Функціонування і розвиток механізмів державного управління

УДК 352.65:658.8

Дєгтяр Олег Андрійович

доцент, доктор наук з державного управління,

професор кафедри управління та бізнес-адміністрування

Прикарпатський національний університет імені Василя Стефаника

Diegtiar Oleg

Doctor of Science in Public Administration,

Professor of the Department of Management and Business Administration

Vasyl Stefanyk Precarpathian National University

ORCID: 0000-0001-6413-3580

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У ПУБЛІЧНОМУ УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ
USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN PUBLIC MANAGEMENT OF INFORMATION SECURITY

Анотація. *Зростання кількості кіберзагроз та необхідність ефективного контролю за інформаційною безпекою в сучасному світі роблять актуальним питання використання технологій штучного інтелекту в публічному управлінні. На тлі постійного розвитку цифрових технологій та зростання об'ємів даних, такий підхід стає невід'ємною складовою забезпечення інформаційної безпеки. Дослідження спрямоване на аналіз переваг та викликів використання технологій штучного інтелекту в публічному управлінні інформаційною безпекою. Проблема полягає у визначенні ефективних стратегій впровадження штучного інтелекту в системи управління безпекою та вирішенні зв'язаних з цим викликів.Метою дослідження є аналіз переваг та викликів використання технологій штучного інтелекту в сфері публічного управління інформаційною*

безпекою з метою визначення оптимальних підходів до їх впровадження. Об'єктом дослідження є процеси управління інформаційною безпекою в сфері публічного управління, а предметом - використання технологій штучного інтелекту для оптимізації цих процесів. У дослідженні використані методи аналізу та синтезу наукових джерел, включаючи літературний огляд вітчизняної та зарубіжної літератури з питань інформаційної безпеки та технологій штучного інтелекту. Також використані методи системного аналізу для оцінки переваг та викликів використання таких технологій у публічному управлінні. Автор провів аналіз сучасного стану досліджень у галузі використання технологій штучного інтелекту в публічному управлінні інформаційною безпекою, ідентифікувавши ключові переваги та виклики цього підходу. Крім того, були запропоновані конкретні рекомендації щодо ефективного впровадження цих технологій у практику публічного управління. На основі проведеного аналізу автор зробив висновок про значний потенціал використання технологій штучного інтелекту для поліпшення публічного управління інформаційною безпекою. Для успішного впровадження таких технологій рекомендується звернути увагу на питання конфіденційності даних, стійкості моделей та етичних аспектів, а також розвивати спеціалізовані програми та навчальні курси для підготовки кадрів у цій області.

Ключові слова: *публічне управління, механізми публічного управління, інформація, інформаційна безпека, публічне управління інформаційною безпекою, цифрові технології, цифровізація, цифрова трансформація*

Summary. *The growing number of cyber threats and the need for effective control over information security in the modern world make the issue of using artificial intelligence technologies in public administration relevant. Against the background of the constant development of digital technologies and the growth of*

data volumes, this approach becomes an integral component of ensuring information security. The study is aimed at analyzing the advantages and challenges of using artificial intelligence technologies in the public management of information security. The problem is to determine effective strategies for the implementation of artificial intelligence in the security management system and to solve the related challenges. The purpose of the study is to analyze the advantages and challenges of using artificial intelligence technologies in the field of public information security management in order to determine the optimal approaches to their implementation. The object of research is information security management processes in the field of public administration, and the subject is the use of artificial intelligence technologies to optimize these processes. The research uses methods of analysis and synthesis of scientific sources, including a literature review of domestic and foreign literature on information security and artificial intelligence technologies. System analysis methods were also used to assess the advantages and challenges of using such technologies in public administration. The author analyzed the current state of research in the field of using artificial intelligence technologies in the public management of information security, identifying the key advantages and challenges of this approach. In addition, specific recommendations were offered for the effective implementation of these technologies in the practice of public administration. On the basis of the conducted analysis, the author concluded about the significant potential of using artificial intelligence technologies to improve the public management of information security. For the successful implementation of such technologies, it is recommended to pay attention to the issues of data privacy, model stability and ethical aspects, as well as to develop specialized programs and training courses to train personnel in this area.

