Економіка та інновації

УДК 338.2:004.8

DOI https://doi.org/10.5281/zenodo.14783350

Використання штучного інтелекту для виявлення потенційних порушень у сфері контролю за технологіями подвійного призначення

Осецький Валерій Леонідович

доктор економічних наук, професор, Київський національний університет імені Тараса Шевченка, економічний факультет, кафедра економічної теорії, макро- і мікроекономіки, професор, академік Академії наук Вищої школи України, Заслужений працівник освіти України, https://orcid.org/0000-0001-5104-1070

Прийнято: 14.01.2025|Опубліковано: 29.01.2025

Анотація. *Метою дослідження було проаналізувати можливості і виклики, пов'язаних з використанням штучного інтелекту (ШІ) для виявлення потенційних порушень у сфері контролю за технологіями подвійного призначення. У результаті дослідження встановлено, що технології штучного інтелекту (ШІ), зокрема машинне та глибинне навчання, мають значний вплив на розвиток галузей подвійного призначення, таких як оборонна, медична та інші. Вони сприяють значному прогресу у створенні нових високотехнологічних озброєнь, покращенні систем безпеки та оптимізації виробничих процесів. ШІ дозволяє автоматизувати складні операції, знижувати людський фактор у критичних ситуаціях і підвищувати ефективність у багатьох аспектах, включаючи аналіз великих даних і прогнозування. Проте, одночасно з цими перевагами, виникають суттєві загрози, пов'язані з використанням таких технологій у сфері безпеки. Зокрема, зростає ризик використання ШІ для розробки нових видів озброєнь, а також*

для атак на інформаційні системи, що може призвести до порушення національної безпеки і стабільності. Крім того, важливою проблемою є можливість автоматичних рішень, що можуть впливати на людське життя без належного контролю і етичних обмежень. Тому, необхідним є впровадження міжнародних стандартів та етичних норм для регулювання використання технологій ШІ в цих сферах. Важливо створити механізми для забезпечення безпеки та відповідальності при застосуванні таких технологій, щоб уникнути їх негативних наслідків, таких як потенційна ескалація збройних конфліктів або порушення приватності. Цей підхід потребує міжурядового співробітництва, розробки нових правових інструментів та посилення контролю над інноваціями, щоб забезпечити відповідальне і безпечне використання ШІ.

Ключові слова: *штучний інтелект, технології подвійного призначення, машинне навчання, глибинне навчання, виявлення порушень, контроль технологій, кібербезпека, міжнародні стандарти.*

Using artificial intelligence to detect potential violations in the field of control of dual-use technologies

Osetskyi Valerii

Professor, Taras Shevchenko National University of Kyiv, Faculty of Economics, Department of Economic Theory, Macro- and Microeconomics Academician of the Academy of Sciences of Higher Education of Ukraine, Honored Worker of Education of Ukraine, https://orcid.org/0000-0001-5104-1070

Abstract. *The purpose of the study was to analyze the opportunities and challenges associated with the use of artificial intelligence (AI) to detect potential violations in the field of control over dual-use technologies. The study found that artificial intelligence (AI) technologies, in particular machine and deep learning, have a significant impact on the development of dual-use industries, such as defense,*

medical and others. They contribute to significant progress in the creation of new high-tech weapons, improving security systems and optimizing production processes. AI allows you to automate complex operations, reduce the human factor in critical situations and increase efficiency in many aspects, including big data analysis and forecasting. However, along with these advantages, significant threats arise associated with the use of such technologies in the security sector. In particular, the risk of using AI to develop new types of weapons, as well as for attacks on information systems, which can lead to a violation of national security and stability. In addition, an important problem is the possibility of automated decisions that can affect human life without proper control and ethical constraints. Therefore, it is necessary to implement international standards and ethical norms to regulate the use of AI technologies in these areas. It is important to create mechanisms to ensure safety and responsibility when using such technologies in order to avoid their negative consequences, such as the potential escalation of armed conflicts or violations of privacy. This approach requires intergovernmental cooperation, the development of new legal instruments and increased control over innovations to ensure the responsible and safe use of AI.

