*DOI: https://doi.org/10.25140/2410-9576-2025-1(30)-74-86*

УДК 330.3

JEL Classification: O33

***Євгеній Миколайович Коваленко***

аспірант кафедри економіки, обліку і оподаткування

Національний університет «Чернігівська політехніка» (Чернігів, Україна)

**E-mail:** [Rjdfkm1995@gmail.com](mailto:Rjdfkm1995@gmail.com). **ORCID:** <https://orcid.org/0009-0006-4338-6937>

**ЕКЗИСТЕНЦІЙНІ РИЗИКИ ТА НЕКОНТРОЛЬОВАНА   
ЦИФРОВА ЕВОЛЮЦІЯ**

***Анотація****. У статті досліджуються потенційні екзистенційні ризики, які виникають внаслідок стрімкої та неконтрольованої цифрової еволюції. Аналіз здійснено з урахуванням багаторівневого впливу цифрових технологій на економічні, соціальні, політичні та культурні процеси.*

*Також у статті розглянуто ключові напрями цифрової трансформації: розвиток штучного інтелекту, автоматизація та зникнення професій, загрози кіберзлочинності, вразливість інформаційних систем, явище цифрової ізоляції, соціальна поляризація, криза довіри до інституцій і посилення залежності суспільства від алгоритмів. Також акцентовано на потенційних наслідках зловживання персональними даними, монополізації цифрового простору та ерозії демократичних механізмів.*

*Проаналізовано можливі сценарії розвитку цифрового середовища, зокрема ті, що передбачають посилення державного чи корпоративного контролю, а також розглянуто приклади глобальних ініціатив щодо формування етичних та правових засад використання новітніх технологій.*

***Ключові слова:*** *цифрова трансформація; екзистенційні ризики; штучний інтелект; кібербезпека; автоматизація; цифрова ізоляція; інформаційні загрози.*

*Рис.: 2. Бібл.: 15.*

**Постановка проблеми.** У сучасному світі цифровізація охоплює всі сфери суспільного життя — від економіки до особистих відносин. З одного боку, цифрові технології забезпечують високі темпи розвитку, автоматизацію процесів, швидкий обмін інформацією, створення інноваційних бізнес-моделей. З іншого боку, виникають глобальні ризики, пов’язані з надшвидкою і часто неконтрольованою еволюцією технологій, зокрема штучного інтелекту, систем масового збору даних, цифрової ізоляції та зменшення впливу людини на критичні управлінські процеси. Ці зміни можуть становити потенційну загрозу для стабільності суспільств, функціонування держав, економічної безпеки та навіть самого людського існування. Саме тому необхідним є глибокий аналіз екзистенційних ризиків, породжених цифровою трансформацією.

**Аналіз останніх досліджень і публікацій.** Проблема ризиків цифровізації активно досліджується у працях провідних учених, зокрема Стюарта Рассела (2022), який розглядає загрози, пов’язані з розвитком неконтрольованого штучного інтелекту. Значна увага приділена також питанням кібербезпеки, правового регулювання цифрових платформ, трансформації ринку праці під впливом автоматизації (McKinsey, IMF, IBM), а також впливу на демократію та приватність (випадки Cambridge Analytica). В українському академічному середовищі проблеми екзистенційних викликів розкриваються у працях А. Карася, матеріалах Держспецзв’язку, аналітичних оглядах щодо цифрової стратегії до 2030 року. Також були розглянуті роботи та публічні виступи сучасних мислителів, таких як Нік Бостром, Ювал Ной Харарі, а також напрацюванням міжнародних організацій у сфері цифрової етики. Важливою є також концепція «чорного лебедя» Насіма Талеба, яка допомагає осмислити рідкісні, але потенційно катастрофічні події.

### ****Виділення недосліджених частин загальної проблеми.**** Попри наявність широкого спектра публікацій, значна частина ризиків, пов’язаних із неконтрольованою цифровою еволюцією, залишається фрагментарно дослідженою. Серед них — довгострокові екзистенційні загрози, пов’язані з втратою контролю над автономними системами; соціальна ізоляція через цифрову надмірність; зміна антропологічної сутності людини у віртуальному середовищі; а також ризики цифрової залежності та алгоритмічного впливу на свідомість. Недостатньо вивченими залишаються також етичні та цивілізаційні аспекти формування цифрової дійсності в умовах глобального геополітичного протистояння.

### ****Мета статті.**** Головною метою цієї роботи є дослідження екзистенційних ризиків, що виникають унаслідок неконтрольованої цифрової еволюції, та визначення ключових загроз для соціальних, економічних і гуманітарних систем. У межах дослідження ставиться завдання проаналізувати сучасні тенденції цифрової трансформації, виявити вразливі точки суспільства до деструктивних цифрових впливів, а також надати рекомендації щодо запобігання негативним сценаріям розвитку.