Key words: *artificial intelligence, public management, information security, mechanisms of public management, information, public management of information security.*

Постановка проблеми. У світі, що швидко змінюється, захист інформації стає все більш актуальною проблемою для публічного управління. Зростаючі кіберзагрози, такі як кібератаки, витік даних і шкідливі програми, ставлять під загрозу інформаційну безпеку у всіх сферах життя, включаючи державні установи. У такому контексті використання технологій штучного інтелекту (ШІ) з'являється як потенційний рішення проблеми забезпечення інформаційної безпеки в публічному управлінні.

Гіпотеза цього дослідження полягає в тому, що впровадження технологій штучного інтелекту у публічне управління інформаційною безпекою може призвести до підвищення ефективності виявлення, аналізу та реагування на кіберзагрози, а також до зменшення ризику порушень безпеки даних. Однак, використання ШІ також вносить свої виклики та обмеження, які потребують уважного вивчення та аналізу.

Статистичні дані свідчать про зростання кількості кібератак у всьому світі. За даними звіту Центру Національної Кібербезпеки 2023 року, кількість кібератак на урядові установи зросла на 25% порівняно з попереднім роком. Також зазначено, що понад 60% цих атак були спрямовані на викрадення конфіденційної інформації.

Отже, використання технологій штучного інтелекту у публічному управлінні інформаційною безпекою стає важливою стратегією для забезпечення захисту від кіберзагроз. Проте перед цим виникають певні виклики, такі як забезпечення конфіденційності даних та стійкості моделей ШІ. Дане дослідження спрямоване на аналіз цих проблем та надання рекомендацій для практичного впровадження технологій ШІ у публічному управлінні інформаційною безпекою.

Аналіз літературних джерел. Наукова література з тематикою дослідження широко розглядає можливості та перспективи застосування ШІ в контексті забезпечення безпеки та захисту інформації в державному секторі. Дослідники Запорожець Т.В., Осьмак А., Карпенко Ю., Семененко

І., Карпенко О. В., Карпенко Ю. В., Максіменцева Н. О., Максіменцев М. Г., Вішвакарма Л.П. та Сінгх Р.К., Ішенгома Ф. Р., Шао Д., Алексопулос К., Саксена С. та Нікіфорова А., Halagatti M., Gadag S., Mahantshetti S., Hiremath C.V., Tharkude D. and Banakar V., Алмхейрі Х.М., Ахмад С.З., Абу Бакар А.Р. і Халід К., Нзобонімпа С., Кріадо Я.І. і Гіл-Гарсія Дж.Р., Магиляс Ю., Корсун В. та Миргородська М., Яровой, Т. С. [1-12] вказують на те, що системи штучного інтелекту, включаючи методи машинного навчання та аналізу даних, можуть допомогти виявляти та протидіяти кіберзагрозам швидше та ефективніше, забезпечуючи високий рівень захисту інформації. Крім того, літературні джерела наголошують на важливості врахування етичних аспектів та забезпечення конфіденційності даних під час впровадження та використання ШІ в публічному управлінні, що вимагає комплексного підходу до розробки та реалізації таких систем.

