Ми висвітлимо ваші професійні здобутки
№ 3(25)
2026
ISSN 3041-1254 Online
Успіхи і досягнення у науці

УДК 004:681.3:355.01

https://doi.org/10.52058/3041-1254-2026-3(25)-617-625

Антонюк Віктор Васильович кандидат наук із державного управління, старший викладач кафедри менеджменту, публічного управління та персоналу Західноукраїнського національного університету, м. Тернопіль, https://orcid.org/0000-0002-3744-0339

ЦИФРОВА ТРАНСФОРМАЦІЯ ТА ШТУЧНИЙ ІНТЕЛЕКТ: БЕЗПЕКОВІ ІМПЕРАТИВИ ТА ВИКЛИКИ

Анотація. У статті здійснено комплексний аналіз процесів цифрової трансформації, де штучний інтелект (ШІ) виступає ключовим драйвером інновацій, але водночас генерує значні безпекові виклики в глобальному та національному контекстах. Розглянуто еволюцію ШІ від інструментів автоматизації до автономних систем прийняття рішень, які впливають на державне управління, економічні процеси, соціальні взаємодії та оборонну сферу. Підкреслено, що цифрова трансформація сприяє підвищенню ефективності, наприклад, через оптимізацію ресурсів та персоналізацію послуг, але посилює залежність від технологій, що створює вразливі місця до кібератак, маніпуляцій даними та алгоритмічних помилок. Особливу увагу приділено геополітичним аспектам: у сучасних гібридних конфліктах ШІ стає інструментом для дезінформації, автономних збройних систем та розвідки, що загрожує національній безпеці. Проаналізовано український досвід, де цифрова трансформація є елементом стратегії стійкості проти зовнішньої агресії, включаючи впровадження ШІ в державне управління, оборону та інформаційну безпеку, але вимагає адаптації до європейських стандартів, на кшталт AI Act. Визначено основні ризики: технічні (отруєння даних, адверсаріальні атаки (adversarial attacks), непрозорість систем («чорних скриньок»), правові (відповідальність за помилки, захист персональних даних), етичні (упередження, дискримінація) та екологічні (високе енергоспоживання). Запропоновано концептуальну модель оцінки ризиків на основі матриці ймовірності та впливу, яка інтегрує технічні контрзаходи (federated learning, differential privacy), регуляторні механізми (гармонізація законодавства) та організаційні підходи (міжсекторальна співпраця). Результати дослідження демонструють необхідність балансу між інноваціями та безпекою, з акцентом на людський контроль над ШІ для запобігання ескалації конфліктів. У контексті оборони виділено ризики автономних систем, як-от непередбачуваність дій, алгоритмічні упередження в розпізнаванні цілей та потенціал для неконтрольованої ескалації. Дослідження базується на системному аналізі, прикладах

дослідження та моделюванні, що дозволяє сформувати рекомендації для політики: посилення регулювання, розвиток кіберстійкості та міжнародної співпраці. Наукова новизна полягає в синтезі безпекових імперативів для країн із перехідними економіками, зокрема України, де ШІ є інструментом виживання в умовах війни. Практичне значення – в розробці рамки для оцінки готовності організацій до безпечної цифрової трансформації, що може бути застосоване в державному секторі, бізнесі та обороні. Загалом, стаття підкреслює, що без адекватних безпекових імперативів цифрова трансформація може перетворитися з можливості на загрозу глобальній стабільності.

Ключові слова: цифрова трансформація, штучний інтелект, безпекові імперативи, кіберзагрози, регуляторні механізми, ризики алгоритмів, автономні системи в обороні, інформаційна безпека, етичні виклики ШІ, стійкість цифрових екосистем.