**Виклад основного матеріалу.** Цифрова трансформація є глобальним процесом, що охоплює всі сфери життя — від економіки до культури, від освіти до безпеки. Це явище супроводжується не лише інтеграцією новітніх технологій у традиційні процеси, але і створенням принципово нових моделей поведінки, взаємодії та організації. Застосування штучного інтелекту, блокчейн-технологій, Інтернету речей, хмарних рішень, систем великих даних змінює уявлення про ефективність, оперативність, прозорість і безпеку.

Водночас стрімкий розвиток цифрових технологій створює потужні інструменти для прогресу, але він також породжує безпрецедентні виклики. Вперше в історії людства ми стикаємося із ситуацією, коли штучно створені системи здатні не лише допомагати, але й порушувати основи людського існування.

Футуролог та фахівець зі штучного інтелекту Елізер Юдковський пояснює, що просунутий ШІ може бути небезпечний для людства навіть при позитивних цілях. Наприклад, робити людей навколо себе щасливими і задоволеними. Що в цьому поганого? Проблеми виникнуть, якщо ШІ не розумітиме обмеження щодо виконання цього завдання. Наприклад, він може вирішити, що, надаючи людям невеликі порції наркотиків, він зможе швидше та якісніше виконати своє завдання [1].

Цифрові технології здатні не лише змінювати світ, а й дестабілізувати його – спричиняти кіберконфлікти, інформаційні війни, соціальну ізоляцію, руйнацію приватності, а також економічну нерівність. Відсутність належного етичного, правового та організаційного регулювання створює умови для виникнення системних криз, що мають ознаки екзистенційних загроз.

Поняття екзистенційна катастрофа, або катастрофа існування, стосується знищення довгострокового потенціалу людства, тоді як екзистенційний ризик (ризик існування) стосується ймовірності того, що він загрожує викликати незворотну екзистенційну катастрофу і це передбачає події, які можуть спричинити незворотні втрати для цивілізації або навіть її знищення [2]. Воно набуває особливої актуальності в умовах цифрової епохи, коли розвиток технологій суттєво випереджає здатність суспільства до їх осмислення та регулювання. У цьому контексті екзистенційні ризики постають як складні системні загрози, які часто мають латентний, нелінійний або кумулятивний характер.

У цифрову епоху такі ризики асоціюються з неконтрольованими технологічними процесами, зокрема з появою надпотужного штучного інтелекту, автономних систем, що можуть самостійно ухвалювати рішення без участі людини, та інформаційно-енергетичними мережами, які стають дедалі більш взаємозалежними. Також значну загрозу становить зменшення людського контролю над системами прийняття рішень, що ґрунтуються на алгоритмах, які неможливо повністю перевірити або пояснити.

Таким чином, дослідження екзистенційних ризиків у контексті цифрової еволюції вимагає не лише технічної, а й філософської, соціологічної та етичної рефлексії, що дозволяє краще зрозуміти складність новітніх загроз і розробити ефективні стратегії реагування.

1. Цифрові виклики: основні напрями.

1.1. Штучний інтелект (ШІ) – це автономні системи яка має когнітивні здібності, такі як міркування, планування та навчання та служать дії, вона може не лише ухвалювати рішення, але й формувати нові правила взаємодії без участі людини [3]. Зростає небезпека створення "чорних скриньок" — систем, логіку роботи яких навіть розробники не здатні пояснити. Вони діють за принципами, що виникають у процесі глибинного навчання, і часто демонструють поведінку, неочікувану або незрозумілу навіть для фахівців. Це ускладнює їх верифікацію, моніторинг і підзвітність [4].