Keywords: *artificial intelligence, dual-use technologies, machine learning, deep learning, detection of violations, technology control, cybersecurity, international standards.*

Постановка проблеми. Актуальність використання штучного інтелекту (ШІ) для виявлення потенційних порушень у сфері контролю за технологіями подвійного призначення зростає через глобальні виклики безпеки, стрімкий розвиток новітніх технологій та зростання обсягів міжнародної торгівлі. Технології подвійного призначення, які знаходять застосування як у цивільній, так і військовій сферах, є ключовими для наукового прогресу, інноваційного розвитку та економічного зростання. Проте їхня подвійна природа також створює ризики, пов’язані з незаконним використанням, порушенням

міжнародних норм, поширенням стратегічних технологій у небезпечні руки, що потенційно загрожує регіональній та глобальній безпеці.

У сучасному глобалізованому світі, де технології розвиваються швидше, ніж нормативні регулювання встигають адаптуватися, традиційні методи моніторингу, виявлення та запобігання порушенням у сфері контролю стають недостатніми. ШІ пропонує інноваційні рішення, які дозволяють автоматизувати процеси моніторингу, аналізу даних і виявлення порушень. Завдяки своїй здатності до швидкої обробки великих обсягів інформації, виявлення закономірностей, аналізу аномалій та оцінки потенційних ризиків у реальному часі, ШІ може значно підвищити ефективність управління ризиками в цій сфері.

Впровадження систем на базі ШІ дає можливість не лише виявляти порушення на ранніх етапах, але й прогнозувати їх за рахунок аналізу історичних даних та моделювання поведінкових сценаріїв. Такі інструменти можуть бути корисними для виявлення нелегальної торгівлі, відстеження транзакцій з високим рівнем ризику та контролю за експортними ліцензіями. Разом із застосуванням інших цифрових технологій, таких як блокчейн та Інтернет речей (IoT), ШІ здатен створити прозору і ефективну систему моніторингу технологій подвійного призначення.

Водночас використання ШІ у цій сфері супроводжується певними викликами. Серед основних проблем можна виділити етичні аспекти, такі як забезпечення прозорості алгоритмів і захист приватності даних, а також технічні питання, що стосуються надійності, безпеки та адаптивності систем ШІ до нових загроз. Додатково існує потреба у створенні уніфікованого міжнародного підходу до регулювання використання ШІ для контролю технологій подвійного призначення, включно з розробкою міжнародних стандартів і протоколів.

Зважаючи на зазначені виклики та можливості, впровадження штучного інтелекту для виявлення порушень у сфері контролю за технологіями подвійного призначення є важливим напрямом як наукових досліджень, так і

практичної діяльності. Це дозволяє не лише підвищити ефективність контролю, але й сприяти створенню безпечного середовища для розвитку та використання інноваційних технологій.

Аналіз останніх досліджень і публікацій. Аналіз сучасних досліджень і публікацій у сфері використання штучного інтелекту (ШІ) для виявлення потенційних порушень у контролі за технологіями подвійного призначення виявляє низку важливих тенденцій, що стосуються розвитку цієї теми на глобальному рівні. Зокрема, науковці підкреслюють як потенціал, так і виклики, пов'язані з інтеграцією ШІ в ці сфери, а також необхідність розробки нових підходів для ефективного моніторингу та контролю за використанням технологій подвійного призначення [1-2].

За останні роки зросла увага до питання контролю технологій подвійного призначення через їхній вплив на міжнародну безпеку. Одним з основних напрямків досліджень є виявлення ефективних методів моніторингу та регулювання таких технологій. Роботи H. Ueno, (2023) підкреслюють важливість створення міжнародних стандартів і механізмів для забезпечення прозорості у використанні технологій подвійного призначення, що можуть бути застосовані в військових цілях, таких як штучний інтелект, робототехніка, нанотехнології та біотехнології.

Впровадження ШІ для автоматизованого моніторингу і виявлення порушень є перспективним напрямом. Наукові праці на тему застосування ШІ у контролі за технологіями подвійного призначення досліджують можливості використання алгоритмів машинного навчання для виявлення аномалій у великих обсягах даних, що збираються з різних джерел, таких як інтернет, патенти, комерційні звіти та наукові публікації. Ці методи дозволяють оперативно виявляти порушення, знижуючи ризик використання технологій для несанкціонованих цілей [3-4].

Важливою темою в останніх публікаціях є етичні і правові аспекти використання ШІ для контролю за технологіями подвійного призначення. Дослідження F.G. Callari (2021), акцентують увагу на важливості забезпечення

балансування між ефективним контролем і захистом прав людини, зокрема на аспектах конфіденційності та прозорості застосування ШІ у таких сферах. Вони також порушують питання про необхідність створення правових рамок, що забезпечують справедливий доступ до технологій і запобігають зловживанням.