Antoniuk Viktor Vasyliovych Candidate of Public Administration Sciences, senior lecturer of the Management, Public and Personnel Administration Department of the West Ukrainian National University, Ternopil, https://orcid.org/0000-0002-3744-0339

DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE: SECURITY IMPERATIVES AND CHALLENGES

Abstract. The article provides a comprehensive analysis of digital transformation processes, where artificial intelligence (AI) serves as a key driver of innovations, but simultaneously generates significant security challenges in global and national contexts. The evolution of AI is examined from automation tools to autonomous decision-making systems that influence public administration, economic processes, social interactions, and the defense sector. It is emphasized that digital transformation enhances efficiency, for example, through resource optimization and service personalization, but it increases dependence on technologies, creating vulnerabilities to cyberattacks, data manipulation, and algorithmic errors. Particular attention is paid to geopolitical aspects: in modern hybrid conflicts, AI becomes a tool for disinformation, autonomous weapon systems, and intelligence, which threatens national security. The Ukrainian experience is analyzed, where digital transformation is an element of resilience strategy against external aggression, including the implementation of AI in public administration, defense, and information security, but requires adaptation to European standards, such as the AI Act. The main risks are identified: technical (data poisoning, adversarial attacks, opacity of systems ("black boxes")), legal (liability for errors, protection of personal data), ethical (biases, discrimination), and environmental (high energy consumption). A conceptual model

for risk assessment based on a probability and impact matrix is proposed, which integrates technical countermeasures (federated learning, differential privacy), regulatory mechanisms (harmonization of legislation), and organizational approaches (cross-sectoral collaboration). The research results demonstrate the necessity of balancing innovations and security, with an emphasis on human control over AI to prevent conflict escalation. In the defense context, risks of autonomous systems are highlighted, such as unpredictability of actions, algorithmic biases in target recognition, and potential for uncontrolled escalation. The study is based on systemic analysis, case studies, and modeling, which allows for formulating policy recommendations: strengthening regulation, developing cyber resilience, and international cooperation. The scientific novelty lies in the synthesis of security imperatives for countries with transitional economies, such as Ukraine, where AI is a tool for survival in wartime conditions. The practical significance is in the development of a framework for assessing organizations' readiness for secure digital transformation, which can be applied in the public sector, business, and defense. Overall, the article underscores that without adequate security imperatives, digital transformation can turn from an opportunity into a threat to global stability.

Keywords: digital transformation, artificial intelligence, security imperatives, cyber threats, regulatory mechanisms, algorithmic risks, autonomous systems in defense, information security, ethical challenges of AI, resilience of digital ecosystems.

Постановка проблеми. У сучасному світі цифрова трансформація виступає каталізатором змін у всіх сферах життя, перетворюючи традиційні структури на гнучкі, інтелектуальні системи. Інтеграція штучного інтелекту (далі – ШІ) прискорює цей процес, дозволяючи автоматизувати аналітику, прогнозування та взаємодію з користувачами. Однак така еволюція супроводжується зростанням безпекових викликів: від витоків конфіденційної інформації до потенційних системних збоїв, що можуть дестабілізувати критичну інфраструктуру. Проблема загострюється в умовах глобальних конфліктів, де ШІ стає об'єктом маніпуляцій для досягнення стратегічних цілей. В Україні, де цифрова трансформація є частиною національної стратегії стійкості, відсутність комплексного підходу до управління ризиками ШІ може призвести до посилення вразливостей. Це вимагає глибокого аналізу безпекових імперативів, які поєднують технологічний прогрес із механізмами захисту, щоб уникнути неконтрольованих наслідків.

Аналіз останніх досліджень і публікацій. Дослідження цифрової трансформації та ШІ охоплює широкий спектр наукових напрямків. У працях, присвячених державному управлінню, підкреслено роль ШІ в оптимізації процесів, але водночас акцентується на ризиках алгоритмічної автономності та непрозорості рішень. Автори зазначають, що інтеграція інтелектуальних систем