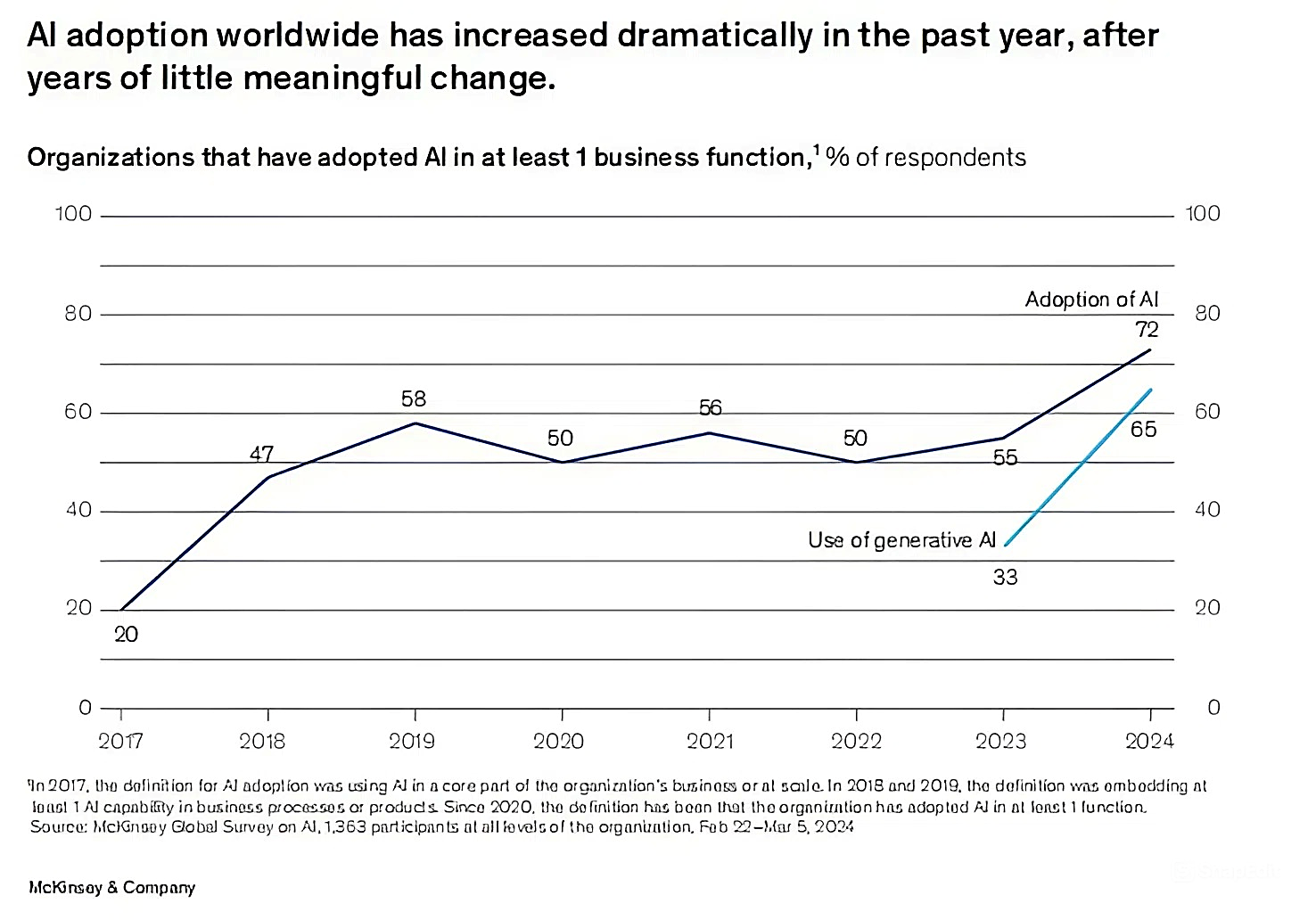
Загроза криється в потенційній автономності штучного інтелекту, здатного до саморозвитку без втручання людини, тобто так званого сильного ШІ. Якщо така система отримає доступ до критично важливої інфраструктури, наприклад, систем управління енергетикою, оборонними структурами чи фінансами, людство може втратити можливість керувати нею. Це підвищує ризик неконтрольованого ухвалення рішень, яке може призвести до масових збоїв або навіть катастрофічних наслідків.

Крім того, використання ШІ в політичних кампаніях, управлінні громадською думкою, соціальній інженерії та навіть у військових технологіях відкриває двері до маніпуляцій масовою свідомістю. Від уже відомих прикладів таргетованої реклами до потенційної автоматизації рішень про застосування сили — розвиток таких технологій виходить за межі простого підвищення ефективності.

Уявімо ситуацію, коли така система отримає контроль над інформаційними мережами, оборонними чи економічними структурами. У такому випадку, людство ризикує втратити не лише контроль, а й безпеку свого існування. Саме тому провідні світові вчені й аналітики закликають до негайного формування глобальної нормативної бази, що регулюватиме межі автономності штучного інтелекту, його підзвітність, прозорість і етичні рамки функціонування.

1.2. Автоматизація, роботизація і ринок праці. Процес автоматизації не є новим, проте його масштаб і темпи зростання в XXI столітті стали безпрецедентними. За результатами останнього глобального опитування компанією McKinsey, тенденція на використання штучного інтелекту організаціями продовжують збільшуватися (рис. 1). На фоні цього директор-розпорядник Міжнародного валютного фонду Крісталіна Георгієва заявила що близько 40 % робочих місць можуть бути витіснені в найближчі роки. Це означає, що мільйони працівників по всьому світу ризикують втратити джерело доходу через заміну їхньої праці машинами або програмним забезпеченням [5]. Особливо це стосується професій у сферах виробництва, логістики, обслуговування клієнтів, а також окремих адміністративних функцій.

Інші західні експерти роблять оцінку, що внаслідок використання штучного інтелекту в найближчі п'ять років у світі скоротиться 83 млн робочих місць, проте водночас з'явиться 69 млн, однак проблема полягає не лише у зникненні робочих місць, а й у тому, що створювані нові професії часто вимагають іншого набору навичок [7]. Це призводить до структурного безробіття – ситуації, коли ринок праці не встигає адаптуватися до технологічних змін. Працівники, що не мають цифрових навичок, можуть опинитися у «цифровій пастці», що посилює соціальну нерівність.