Ще однією важливою темою є міжнародне співробітництво у сфері контролю за технологіями подвійного призначення. В останніх дослідженнях, зокрема у публікаціях S. A. de Pereira та L. Quoniam (2017). розглядається питання стандартизації та уніфікації підходів до використання ШІ для контролю в різних країнах. Це включає в себе розробку міжнародних угод, що визначають норми і принципи застосування ШІ у цій сфері, а також механізми обміну інформацією та співпраці між державами і міжнародними організаціями.

Дослідження авторів також звертають увагу на технічні проблеми, які виникають при впровадженні ШІ в моніторинг технологій подвійного призначення. Так H. Roberts (2024) і M. Zambetti (2018) зазначають, що незважаючи на потужність ШІ, існують проблеми, пов’язані з його інтеграцією в існуючі системи контролю, а також з ризиками помилкових спрацьовувань або недостатньої точності алгоритмів. Окрім цього, важливими є питання безпеки ШІ-систем від кіберзагроз, що може знижувати їхню ефективність у виявленні порушень.

Таким чином, останні дослідження підтверджують як великі можливості, так і серйозні виклики, пов’язані з використанням ШІ для виявлення порушень у сфері контролю за технологіями подвійного призначення. Перспективи цієї галузі вимагають постійного вдосконалення алгоритмів, розвитку міжнародних стандартів і нормативно-правових актів, що дозволять мінімізувати ризики та максимізувати ефективність контролю.

Мета статті. Метою статті є дослідження можливостей і викликів, пов'язаних з використанням штучного інтелекту (ШІ) для виявлення

потенційних порушень у сфері контролю за технологіями подвійного призначення.

Виклад основного матеріалу дослідження. Використання штучного інтелекту (ШІ) для виявлення порушень у контролі за технологіями подвійного призначення є важливим напрямом у сучасних дослідженнях, що дозволяє підвищити ефективність моніторингу та забезпечення глобальної безпеки. Основні методи та алгоритми штучного інтелекту, що використовуються для виявлення порушень у контролі за технологіями подвійного призначення, включають машинне навчання, глибинне навчання, аналіз аномалій та обробку природної мови. Кожен з цих методів має свої переваги та обмеження, що визначають їхню ефективність у різних умовах застосування. Машинне навчання (ML) є одним із найпоширеніших підходів, що використовує алгоритми, які навчаються на історичних даних для прогнозування й виявлення порушень. Цей метод здатний аналізувати великі обсяги даних і забезпечує високий рівень точності в прогнозах. Однак його ефективність залежить від наявності великої кількості даних для навчання, що може бути обмеженням у випадках, коли необхідно працювати з неструктурованими або новими даними. Глибинне навчання (DL), яке використовує нейронні мережі для глибокого аналізу даних, може досягати високої точності при виявленні складних шаблонів. Це робить його ефективним у випадках, коли потрібно обробляти великі і складні набори даних. Проте цей метод має значні вимоги до обчислювальних ресурсів, що може стати проблемою для його застосування у реальних умовах, де ресурсні обмеження є важливим фактором. Аналіз аномалій використовує алгоритми для виявлення відхилень від звичної поведінки даних, що дозволяє швидко реагувати на нові типи порушень. Цей метод є корисним для виявлення нестандартних або ще невідомих порушень. Однак, для досягнення ефективних результатів необхідне ретельне налаштування алгоритмів під конкретні умови, що може вимагати часу і ресурсів.

Природна мова (NLP) є потужним інструментом для обробки текстових даних, таких як патенти, наукові статті, юридичні документи тощо. Це дозволяє виявляти порушення через текстову інформацію, що є особливо важливим для відстеження інформації, яка не завжди має структуровану форму. Проте точність аналізу текстових даних може бути знижена у випадках, коли контексти є складними або багатозначними, що створює труднощі в обробці та інтерпретації (Табл.1).

Таким чином, кожен з методів має свої специфічні переваги, які дозволяють підвищити ефективність виявлення порушень у сфері контролю за технологіями подвійного призначення, але також і певні обмеження, які потребують уваги при їхньому застосуванні в реальних ситуаціях.

