aspect. *Vcheni zapysky Universytetu «KROK»*, *1*, 52–59. https://doi.org/10.31732/2663-2209-2022-69-52-59 [in Ukrainian].

6. Pushak, Ya. Ya., & Trushkina, N. V. (2022). Legal support of the state's economic security in the conditions of Industry 4.0. *Tsyfrova ekonomika ta ekonomichna bezpeka*, *1*, 135–142. https://doi.org/10.32782/dees.1-22 [in Ukrainian].

7. Chernikov, D., & Hryshko, S. (2023). Modern trends and strategic risks of implementing Industry 4.0 and Industry 5.0 technologies. *Ekonomika ta suspilstvo*, *54*. https://doi.org/10.32782/2524-0072/2023-54-68 [in Ukrainian].

8. Mosteiro-Sanchez, A., Barcena, M. M., Bahillo, A., & Eizmendi, I. (2020). Securing IIoT using defence-in-depth: Towards an end-to-end secure Industry 4.0. *Journal of Manufacturing Systems*, *57*, 367–378. https://doi.org/10.1016/j.jmsy.2020.10.011

9. Isaza Domínguez, L. G. (2024). Digital twins in Industry 5.0 – a systematic literature review. *European Public & Social Innovation Review*, *9*, 1–21. https://doi.org/10.31637/epsir-2024-641

10. Davila-Gonzalez, S., & Martin, S. (2024). Human digital twin in Industry 5.0: A holistic approach to worker safety and well-being through advanced AI and emotional analytics. *Sensors*, *2*(2), 655. https://doi.org/10.3390/s24020655

11. Knafo, S. (2025). Report on European technological sovereignty and digital infrastructure. *European Parliament.* https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html

12. Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics*, *9*(11), 1864. https://doi.org/10.3390/electronics9111864

13. Al Kez, D., Foley, A. M., Laverty, D., Furszyfer Del Rio, D., & Sovacool, B. (2022). Exploring the sustainability challenges facing digitalization and internet data centers. *Journal of Cleaner Production*, *371*, 133633. https://doi.org/10.1016/j.jclepro.2022.133633

Received: 19.01.2026
Accepted: 20.02.2026
Published: 20.03.2026

Хандій О. О. Безпекові та екологічні ризики інноваційного розвитку промисловості України в контексті забезпечення економічної безпеки та переходу до Індустрій 4.0 і 5.0

Дослідження присвячено критичному аналізу взаємопов'язаних безпекових та екологічних викликів, що супроводжують інноваційний розвиток та цифрову трансформацію промисловості України в умовах переходу до парадигм Індустрії 4.0 та Індустрії 5.0. Актуальність роботи зумовлена посиленням цих викликів на тлі повномасштабної війни, необхідності післявоєнного відновлення, завдань європейської інтеграції та участі в глобальній конкуренції. У роботі проведено систематизацію комплексних загроз, властивих кожній з концепцій. Для Індустрії 4.0 це, перш за все, технологічно детерміновані ризики: кібервразливість кіберфізичних систем та Інтернету речей, залежність від іноземних цифрових платформ, невизначеність регуляторного середовища та вразливість ланцюгів поставок. Екологічний вимір трансформації представлено через призму високої енергоємності, зростаючого вуглецевого сліду цифрової інфраструктури та проблеми електронних відходів.

Індустрія 5.0 робить акцент на людиноцентричності, сталому розвитку та соціальній відповідальності, формує новий простір ціннісно орієнтованих ризиків. До них віднесено загрози, пов'язані з безпекою та етикою людино-машинної взаємодії, соціальною справедливістю трансформації, психофізіологічним добробутом працівників, а також необхідністю інтеграції принципів ESG (екологічні, соціальні, управлінські критерії) у промислову політику. В умовах війни ці структурні проблеми загострюються через масштабне руйнування інфраструктури, забруднення довкілля та критичну втрату людського та інтелектуального капіталу, що формує додаткові обмеження для модернізації.

Обґрунтовано, що для реалізації потенціалу Індустрій 4.0 та 5.0, як драйверів довгострокової економічної безпеки, необхідна комплексна державна політика, що синхронізує післявоєнне відновлення з екологічною реабілітацією, прискореною декарбонізацією, розвитком «зеленої» енергетики, побудовою кіберстійких екосистем та системними інвестиціями в людський капітал.

Ключові слова: Індустрія 4.0, Індустрія 5.0, економічна безпека, екологічні ризики, цифрова трансформація, сталий розвиток, людський капітал, інноваційний розвиток.

Khandii O. Security and environmental risks of innovative development of Ukrainian industry in the context of ensuring economic security and transition to Industries 4.0 and 5.0

The study is devoted to a critical analysis of the interconnected security and environmental challenges that accompany the innovative development and digital transformation of Ukrainian industry in the context of the transition to the Industry 4.0 and Industry 5.0 paradigms. The relevance of the work is due to the intensification of these challenges against the backdrop of a full-scale war, the need for post-war reconstruction, the tasks of European integration and participation in global competition. The work systematizes the complex threats inherent in each of the concepts. For Industry 4.0, these are, first of all, technologically determined risks: cyber vulnerability of cyber-physical systems and the Internet of Things, dependence on foreign digital platforms, uncertainty of the regulatory environment and vulnerability of supply chains. The environmental dimension of transformation is presented through the prism of high energy intensity, the growing carbon footprint of digital infrastructure and the problem of e-waste.

Industry 5.0 emphasizes human-centricity, sustainable development and social responsibility, forming a new space of value-oriented risks. These include threats related to the safety and ethics of human-machine interaction, the social justice of transformation, the psychophysiological well-being of workers, as well as the need to integrate ESG principles (environmental, social, governance criteria) into industrial policy. In war conditions, these structural problems are exacerbated by large-scale destruction of infrastructure, environmental pollution and critical loss of human and intellectual capital, which forms additional constraints for modernization.

It is substantiated that to realize the potential of Industries 4.0 and 5.0 as drivers of long-term economic security, a comprehensive state policy is needed that synchronizes post-war recovery with environmental rehabilitation, accelerated decarbonization, development of "green" energy, construction of cyber-resilient ecosystems and systemic investments in human capital.

Keywords: Industry 4.0, Industry 5.0, economic security, environmental risks, digital transformation, sustainable development, human capital, innovative development.