Мета та завдання статті. Стаття спрямована на дослідження переваг та викликів використання технологій штучного інтелекту в публічному управлінні інформаційною безпекою. Головною метою є вивчення можливостей використання штучного інтелекту для підвищення ефективності виявлення та аналізу кіберзагроз, а також ідентифікації та вирішення проблем, що виникають при такому використанні. Основні завдання статті:

– провести огляд та аналіз сучасних методів та технологій штучного інтелекту, які можуть бути застосовані в публічному управлінні інформаційною безпекою;

– проаналізувати переваги використання технологій штучного інтелекту, таких як підвищена ефективність виявлення кіберзагроз, автоматизація процесів аналізу та реагування, і підготувати відповідні висновки;

– виявити основні виклики та обмеження, пов'язані з використанням технологій штучного інтелекту в сфері публічного управління

інформаційною безпекою, такі як проблеми конфіденційності, ризики стійкості моделей та етичні питання;

– на основі отриманих результатів надати рекомендації щодо практичного впровадження технологій штучного інтелекту в публічне управління інформаційною безпекою та зменшення впливу виявлених викликів.

Виклад основного матеріалу. Штучний інтелект (ШІ) швидко стає ключовим інструментом у багатьох галузях, включаючи публічне управління, де він відкриває нові можливості для покращення ефективності та безпеки процесів. Використання ШІ у публічному управлінні інформаційною безпекою стає особливо важливим, оскільки державні установи мають великий обсяг конфіденційної інформації, яка потребує захисту від кіберзагроз.

Один із найважливіших методів ШІ, що застосовується в публічному управлінні інформаційною безпекою, - це машинне навчання. Цей метод дозволяє алгоритмам самостійно вивчати та аналізувати великі обсяги даних, шукати в них патерни та здійснювати прогнози. В контексті інформаційної безпеки, машинне навчання може бути використане для виявлення аномальних патернів в мережевому трафіку, ідентифікації атак та виявлення незвичайних змін в системах [1].

Інший метод ШІ, який застосовується в публічному управлінні інформаційною безпекою, – це обробка природної мови (Natural Language Processing, NLP). За допомогою NLP можна аналізувати текстову інформацію з різних джерел, включаючи листування, заяви та звіти, для виявлення підозрілих патернів або загроз.

Технологія аналізу поведінки користувачів (User Behavior Analytics, UBA) також стає дедалі популярнішою в публічному управлінні. Вона дозволяє виявляти незвичайні дії або активності користувачів, що можуть вказувати на потенційні загрози безпеці. UBA базується на аналізі великих

обсягів даних про користувачів, включаючи їхню звичну поведінку та зв'язки між ними [2].

Крім того, технологія автоматизації відкриває можливості для автоматизації процесів управління інформаційною безпекою. Наприклад, застосування автоматичних систем виявлення та реагування на кібератаки дозволяє значно зменшити час реакції на загрози та мінімізувати ризик помилок від людського фактору [3].

Однак, на шляху до впровадження технологій ШІ в публічне управління інформаційною безпекою стоять певні виклики. Наприклад, збір та обробка великих обсягів даних може породжувати проблеми конфіденційності та приватності. Крім того, важливо враховувати можливість помилок та нестійкість моделей, а також виклики етичного характеру, пов'язані з використанням ШІ у контексті збору та обробки даних про громадян.

Загалом, технології штучного інтелекту мають великий потенціал для підвищення рівня інформаційної безпеки в публічному управлінні. Проте їх впровадження потребує уваги до вирішення викликів, які можуть виникнути під час процесу імплементації та експлуатації.

В сучасному цифровому світі, де кіберзагрози стають все більш складними та руйнівними, використання технологій штучного інтелекту (ШІ) в публічному управлінні інформаційною безпекою визнається ключовим елементом захисту від кібератак та зловживань. Огляд сучасних методів і технологій ШІ демонструє, що вони проникають у різні аспекти управління інформаційною безпекою, починаючи від виявлення загроз і закінчуючи реагуванням на інциденти [4].

Однією з переваг використання технологій ШІ є підвищена ефективність виявлення кіберзагроз. Алгоритми машинного навчання та аналізу великих обсягів даних дозволяють автоматично виявляти незвичайні та підозрілі активності, що може вказувати на потенційні

загрози. Наприклад, системи навчаються розпізнавати аномальні патерни в мережевому трафіку або надзвичайні дії в корпоративних системах, що дозволяє оперативно реагувати на можливі загрози.