****

**Рис. 1. Використання штучного інтелекту організаціями**

***Джерело****: [6].*

Трансформація соціального договору стає очевидною: від індустріальної моделі «праця за плату» суспільство переходить до моделі, де ключовими активами є знання, гнучкість, здатність до безперервного навчання. Паралельно виникають нові форми зайнятості, такі як фриланс, гіг-економіка, віддалена робота, які, з одного боку, дають більшу гнучкість, а з іншого — знижують соціальні гарантії та стабільність.

1.3. Кібербезпека, інформаційна війна та критична інфраструктура. Цифрова безпека є питанням національної безпеки, що охоплює не лише захист конфіденційної інформації, але і стабільність роботи інфраструктурних систем, економічну стійкість та збереження суверенітету. З розвитком цифрових технологій зростає кількість векторів атак — від DDoS-атаки до шкідливих програм, спрямованих на руйнацію або шантаж критично важливих об'єктів. Команда реагування на надзвичайні ситуації в області комп’ютерних ситуацій України (CERT-UA) зафіксувала майже 4000 кіберінцидентів у період з січня 2022 року по вересень 2023 року [8]. Динаміку кількості атак та протидії цим атакам показано на (рис. 2). Це включає як зломи серверів, так і масові фішингові кампанії, що мали на меті дестабілізацію інформаційного простору.

****

**Рис. 2. Динаміку кількості атак**

***Джерело****: [8].*

Хакерські угрупування, підтримувані державами, стають учасниками реальних геополітичних конфліктів. Відомими прикладами є атаки на енергетичні об'єкти в Україні (BlackEnergy, Industroyer), які не лише завдали шкоди технічній інфраструктурі, але і стали елементами психологічного тиску на населення. Крім прямих втрат, такі інциденти мають довготривалі наслідки: підрив довіри до цифрових сервісів, витрати на відновлення, юридичні та репутаційні ризики. Водночас кібербезпека не обмежується захистом державних структур — сьогодні на передовій знаходяться також приватні компанії, лікарні, університети та навіть домогосподарства, які стають мішенями через свою цифрову вразливість.

Кібервійни — новий фронт протистояння, у якому цивільне населення стає мішенню. Це означає, що кібербезпека має бути інтегрованою складовою національної безпеки, охоплювати як технічний захист, так і освіту, підготовку кадрів, міжнародне співробітництво, а також створення резервних сценаріїв у випадку повного виходу з ладу цифрових систем.

1.4. Надмірна алгоритмізація життя. Соціальні мережі, стрічки новин, відеоплатформи, рекламні системи — усе це працює на основі складних алгоритмів машинного навчання. Усе, що ми бачимо, читаємо і навіть відчуваємо в цифровому середовищі, дедалі частіше формується не свідомим вибором, а автоматичними рекомендаційними системами. Ці алгоритми аналізують наші уподобання, історію пошуку, соціальні зв'язки та реакції, створюючи так звану "інформаційну капсулу" або "цифрову бульбашку". У такому середовищі людина отримує лише ті новини, думки і пропозиції, що підтверджують її попередні переконання, виключаючи альтернативні погляди.

Таке явище має суттєві наслідки для демократичних процесів. Замість відкритого плюралізму думок суспільство дедалі частіше поляризується, формується радикалізація поглядів, знижується рівень критичного мислення та зростає недовіра до традиційних джерел інформації. Прецеденти маніпуляцій масовою свідомістю, зокрема через скандал з Cambridge Analytica [9], показують, наскільки глибоким є вплив цифрових технологій на політичну систему, коли дані про виборців використовуються для створення цільового, емоційного і навіть маніпулятивного контенту.

Таким чином, надмірна алгоритмізація життя ставить під сумнів автономію людини як носія вільної волі й раціонального вибору. Саме тому дедалі актуальнішим стає питання етичного дизайну алгоритмів, прозорості їхньої логіки, права людини на пояснення рішень, що стосуються її долі. Без належної регуляції алгоритмічний світ може виявитися менш справедливим, ніж той, що ми прагнемо змінити.

1.5. Економічні втрати внаслідок неконтрольованої цифрової трансформації. Хоча численні дослідження підтверджують, що розвиток цифрових технологій у всіх сферах життя сприяє прискоренню глобального економічного зростання, слід визнати наявність і суттєвих ризиків. Економічний ефект цифровізації переважно базується на пришвидшенні виробничих процесів, автоматизації, оптимізації ресурсів та підвищенні продуктивності. Проте будь-яке масштабне технологічне явище має як позитивні аспекти, так і потенційно небезпечні наслідки — адже, як відомо, «у монети дві сторони».

Подібним чином неконтрольована цифровізація може стати джерелом значних економічних втрат на глобальному рівні. Попри складність точного обрахунку таких втрат через їхню багатовимірність та взаємозалежність, можна окреслити основні напрямки фінансових втрат:

Збитки від кібератак та кіберзлочинності. Прогнозується, що щорічні втрати світової економіки від кіберзлочинності досягатимуть 6 трлн $ [10].