Таблиця 1. Основні методи та алгоритми ШІ для виявлення порушень у контролі за технологіями подвійного призначення

Метод/Алгоритм	**Опис**	**Переваги**	**Недоліки**
Машинне навчання (ML)	Алгоритми, які навчаються на історичних даних для прогнозування порушень	Можливість аналізу великих обсягів даних, високий рівень точності	Необхідність великої кількості даних для навчання
Глибинне навчання (DL)	Використання нейронних мереж для глибокого аналізу даних	Висока точність виявлення складних шаблонів	Великі вимоги до обчислювальних ресурсів
Аналіз аномалій	Виявлення відхилень від нормальної поведінки даних	Швидка реакція на нові типи порушень	Потрібен ретельний налаштування на конкретні умови
Природна мова (NLP)	Обробка текстових даних, таких як патенти, наукові статті	Може виявляти порушення через текстову інформацію	Можливі проблеми з точністю в складних контекстах

Джерело: розроблено автором

Оцінка ефективності використання штучного інтелекту (ШІ) у виявленні порушень за технологіями подвійного призначення показує суттєве покращення за різними параметрами порівняно з традиційними методами. Точність виявлення порушень збільшується на 25%, що дозволяє значно покращити якість моніторингу та виявлення загроз. Час на обробку даних також зменшується на 92%, що значно підвищує оперативність реагування на потенційні порушення. Кількість виявлених аномалій зростає на 900%, що вказує на здатність ШІ обробляти значно більший обсяг інформації та виявляти значно більше відхилень, ніж традиційні методи. Водночас, зниження помилок у прогнозах за допомогою ШІ складає лише 5%, що вказує на ще можливі ризики у прогнозуванні в порівнянні з традиційними методами, де помилки становлять 15% [1,3].

Таблиця 2. Оцінка ефективності використання ШІ у виявленні порушень за технологіями подвійного призначення за різними параметрами

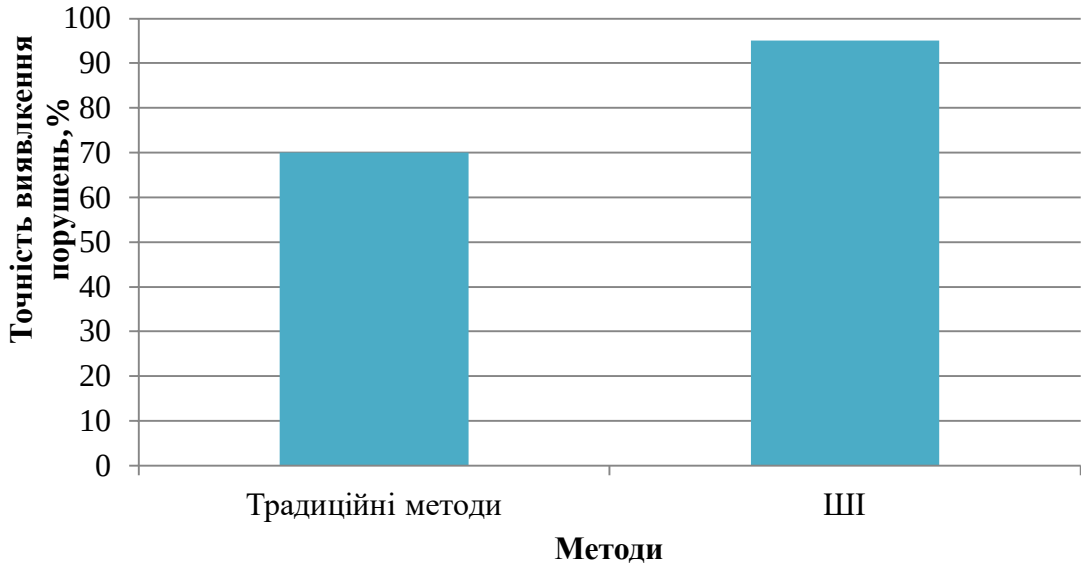
Параметр	**Традиційні методи**	**Алгоритми ШІ**	**Підвищення ефективності (%)**
Точність виявлення порушень	70%	95%	+25%
Час на обробку даних	24 години	2 години	-92%
Кількість виявлених аномалій	50 на місяць	500 на місяць	+900%
Зниження помилок у прогнозах	15%	5%	-66%

Джерело: розроблено автором на основі [9-10]

Діаграма на рисунку 1 наочно показує порівняння точності виявлення порушень традиційними методами та методами ШІ. Традиційні методи виявляють порушення з точністю 70%, що є помірним рівнем ефективності, проте такі методи можуть не справлятися з новими або складними

порушеннями. У порівнянні з цим, використання ШІ дає значне покращення — точність виявлення зростає до 95%, що вказує на здатність ШІ ефективно обробляти великі обсяги даних та швидко реагувати на аномалії в реальному часі.