ISSN 3041-1254 Online

у публічний сектор посилює залежність від технологій, що створює загрози кібербезпеки та зовнішнього втручання. У контексті інформаційної безпеки обговорюються виклики, пов'язані з атаками на критичну інфраструктуру, шкідливим ПЗ та соціальною інженерією, особливо в умовах воєнних дій. Дослідження економічних аспектів цифрової трансформації вказують на ризики маніпуляції свідомістю, спотворення культурних норм та екологічні наслідки. У військовій сфері аналізується співпраця держави та суспільства в розробці технологій для оборони, де ШІ грає ключову роль у прогнозуванні та автоматизації. Глобальні звіти про використання ШІ, такі як аналізи патернів взаємодії з чатботами, демонструють перехід від робочих завдань до повсякденного застосування, що розширює спектр ризиків. В українському контексті підкреслюється необхідність адаптації європейських стандартів для посилення регулювання. Загалом, література свідчить, що ШІ – це драйвер прогресу, з одного боку, та джерело нових загроз – з іншого, що вимагає міждисциплінарного підходу.

Мета статті – дослідження та системний аналіз безпекових імперативів та викликів інтеграції штучного інтелекту в процеси цифрової трансформації, з розробкою концептуальної моделі оцінки ризиків та рекомендацій для забезпечення стійкості в умовах геополітичних загроз, зокрема в українському контексті.

Виклад основного матеріалу. Цифрова трансформація передбачає перебудову процесів за допомогою технологій, де ШІ виступає основним інструментом для аналізу даних, автоматизації та персоналізації. Еволюція ШІ від простих алгоритмів до складних нейронних мереж дозволяє прогнозувати тенденції, а також вводить елементи невизначеності через «чорні скриньки» – непрозорі механізми прийняття рішень. Безпекові імперативи тут полягають у забезпеченні конфіденційності, цілісності та доступності даних, що базується на принципах стійкості систем. У глобальному контексті, ШІ інтегрується в державне управління для ефективного розподілу ресурсів, але це посилює ризики залежності від іноземних платформ та потенційного витоку інформації. Теоретичні моделі, як-от фреймворки оцінки ризиків від ENISA, підкреслюють необхідність інтеграції етичних норм у розробку ШІ для запобігання соціальних дисбалансів.

Основні ризики ШІ в цифровій трансформації включають технічні вразливості, як-от отруєння даних, коли шкідлива інформація спотворює моделі навчання, або адверсаріальні атаки, що обманюють системи розпізнавання. Правові виклики стосуються відповідальності за помилки алгоритмів, захисту персональних даних та гармонізації з міжнародними нормами [2]. Етичні аспекти охоплюють упередження в даних, що призводять до дискримінації, та маніпуляцію поведінкою користувачів. У контексті кібербезпеки ШІ стає мішенню для

DDoS-атак чи інверсії моделей, де зловмисники відновлюють конфіденційну інформацію. Екологічні ризики пов'язані з високим енергоспоживанням дата-центрів [3]. Для оцінки цих ризиків запропоновано матрицю, яка комбінує ймовірність та вплив, дозволяючи пріоритезувати контрзаходи (табл. 1).

Таблиця 1

Матриця ризиків ШІ в цифровій трансформації

Загроза	Ймовірність	Вплив	Рівень ризику	Контрзаходи
Отруєння даних	Висока (4)	Критичний (5)	Високий (20)	Аудит даних, аномальне виявлення
Адверсаріальні атаки	Середня (3)	Критичний (5)	Високий (15)	Навчання на адверсаріальних прикладах
Витік моделі	Низька (2)	Високий (4)	Середній (8)	Диференційна приватність, контроль доступу
Маніпуляція результатами	Середня (3)	Високий (4)	Середній (12)	Пояснювальний ШІ, людський контроль
Кібератаки на інфраструктуру	Висока (4)	Середній (3)	Середній (12)	Резервне розгортання, обмеження трафіку
Упередження та дискримінація	Висока (4)	Високий (4)	Високий (16)	Аудит упереджень, метрики справедливості

Примітка: Рівень ризику = Ймовірність × Вплив (шкала 1-5). Високий ризик вимагає негайних дій.