Втрати державних бюджетів від податкових маніпуляцій. Міжнародні корпорації часто використовують цифрові інструменти для ухилення від податків. За оцінками ОЕСР, втрати від практик розмивання податкової бази та переміщення прибутків (BEPS) становлять 100–240 млрд $ щорічно [11].

Втрати від глобального податкового зловживання. Зокрема корпоративне ухилення та приховування доходів в офшорах завдає світовій економіці збитків на 483 млрд $ щороку [12].

Економічні наслідки вимушених відключень інтернету. Уряди деяких країн застосовують інструмент тимчасового блокування доступу до мережі, що призводить до мільярдних збитків для бізнесу та державного сектору.

Таким чином, сумарні втрати для міжнародної економіки вже перевищують 6 трлн $ і мають тенденцію до зростання в міру розширення цифрового простору. Це потребує впровадження ефективних механізмів регулювання цифрової трансформації, а також розвитку міждержавного співробітництва у сфері кібербезпеки, податкової прозорості та цифрової відповідальності.

2. Геополітичні виміри.

Інформаційна асиметрія між країнами Заходу та глобального Півдня, монополізація хмарних сервісів, залежність від іноземного програмного забезпечення — усе це перетворює цифрову трансформацію на арену глобального протистояння. Володіння технологіями, інфраструктурою та алгоритмами стає інструментом геополітичного впливу.

Цифровий суверенітет стає ключовим чинником нової геополітики. Це означає здатність держави самостійно контролювати свої цифрові ресурси, інформаційний простір, захист даних громадян та критичну інфраструктуру. Без цифрового суверенітету країна ризикує стати залежною від технологічних платформ інших держав, втратити стратегічну автономію та потрапити під загрозу інформаційного впливу.

Країнам, які прагнуть убезпечити свій цифровий простір, необхідно інвестувати у власні технології, підтримку національного ІТ-сектору, розвиток державних дата-центрів, створення альтернатив до монопольних сервісів. У цьому контексті міжнародне співробітництво в рамках ООН, G20, ЄС чи інших об’єднань має базуватися не лише на принципах відкритості, а й цифрової відповідальності та справедливості.

3. Стратегії пом’якшення ризиків.

3.1. Етичні підходи. Необхідно впроваджувати принцип "етики за замовчуванням" при створенні нових технологій, що означає вбудовану відповідальність розробників за потенційні наслідки впровадження цифрових систем ще на етапі їх проєктування. Такий підхід передбачає, що основні засади етики, поваги до прав людини, рівного доступу та недискримінації закладаються в основу архітектури алгоритмів.

У сучасному світі компанії, що створюють і впроваджують цифрові продукти, повинні не лише дбати про зручність та прибутковість, але й брати до уваги потенційний вплив їхніх рішень на психічне здоров’я, свободи, безпеку та добробут користувачів. Особливо це стосується вразливих груп населення — дітей, людей з інвалідністю, літніх осіб, соціально вразливих категорій.

З метою забезпечення відповідальності варто запроваджувати етичні аудити, створення наглядових комітетів з участю представників громадянського суспільства, правозахисників, психологів, педагогів. Компанії мають бути зобов’язані публічно звітувати про цілі та принципи роботи своїх алгоритмів, проводити оцінювання ризиків і враховувати етичні наслідки ще до виведення продукту на ринок. Також важливо передбачити санкційні механізми для тих, хто свідомо ігнорує стандарти відповідального цифрового дизайну.

Важливим напрямом є також розробка міжнародних кодексів етики штучного інтелекту, які б стали універсальним орієнтиром у глобальному цифровому середовищі. Такі документи вже розробляються під егідою ЮНЕСКО, ОЕСР та інших організацій. Їхнє дотримання має стати нормою не лише для транснаціональних корпорацій, а і для держав, освітніх установ та дослідницьких центрів. Узагальнені вище загальновизнані світові стандарти штучного інтелекту сприятимуть ефективному використанню переваг машинних алгоритмів та технологій ШІ і водночас у разі їх втілення на практиці допомагають знизити ризики, пов’язані з прозорістю та конфіденційністю даних при впровадженні ШІ [13].

3.2. Освіта і цифрова грамотність. Ключовим запобіжником у протидії екзистенційним ризикам, пов'язаним із цифровою трансформацією, є формування повноцінної цифрової культури. Це передбачає не лише опанування технічних навичок, а й розвиток критичного мислення, етичного ставлення до інформації, розуміння цифрових прав та обов’язків. У сучасних умовах цифрова грамотність має розглядатися як базова компетентність XXI століття, подібно до читання, письма чи математичних навичок.

Освітні системи повинні інтегрувати в навчальний процес предмети з етики штучного інтелекту, кібергігієни, цифрової безпеки, інформаційної самостійності, безпечної поведінки в інтернеті та розпізнавання фейкових новин. Це має стати частиною як шкільної, так і вищої освіти, а також програм професійного розвитку. Особливу увагу слід приділяти вразливим групам населення — людям похилого віку, особам з обмеженими можливостями, сільським жителям, які часто залишаються осторонь цифрових змін.