Крім того, автоматизація процесів аналізу та реагування є ще однією важливою перевагою використання ШІ. Технології машинного навчання можуть автоматично аналізувати великі обсяги даних та приймати рішення на основі певних критеріїв. Наприклад, системи можуть автоматично визначати рівень серйозності інциденту та приймати рекомендації щодо його подальшого реагування, зменшуючи час, який витрачається на аналіз та прийняття рішень людськими операторами [5].

Аналіз переваг використання технологій ШІ в публічному управлінні інформаційною безпекою демонструє, що вони можуть значно підвищити швидкість та точність реагування на кіберзагрози, що в свою чергу зменшує ризик негативних наслідків для систем і даних. Автоматизація процесів також може звільнити людські ресурси та зробити управління інформаційною безпекою більш ефективним та відповідальним [6].

Використання технологій штучного інтелекту в публічному управлінні інформаційною безпекою стикається з рядом викликів та обмежень, які необхідно ураховувати для забезпечення ефективності та етичності цього процесу. Представлена таблиця 1 висвітлює основні виклики та обмеження, пов'язані з використанням технологій штучного інтелекту в сфері публічного управління інформаційною безпекою. Забезпечення конфіденційності, стійкості моделей та вирішення етичних питань виявляються ключовими аспектами, які вимагають уваги та вирішення для успішного впровадження технологій ШІ.

Таблиця 1

Основні виклики та обмеження, пов'язані з використанням технологій штучного інтелекту в сфері публічного управління інформаційною безпекою

Виклик / Обмеження	Опис	Висновок
Проблеми конфіденційності	Технології штучного інтелекту можуть потребувати доступу до великих обсягів даних, що може порушити конфіденційність особистої інформації.	Забезпечення конфіденційності даних має високий пріоритет і вимагає ретельної уваги та заходів захисту з боку організацій, що використовують технології ШІ.
Ризики стійкості моделей	Моделі штучного інтелекту можуть бути вразливі до атак, змін та впливів, що може призвести до непередбачуваних результатів та помилок.	Забезпечення стійкості та надійності моделей штучного інтелекту вимагає постійного моніторингу, тестування та застосування заходів безпеки для запобігання небажаним впливам та атакам.
Етичні питання	Використання штучного інтелекту в публічному управлінні може викликати етичні дилеми, такі як вплив на приватність, або вирішення важливих соціальних питань.	Забезпечення етичного використання технологій штучного інтелекту вимагає обговорення та розробки відповідних нормативно-правових актів та стандартів, що враховують питання приватності, справедливості та довіри громадськості.

Джерело: узагальнено авторами на основі [7; 8]

Урахування цих викликів та обмежень є важливим для розробки ефективних та етичних стратегій використання технологій штучного інтелекту в публічному управлінні інформаційною безпекою. Тільки шляхом врахування цих аспектів можна забезпечити максимальну користь від використання ШІ, уникнути можливих негативних наслідків та забезпечити дотримання принципів правопорядку та етики.

Впровадження технологій штучного інтелекту у сферу публічного управління інформаційною безпекою вносить ряд викликів та обмежень, які потребують уважного розгляду та вирішення.

Одним із найважливіших викликів є проблеми конфіденційності. Використання технологій ШІ передбачає обробку великих обсягів даних, часто чутливої за природою. Це може викликати занепокоєння з приводу можливості порушення конфіденційності особистої інформації, тому необхідно ретельно розробляти та впроваджувати заходи захисту даних [9].

Ще одним важливим викликом є ризики стійкості моделей ШІ. Технології штучного інтелекту можуть бути вразливі до атак, зловживань та непередбачених ситуацій. Неправильно розроблені чи недостатньо адаптовані моделі можуть призвести до негативних наслідків, включаючи помилкові рішення та порушення безпеки. Тому необхідно постійно перевіряти та вдосконалювати алгоритми та моделі на предмет їхньої стійкості та надійності [10].