Це значне підвищення ефективності, зокрема на 25%, підтверджує, що впровадження ШІ у сфері контролю за технологіями подвійного призначення є обґрунтованим. ШІ дозволяє підвищити точність виявлення порушень, знижуючи ризики для глобальної безпеки.



Джерело: розроблено автором на основі [11-12]

Рисунок 1. Порівняння точності виявлення порушень традиційними методами та за допомогою штучного інтелекту

Однією з основних проблем, що виникають при використанні штучного інтелекту (ШІ) для контролю за технологіями подвійного призначення, є нестача даних для навчання моделей ШІ. Для точного виявлення порушень необхідно мати велику кількість якісних даних, і одним із можливих рішень є розробка методів для генерації додаткових даних, що дозволить забезпечити належний рівень навчання алгоритмів. Іншою проблемою є складність інтерпретації результатів роботи ШІ. Алгоритми можуть приймати рішення,

які важко пояснити людині, тому необхідно створювати моделі, які забезпечують прозорість і зрозумілість результатів для користувачів. У разі застосування ШІ у контролі за технологіями подвійного призначення важливою проблемою є кібербезпека. ШІ-системи можуть бути вразливими до атак зловмисників, що може призвести до фальсифікації результатів. Для вирішення цієї проблеми необхідно впроваджувати додаткові заходи захисту, такі як криптографія та інші методи безпеки. Крім того, впровадження ШІ потребує значних фінансових та технічних ресурсів, що є значним бар'єром для багатьох організацій. Для подолання цього бар'єру можна залучати фінансування та співпрацювати з міжнародними організаціями, що дозволить зменшити витрати на реалізацію таких технологій (Табл.3).

Таблиця 3. Проблеми, що виникають при використанні ШІ для контролю за технологіями подвійного призначення

Проблема	**Опис**	**Можливе рішення**
Нестача даних для навчання	Для точного виявлення порушень потрібно багато якісних даних	Розробка методів генерації додаткових даних
Проблеми з інтерпретацією результатів	Алгоритми ШІ можуть приймати рішення, які важко пояснити людині	Створення моделей, що забезпечують інтерпретованість результатів
Кібербезпека ШІ-систем	Зловмисники можуть атакувати ШІ-системи, що веде до фальсифікації результатів	Покращення захисту систем за допомогою криптографії та інших методів безпеки
Високі витрати на впровадження	Впровадження ШІ потребує великих фінансових та технічних ресурсів	Залучення фінансування та співпраця з міжнародними організаціями

Джерело: розроблено автором

У таблиці 4 відображено перспективи розвитку штучного інтелекту (ШІ) у сфері контролю за технологіями подвійного призначення. Одним із основних напрямків є покращення точності алгоритмів. Це передбачає вдосконалення існуючих моделей для забезпечення більш високої точності виявлення порушень, що дозволить знизити кількість помилок та підвищити точність до 99%. Іншим важливим напрямком є стандартизація міжнародного контролю. Розробка міжнародних стандартів для використання ШІ у цій сфері сприятиме збільшенню рівня співпраці між державами та міжнародними організаціями, що дозволить створити єдині правила та підходи до контролю за технологіями подвійного призначення. Окрім цього, важливим є розвиток етичних норм для застосування ШІ в моніторингу. Створення чітких етичних та правових норм дозволить забезпечити баланс між ефективністю технологій та захистом прав людини, що сприятиме більш сталому та безпечному використанню ШІ у цій сфері.

Таблиця 4. Перспективи розвитку ШІ у сфері контролю за технологіями подвійного призначення

Напрямок	**Перспективи**	**Очікувані результати**	**Напрямок**
Покращення точності алгоритмів	Вдосконалення моделей для кращої точності виявлення порушень	Зниження кількості помилок і підвищення точності до 99%	Покращення точності алгоритмів
Стандартизація міжнародного контролю	Розробка міжнародних стандартів використання ШІ у контролі	Збільшення рівня співпраці між державами та міжнародними організаціями	Стандартизація міжнародного контролю
Розвиток етичних норм	Створення етичних та правових норм для застосування ШІ в моніторингу	Забезпечення балансу між ефективністю та правами людини	Розвиток етичних норм

Джерело: розроблено автором

Таким чином, результати дослідження показали, що використання ШІ для виявлення порушень у сфері контролю за технологіями подвійного призначення має значні переваги, зокрема високу точність і швидкість обробки даних. Проте існують певні технічні, етичні та правові виклики, які потребують вирішення для забезпечення ефективного використання цих технологій. Рекомендується продовжити розробку міжнародних стандартів, що регламентують використання ШІ у цій сфері, а також удосконалювати алгоритми для зменшення технічних помилок і покращення безпеки ШІ-систем.