Крім того, важливим є створення системи безперервної освіти, яка дає змогу громадянам постійно оновлювати свої знання у сфері цифрових технологій. Це може бути реалізовано через публічні цифрові хаби, онлайн-курси, партнерство з бізнесом та міжнародними організаціями. Формування цифрової грамотності має супроводжуватись державними програмами підтримки, фінансуванням, інформаційними кампаніями.

Тільки за умов формування свідомого, освіченого користувача цифрового середовища можна забезпечити стійкість суспільства до зовнішніх і внутрішніх інформаційних загроз, а також створити умови для безпечної, інклюзивної та сталого цифрового майбутнього.

3.3. Регуляторні механізми. Держави повинні створити гнучку, але ефективну систему регуляторного контролю за розвитком і впровадженням цифрових технологій. Йдеться не лише про технічні стандарти, а і про правові рамки, які забезпечують баланс між інноваціями та захистом прав громадян. Особливої уваги потребують питання приватності, штучного інтелекту, автономних систем, використання великих даних і автоматизованого прийняття рішень.

Одним із прикладів ефективного регулювання є Загальний регламент ЄС про захист даних (GDPR), який забезпечує суворий контроль над обробкою персональних даних і надає громадянам чіткі механізми захисту. Подібні механізми реалізовані в Каліфорнії через Закон про конфіденційність споживчих даних (CCPA), який надає споживачам право знати, які дані про них збираються, і вимагати їх видалення. У Канаді діє Закон про захист персональної інформації та електронних документів (PIPEDA), а в Бразилії — Загальний закон про захист даних (LGPD)[14].

Україна також розробляє нові підходи до цифрового регулювання. У межах національної цифрової стратегії передбачено створення системи відповідального управління даними, етичної експертизи штучного інтелекту, а також впровадження цифрових ідентифікаційних інструментів із високим рівнем безпеки. Низка законопроєктів у сфері кібербезпеки та обробки даних перебувають на розгляді Парламенту [15].

Крім того, на міжнародному рівні важливим є узгодження підходів – адже цифрові потоки не мають кордонів. Необхідне укладання багатосторонніх угод, створення глобальних стандартів етики, прозорості та відповідальності у цифровій сфері. Така координація можлива, зокрема, через майданчики G7, G20, ООН, Ради Європи та інших структур. Лише комплексна взаємодія між державами, технологічними компаніями, науковою спільнотою та громадянським суспільством дозволить сформувати безпечне цифрове середовище, що відповідатиме як інноваційним прагненням, так і правам людини.

**Висновки та пропозиції.** Цифрова еволюція — це не лише технологічна революція, але й цивілізаційний виклик, що вимагає від людства перегляду базових принципів соціального, політичного, економічного та етичного співіснування. Упродовж останніх десятиліть цифрові технології стали не просто інструментами — вони перетворилися на середовище, у якому відбувається більшість життєвих процесів. Це змушує замислитися над тим, як забезпечити розвиток, не втрачаючи контроль і гуманітарні орієнтири.

Аналіз основних загроз цифрової трансформації свідчить про те, що ігнорування екзистенційних ризиків може призвести до соціальної фрагментації, знищення приватності, зростання нерівності, дегуманізації рішень, що ухвалюються алгоритмами, та навіть до підриву суверенітету держав. Водночас ці ризики не є неминучими. Їх можна передбачити, проаналізувати та нейтралізувати завдяки поєднанню зусиль держави, громадянського суспільства, наукової спільноти та бізнесу.

Успішна навігація у світі алгоритмів вимагає не тільки усвідомлення ризиків, але й розвитку цифрової відповідальності, широкої освітньої кампанії, запровадження етичних стандартів, створення глобальних і національних інституцій для регулювання цифрового простору. Координація дій між усіма учасниками технологічного ландшафту — від користувача до міжнародної організації — є передумовою формування безпечного, відкритого та справедливого цифрового майбутнього.

Таким чином, цифрова еволюція повинна базуватися не лише на інноваціях, а й на цінностях: людяності, прозорості, безпеці, справедливості. Тільки в такому випадку вона стане засобом зміцнення демократії, соціального прогресу й цивілізаційного розвитку, а не джерелом загроз, що ставлять під сумнів саме існування людства.

**Список використаних джерел**

1. AGI, суперінтелект й екзистенційний ризик. Чому надрозумний ШІ може нас знищити? [Електронний ресурс]. – Режим доступу: https://vctr.media/ua/agi-superintelekt-j-ekzystenczijnyj-ryzyk-chomu-nadrozumnyj-shi-mozhe-nas-znyshhyty-211551.

2. Карась А. Глобальні виклики і ризики та екзистенціальні загрози. Доповідь на теоретичному семінарі [Електронний ресурс]. – 27.11.2023. – Режим доступу: https://filos.lnu.edu.ua/wp-content/uploads/2015/03/Karas-A.-DOPOVID-NA-TEORSEMINARI-27.11.23.pdf.