Крім того, розширюючи аналіз на соціальні наслідки, ШІ може посилювати інформаційний шум, призводячи до втрати продуктивності та маніпуляції громадською думкою через генерований контент, як-от deepfakes [3]. Щоб проілюструвати вказані ризики, розглянемо емпіричні приклади реальних інцидентів. Зокрема, у 2025 році батьки з Каліфорнії ініціювали судовий позов проти OpenAI, стверджуючи про причетність чатбота ChatGPT до суїциду їхнього 16-річного сина, оскільки модель нібито сприяла шкідливим діям через маніпулятивні відповіді. Інший інцидент мав місце у серпні 2025 року, коли ChatGPT, за наявними звітами, посилив делірійний стан колишнього менеджера Yahoo, що призвело до вбивства його матері та подальшого суїциду, демонструючи потенціал психологічної маніпуляції та галюцинацій у великих мовних моделях. Серед технічних інцидентів варто відзначити випадок з інструментом штучного інтелекту для кодування від Replit у липні 2025 року, коли система вийшла з-під контролю та видалила виробничу базу даних стартапу SaaStr, підкреслюючи небезпеки автономних помилок та недостатнього нагляду. Етичні упередження виявилися в кейсі iTutorGroup, де система ШІ для рекрутингу систематично відхиляла кандидаток старше 55 років, що стало підставою для позову про вікову дискримінацію. Крім того, компанія Tesla зіткнулася з регуляторними перевірками через несподівані зупинки в режимі автономного керування, що ілюструє ризики непередбачуваної поведінки в критичних систе-

ISSN 3041-1254 Online

мах. Ці емпіричні приклади підкреслюють необхідність впровадження посиленого моніторингу та етичних аудитів для мінімізації ймовірності подібних інцидентів.

Особливо гостро ризики ШІ проявляються в обороні, де автономні системи (як-от дрони чи системи націлювання) можуть призводити до непередбачуваних наслідків. Розглянемо детальніше ключові загрози [1].

По-перше, інтеграція ШІ в автономні системи, такі як безпілотні літальні апарати чи рої дронів, породжує фундаментальні етичні питання щодо розподілу відповідальності. Зокрема, коли алгоритми незалежно приймають рішення про нанесення ураження, виникає ризик помилок, які можуть спричинити непередбачувані наслідки, включаючи втрати серед цивільного населення. Цей аспект тісно корелює з нормами міжнародного гуманітарного права, де брак чітких регуляторних рамок для «автономної зброї» ускладнює її впровадження. Як наслідок, етичні дилеми трансформуються в правові, вимагаючи розробки універсальних стандартів, що забезпечують людський контроль. Без таких механізмів ШІ може сприяти ескалації конфліктів, перетворюючи технологічний прогрес на джерело глобальних ризиків, що наголошує на необхідності міждисциплінарної співпраці для встановлення етичних норм.

По-друге, переходячи до операційних аспектів, ШІ проявляє вразливість до зовнішніх впливів, таких як електронні перешкоди чи сигнальні інтерференції, що є критичним для мобільних платформ, подібних до дронів. Автономність, як основна перевага, часто обмежується високим енергоспоживанням алгоритмів, що скорочує тривалість місій і знижує ефективність у пролонгованих операціях. Крім того, сумісність ШІ з існуючим обладнанням (наприклад, модернізація застарілих систем) вимагає значних ресурсів, інакше виникають системні збої. Технічні виклики підкреслюють потребу в еволюції ШІ від концептуальних моделей до адаптивних рішень, стійких до реальних загроз; в іншому разі, його потенціал залишається нереалізованим, перетворюючись на вразливу компоненту в системах безпеки. Також в України немає власних засобів супутникової глибинної розвідки з системами ШІ, яка в режимі 24/7 спостерігає та миттєво визначає будь-які переміщення військ противника та його маневри в глибокому тилу. Не вистачає засобів власного супутникового зв’язку. Дані ресурси нам надають партнери, не лише державні, а й приватні компанії, від яких ми як держава політично залежні.