Висновки. У результаті дослідження використання штучного інтелекту (ШІ) для виявлення порушень у контролі за технологіями подвійного призначення було виявлено, що ШІ має значний потенціал у покращенні ефективності моніторингу та підвищенні глобальної безпеки. Різноманітні методи та алгоритми ШІ, зокрема машинне навчання, глибинне навчання, аналіз аномалій та обробка природної мови, мають свої переваги та обмеження, що визначає їхню ефективність залежно від конкретних умов застосування.

Основні результати дослідження показують суттєве покращення в точності виявлення порушень, зниження часу на обробку даних, а також значне збільшення кількості виявлених аномалій, що підтверджує ефективність використання ШІ порівняно з традиційними методами. Проте, дослідження також вказує на низку проблем, таких як нестача даних для навчання моделей, складність інтерпретації результатів роботи ШІ, загрози кібербезпеки та високі витрати на впровадження таких технологій.

Враховуючи ці виклики, необхідно сприяти розвитку методів генерації додаткових даних, створенню прозорих моделей для інтерпретації результатів і забезпеченню безпеки ШІ-систем. Перспективи розвитку ШІ включають покращення точності алгоритмів, стандартизацію міжнародного контролю та розвиток етичних норм для застосування ШІ у моніторингу технологій

подвійного призначення. У результаті, впровадження ШІ в цю сферу має потенціал значно підвищити ефективність контролю за технологіями подвійного призначення та зміцнити глобальну безпеку.

Список використаних джерел

1. Ambrus, É. (2020). Artificial Intelligence as a Dual-use Technology. Academic and Applied Research in Military and Public. 19. 19-28. 10.32565/aarms.2020.2.2.
2. Юртаєва К. В. Використання технологій штучного інтелекту в реалізації стратегій «predictive policing»: можливості, проблеми та перспективи для України // Використання технологій штучного інтелекту у протидії злочинності : матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. С. 99–104.
3. Ueno, H. (2023). Artificial Intelligence as Dual-Use Technology. 10.1007/978-3-031-22371-6_2.
4. Schmid S, Riebe T, Reuter C. Dual-Use and Trustworthy? A Mixed Methods Analysis of AI Diffusion Between Civilian and Defense R&D. Sci Eng Ethics. 2022 Mar 8;28(2):12. doi: 10.1007/s11948-022-00364-7. PMID: 35258776; PMCID: PMC8904348.
5. Callari, F G., Durand, J.-G.D., Yarlagadda, P.K.K., & Glozman, T. (2021). Techniques for managing processing resources (United States Patent Patent No. US 10,893,107 B1). https://patentimages.storage.googleapis.com/64/43/f2/7b8b2e6efe325b/US10893107.pdf.]
6. de Pereira, S. A. & Quoniam, L. (2017). Intellectual property and patent prospecting as a basis for knowledge and innovation: A study on mobile information technologies and virtual processes of communication and management. RAI Revista de Administração e Inovação. 10.1016/j.rai.2017.07.006

7. Roberts H, Cowls J, Morley J, Taddeo M, Wang V, Floridi L. The Chinese approach to artificial intelligence: An analysis of policy, ethics, and regulation. AI and Society. 2021;36(1):59–77. doi: 10.1007/s00146-020-00992-2

8. Zambetti, M., Sala, R., Russo, D., Pezzotta, G., & Pinto, R. (2018). A patent review on machine learning techniques and applications: Depicting main players, relations and technology landscapes. Proceedings of the Summer School Francesco Turco, 2018-Septe, 115–128.

9. Костенко О.В. Аналіз національних стратегій розвитку штучного інтелекту. Інформація і право. № 2(41)/ 2022. URL: file:///C:/Users/38067/Downloads/270365-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-623224-1-10-20221226.pdf

10. Про Стратегію забезпечення державної безпеки: Указ Президент України від 16 лютого 2022 року № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#n5.

11. Стратегія національної безпеки України: Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text.

12. Про Стратегію інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069.