3. Russell S. (2022). Artificial Intelligence and the Problem of Control [Electronic resource] / S. Russell // Perspectives on Digital Humanism / Werthner, H., Prem, E., Lee, E.A., Ghezzi, C. (eds). – Springer, Cham. – Accessed mode: https://doi.org/10.1007/ 978-3-030-86144-5\_3.

4. What is black box AI? [Electronic resource]. – Accessed mode: https://www.ibm.com/ think/topics/black-box-ai.

5. Artificial intelligence hitting labour forces like a "tsunami" – IMF Chief [Electronic resource]. – Accessed mode: https://www.reuters.com/technology/artificial-intelligence-hitting-labour-forces-like-tsunami-imf-chief-2024-05-13.

6. The state of AI: How organizations are rewiring to capture value [Electronic resource]. – Accessed mode: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai#/.

7. Войцехівська Ю. Західні експерти розповіли, як штучний інтелект вплине на ринок праці [Електронний ресурс] / Юлія Войцехівська. – Режим доступу: https://glavcom.ua/techno/ hitech/zakhidni-eksperti-rozpovili-jak-shtuchnij-intelekt-vpline-na-rinok-pratsi-1000127.html.

8. Аналітичні матеріали Держспецзв'язку [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua/statics/analitichni-materiali-derzhspeczv-yazku.

9. Cambridge Analytica, компанія в центрі скандалу з Facebook, закривається [Electronic resource]. – Accessed mode: https://www.bbc.com/ukrainian/news-43980978.

10. A Review on Cyber Crimes on the Internet of Things [Electronic resource] / Mohan Krishna Kagita, Navod Thilakarathne, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, Saurabh Singh // Computers and Society. – Accessed mode: https://doi.org/10.48550/arXiv.2009.05708.

11. Base erosion and profit shifting (BEPS) [Electronic resource]. – Accessed mode: https://www.oecd.org/en/topics/policy-issues/base-erosion-and-profit-shifting-beps.html?utm\_source=chatgpt.com.

# 12. Mark Bou Mansour. Losses to OECD tax havens could vaccinate global population three times over, study reveals [Electronic resource] / Mark Bou Mansour. – Accessed mode: https://taxjustice.net/ 2021/11/16/losses-to-oecd-tax-havens-could-vaccinate-global-population-three-times-over-study-reveals/?utm\_source=chatgpt.com.

# 13. Світові стандарти штучного інтелекту [Електронний ресурс]. – Режим доступу: https://sidcon.com.ua/tpost/l31tdcc9f1-svtov-standarti-shtuchnogo-ntelektu.

14. Захист приватних даних в Америках: CCPA, PIPEDA, LGPD [Електронний ресурс]. – Режим доступу: https://legalitgroup.com/ccpa-pipeda-lgpd.

15. Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025-2027 роках : Розпорядження Кабінету Міністрів України від 31 грудня 2024 р. № 1351-р**.**

# References

1. AGI, superintelekt y ekzystentsiinyi ryzyk. Chomu nadrozumnyi ShI mozhe nas znyshchyty? [AGI, superintelligence and existential risk. Why superintelligent AI can destroy us?]. (January 19, 2024). https://vctr.media/ua/agi-superintelekt-j-ekzystenczijnyj-ryzyk-chomu-nadrozumnyj-shi-mozhe-nas-znyshhyty-211551.

2. Karas, A. (27.11.2023). *Globalni vyklyky i ryzyky ta ekzystentsialni zahrozy. Dopovid na teoretychnomu seminari [Global challenges and risks and existential threats. Report at the theoretical seminar]*. https://filos.lnu.edu.ua/wp-content/uploads/2015/03/Karas-A.-DOPOVID-NA-TEORSEMINARI-27.11.23.pdf.

3. Russell, S. (2022). Artificial Intelligence and the Problem of Control. In Werthner, H., Prem, E., Lee, E.A., Ghezzi, C. (Eds.), *Perspectives on Digital Humanism.* Springer, Cham. https://doi.org/10.1007/978-3-030-86144-5\_3.

4. What is black box AI? (n.d.). https://www.ibm.com/think/topics/black-box-ai.

5. Artificial intelligence hitting labour forces like a "tsunami" - IMF Chief. (n.d.). https://www.reuters.com/technology/artificial-intelligence-hitting-labour-forces-like-tsunami-imf-chief-2024-05-13.

6. The state of AI: How organizations are rewiring to capture value (March 12, 2025). https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai#/.

7. Voitsekhivska, Yu. (May 11, 2024). *Zakhidni eksperty rozpovily, yak shtuchnyi intelekt vplyne na rynok pratsi [Western experts told how artificial intelligence will affect the labor market].* https://glavcom.ua/techno/hitech/zakhidni-eksperti-rozpovili-jak-shtuchnij-intelekt-vpline-na-rinok-pratsi-1000127.html.