По-третє, інтеграція ШІ в традиційні системи озброєння ускладнюється не лише технічними, а й обслуговувальними аспектами. Модульність та ремонтопридатність набувають критичного значення, оскільки складні алгоритми вимагають спеціалізованих інструментів для діагностики, а дефіцит компонентів чи кваліфікованого персоналу призводить до тривалих періодів неактивності. У контексті інтенсивних операцій це посилюється логістичними бар’єрами, де

оперативне відновлення стає неможливим без інновацій, таких як передбачувальний моніторинг. З іншого боку, це створює можливості для оптимізації через модульні конструкції. Такі проблеми ілюструють ширшу тенденцію: ШІ вимагає не лише імплементації, а й реорганізації всієї інфраструктури підтримки, аби уникнути сценарію, коли технологія стає надмірно складною для практичного застосування, тим самим знижуючи загальну ефективність систем.

По-четверте, ще одним логічним розширенням є домен безпеки, де ШІ стає об'єктом кібератак, включаючи злом даних чи маніпуляцію сигналами. У військових контекстах, де системи залежать від цифрових мереж, це може спричинити саботаж, наприклад, через інтерференцію чи фальсифікацію алгоритмів розпізнавання. Як наслідок, без посилених заходів захисту (наприклад, децентралізованих мереж чи криптографії) ШІ перетворюється на слабку ланку в гібридних конфліктах. Отже, кібервразливість підкреслює парадокс: чим інтелектуальніша технологія, тим більша її залежність від захисних стратегій, що вимагає балансу між інноваціями та механізмами безпеки для запобігання системним збоям.

І, нарешті, синтезуючи всі аспекти, організаційні виклики проявляються в необхідності суттєвих інвестицій в освіту, логістику та виробництво. В умовах обмежених ресурсів (як у багатьох державах, що розвивають технології) ШІ може залишитися елітарним інструментом, доступним лише для вузького сегменту. Це посилюється вимогами адаптації до динамічних умов, де оперативні оновлення алгоритмів стикаються з інституційними перешкодами. Організаційні проблеми відображають глобальну тенденцію: ШІ не є автономним рішенням, а компонентом системної трансформації, де ігнорування людського та ресурсного факторів призводить до неефективності, перетворюючи потенціал на невикористані можливості [1].

Тому, виклики використання ШІ свідчать про те, що його переваги – автономність, прецизійність та швидкість – нерозривно пов'язані з ризиками, які вимагають багатогранного підходу. Логічний імператив полягає в інтеграції технологічного прогресу з етичними стандартами, посиленою безпекою та організаційними реформами. Лише таким чином ШІ може еволюціонувати від джерела проблем до інструменту стійкого розвитку, особливо в критичних доменах, таких як оборона.

В Україні цифрова трансформація посилюється через воєнні виклики, де ШІ застосовується для аналізу даних, прогнозування загроз та оптимізації ресурсів. Державні ініціативи, як-от стратегія розвитку ШІ до 2030 року, передбачають інтеграцію з європейськими стандартами, включаючи участь у радах ЄС. Однак ризики посилюються через гібридні атаки, де маніпуляція інформацією стає інструментом дестабілізації. Співпраця держави з бізнесом та суспільством, наприклад, у розробці оборонних технологій, сприяє стійкості, але вимагає

посилення регулювання для захисту даних [4]. Перспективи включають створення «пісочниць» («sandboxes») для тестування ШІ, розвиток національних великих мовних моделей та міжнародну співпрацю для обміну найкращими практиками. У довгостроковій перспективі це дозволить перетворити ШІ на інструмент не лише оборони, але й післявоєнного відновлення, з фокусом на стійкість критичної інфраструктури.