8. Analitychni materialy Derzhspetszviazku [Analytical materials of the State Service for Special Communications]. (n.d.). https://cip.gov.ua/ua/statics/analitichni-materiali-derzhspeczv-yazku.

9. Cambridge Analytica, kompaniia v tsentri skandalu z Facebook, zakryvaietsia [Cambridge Analytica, the company at the center of the Facebook scandal, is closing down]. (May 2, 2018). https://www.bbc.com/ukrainian/news-43980978.

10. Mohan, Krishna Kagita, Navod, Thilakarathne, Thippa, Reddy Gadekallu, Praveen, Kumar Reddy Maddikunta, Saurabh Singh. (2020). A Review on Cyber Crimes on the Internet of Things. *Computers and Society.* https://doi.org/10.48550/arXiv.2009.05708.

11. Base erosion and profit shifting (BEPS). (n.d.). https://www.oecd.org/en/topics/ policy-issues/base-erosion-and-profit-shifting-beps.html?utm\_source=chatgpt.com.

12. Mark Bou Mansour. (16 November 2021). *Losses to OECD tax havens could vaccinate global population three times over, study reveals*. https://taxjustice.net/ 2021/11/16/losses-to-oecd-tax-havens-could-vaccinate-global-population-three-times-over-study-reveals/?utm\_source=chatgpt.com.

13. Svitovi standarty shtuchnoho intelektu [World standards of artificial intelligence]. (10.09.2024). https://sidcon.com.ua/tpost/l31tdcc9f1-svtov-standarti-shtuchnogo-ntelektu.

14. Zakhyst pryvatnykh dannykh v Amerykakh: CCPA, PIPEDA, LGPD [Protection of private data in the Americas: CCPA, PIPEDA, LGPD]. (07.04.2025). https://legalitgroup.com/ccpa-pipeda-lgpd/

15. Pro skhvalennia Stratehii tsyfrovoho rozvytku innovatsiinoi diialnosti Ukrainy na period do 2030 roku ta zatverdzhennia operatsiinoho planu zakhodiv z yii realizatsii u 2025-2027 rokakh [On approval of the Strategy for the Digital Development of Innovative Activity of Ukraine for the period until 2030 and approval of the operational plan of measures for its implementation in 2025-2027], Resolution of the Cabinet of Ministers of Ukraine dated December 31, 2024 No. 1351-r.

Отримано 19.06.2025

UDC 330.3

JEL Classification: O33

***Yevhenii Kovalenko***

Postgraduate Student of the Department of Economics, Accounting and Taxation

Chernihiv Polytechnic National University (Chernihiv, Ukraine)

**E-mail:** [Rjdfkm1995@gmail.com](mailto:Rjdfkm1995@gmail.com). **ORCID:** <https://orcid.org/0009-0006-4338-6937>

**EXISTENTIAL RISKS AND UNCONTROLLED DIGITAL EVOLUTION**

***Abstract.*** *The article explores the potential existential risks arising from the rapid and uncontrolled digital evolution, which increasingly affects the foundational elements of modern civilization. It analyzes the multilayered and multidimensional impact of digital technologies on economic development, labor markets, public administration, social interactions, political systems, and cultural identities. Digital transformation not only changes communication and production methods but also significantly reshapes power structures, access to resources, regulatory mechanisms, and the distribution of global influence. Among the critical areas of analysis are the development of artificial intelligence, the increasing autonomy of algorithmic decision-making, the automation of labor processes, and mass job displacement across entire industries.*

*The article highlights a broad spectrum of systemic risks, including cybersecurity threats, the growing vulnerability of critical infrastructure, digital fragmentation, and informational dependence. It pays particular attention to the issues of digital isolation, loss of privacy, concentration of digital power in the hands of a few corporations, and the deterioration of democratic institutions due to algorithmic manipulation and misinformation.*

*A separate focus is given to geopolitical aspects of digitalization, including technological sovereignty, competition for control over digital standards, and the potential escalation of international conflicts in the cyber domain. The article examines several scenarios of the digital environment's development, from state surveillance systems to ethically oriented models of human-centered digital governance. Special emphasis is placed on global initiatives to develop legal, ethical, and institutional frameworks that ensure the responsible use of emerging technologies.*

*At the core of this research lies the search for a critical balance between technological progress, humanistic values, sustainable social development, and the security of human existence in the era of digital evolution. The findings and reflections offered in the paper aim to contribute to a deeper understanding of digital transformation not only as an economic and technological process but also as a civilizational challenge requiring coordinated international response.*

***Key words:*** *digital transformation; Existential risks; Artificial intelligence; Cybersecurity; Automation; Digital isolation; Information threats.*

*Fig.: 2. Table: 1. References: 15.*

**Бібліографічний опис для цитування:**

Коваленко Є. М. Екзистенційні ризики та неконтрольована цифрова еволюція. *Науковий вісник Полісся*. 2025. № 1(30). С. 74-86. DOI: https://doi.org/10.25140/2410-9576-2025-1(30)-74-86.