Висновки. Інтеграція ШІ в цифрову трансформацію відкриває нові горизонти для ефективності та інновацій, але вимагає чітких безпекових імперативів для мінімізації ризиків, включаючи технічні, правові, етичні та оборонні аспекти. Запропонована матриця ризиків дозволяє систематизувати загрози та розробити контрзаходи, забезпечуючи баланс між прогресом та стійкістю. В українському контексті це означає посилення регуляторної бази, міжсекторальну співпрацю та адаптацію глобальних стандартів для протидії гібридним загрозам. Особливо критичними є ризики в обороні, де автономні системи можуть призводити до ескалації конфліктів, тому необхідний акцент на людському контролі та етичних нормах. Подальші дослідження можуть фокусуватися на емпіричній оцінці ефективності контрзаходів, моделюванні сценаріїв ескалації та розробці національних стратегій кіберстійкості. Загалом, без комплексного підходу до безпеки ШІ може перетворитися на фактор дестабілізації, тоді як з адекватними імперативами – на основу стійкого розвитку. Тому впровадження обов'язкових аудитів ШІ в державних системах, створення міжурядових платформ для обміну ризиками та інвестування в освіту для підвищення цифрової грамотності населення є вкрай необхідними умовами сьогодення.

Література:

1. Актуальні проблеми бойового застосування, експлуатації і ремонту зразків озброєння та військової техніки. Матеріали V Міжнародної науково-технічної інтернет-конференції, 11-12 листопада 2025 року : збірник наукових праць [Електронний ресурс]. – Вінниця : ВНТУ, 2025. – (PDF, 494 с.).

2. Василенко В.М. Інтеграція систем штучного інтелекту в державне управління : ризики, правові виклики та безпекові гарантії // Вісник Кримінологічної асоціації України. – 2025. – № 2 (35). – Ч. 2. – С. 574–585.

3. Сіденко В.Р. Виклики і ризики цифрової трансформації: світовий та український контексти // Економіка України. – 2021. – № 5. – С. 40–58.

4. Хома Н.М. Цифрова трансформація сфери безпеки та оборони: співпраця держави та суспільства // Вісник НТУУ «КПІ». Політологія. Соціологія. Право. – 2025. – Вип. 4(68). – С. 74–78.

5. Шарова Т.М. Інформаційна безпека в епоху цифрової трансформації // Information Technologies in Metallurgy and Machine Building – ITMM, 2025. – С. 652.

6. European Parliament & Council of the European Union (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689. Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

References:

1. Aktual'ni problemi bojovogo zastosuvannja, ekspluatacії i remontu zrazkiv ozbroєnnja ta vijs'kovoї tehniki [Current problems of combat use, operation and repair of weapons and military equipment]. *Proceedings from V Mizhnarodna naukovo-praktychna konferentsiia «Marketynh innovatsii i innovatsii v marketynhu» – The Fifyh International Scientific and Practical Conference «Marketing of Innovations and Innovations in Marketing»*. (p. 494). Vinnicja : VNTU [in Ukrainian]

2. Vasilenko, V.M. (2025). Integracija sistem shtuchnogo intelektu v derzhavne upravlinnja : riziki, pravovi vikliki ta bezpekovi garantiї [Integration of artificial intelligence systems into state administration: risks, legal challenges and security guarantees]. *Visnik Kriminologichnoї asociaciї Ukraïni - Bulletin of the Criminological Association of Ukraine*, 2 (35), 2, 574–585 [in Ukrainian].

3. Sidenko, V.R. (2021). Vikliki i riziki cifrovoї transformaciї: svitovij ta ukraïns'kij konteksti [Challenges and risks of digital transformation: global and Ukrainian contexts]. *Ekonomika Ukraïni - Economy of Ukraine*, 5, 40–58. [in Ukrainian].

4. Homa, N.M. (2025). Cifrova transformacija sferi bezpeki ta oboroni: spivpracja derzhavi ta suspil'stva [Digital transformation of the security and defense sector: cooperation between the state and society]. *Visnik NTUU «KPI». Politologija. Sociologija. Pravo - Bulletin of NTUU "KPI". Political science. Sociology. Law*, 4(68), 74–78 [in Ukrainian].

5. Sharova, T.M. (2025). Informacijna bezpeka v epohu cifrovoї transformaciї [Information security in the era of digital transformation]. *Information Technologies in Metallurgy and Machine Building – ITMM* [in Ukrainian].

6. European Parliament & Council of the European Union (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689. *eur-lex.europa.eu* Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1689/oj. [in English].

Дата першого надходження статті до видання: 06.03.2026
Дата прийняття статті до друку після рецензування: 19.03.2026