Також слід звернути увагу на етичні питання, пов'язані з використанням ШІ в публічному управлінні інформаційною безпекою. Враховуючи потенціал впливу технологій на суспільство та індивідів, важливо дотримуватися принципів етики та забезпечити відповідність з правовими нормами та стандартами [11].

Отже, для практичного впровадження технологій штучного інтелекту в публічне управління інформаційною безпекою рекомендується:

1. Ретельно аналізувати та оцінювати потенційні ризики та виклики, пов'язані з використанням ШІ.
2. Розробляти та впроваджувати ефективні заходи захисту даних та забезпечення конфіденційності.
3. Постійно вдосконалювати та перевіряти алгоритми та моделі ШІ на стійкість та надійність.

4. Дотримуватися етичних принципів та законодавчих вимог у використанні технологій ШІ, забезпечуючи високий рівень відповідності з правовими стандартами [12].

Висновки та пропозиції. У висновку до статті про використання технологій штучного інтелекту у публічному управлінні інформаційною безпекою важливо підкреслити значущість та потенціал цих технологій у підвищенні ефективності та надійності систем захисту від кіберзагроз.

Перш за все, використання ШІ дозволяє швидко виявляти та аналізувати кіберзагрози, що дозволяє здійснювати ефективні заходи протидії. Автоматизація процесів аналізу та реагування значно збільшує швидкість реакції на можливі загрози, зменшуючи час на виявлення та вирішення інцидентів.

Проте, варто враховувати, що впровадження технологій ШІ також вносить свої виклики та обмеження. Проблеми конфіденційності, ризики стійкості моделей та етичні питання потребують уважного вивчення та врахування під час розробки та впровадження систем інформаційної безпеки на основі ШІ.

Загалом, висновки свідчать про потенціал та перспективи використання технологій штучного інтелекту в публічному управлінні інформаційною безпекою. Правильне та обережне впровадження цих технологій може сприяти підвищенню рівня захисту даних та систем у сфері публічного управління. Однак необхідно бути уважними до можливих ризиків та вживати відповідних заходів для їх управління, забезпечуючи збалансований підхід до використання ШІ в публічному секторі.

Література

1. Запорожець Т.В. Застосування інтелектуальних технологій та систем штучного інтелекту для підтримки прийняття управлінських рішень. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне*

управління. 2020. Т. 31(70), № 2. С. 79-85. doi: https://doi.org/10.32838/2663-6468/2020.2/13.

2. Осьмак А., Карпенко Ю., Семененко І. Використання інструментів штучного інтелекту в мережевому управлінні: переваги, ризики та розвиток. *Аспекти публічного управління*. 2023. 11(3). С. 38-42. doi: https://doi.org/10.15421/152333.
3. Карпенко О. В., Карпенко Ю. В. Штучний інтелект як інструмент публічного управління соціально-економічним розвитком: смарт-інфраструктура, цифрові системи бізнес-аналітики та трансферти. *Державне управління: удосконалення та розвиток*. 2021. № 10. doi: https://doi.org/10.32702/2307-2156-2021.10.2; URL: http://www.dy.nayka.com.ua/?op=1&z=2257 (дата звернення: 19.03.2024).
4. Максіменцева Н. О., Максіменцев М. Г. Штучний інтелект у публічному управлінні: переваги цифрових технологій та загрози суверенному інформаційному простору. *Державне управління: удосконалення та розвиток*. 2024. № 2. doi: https://doi.org/10.32702/2307-2156.2024.2.7.
5. Vishwakarma L.P., Singh R.K. An Analysis of the Challenges to Human Resource in Implementing Artificial Intelligence. Tyagi, P., Chilamkurti, N., Grima, S., Sood, K. and Balusamy, B. (Ed.). *The Adoption and Effect of Artificial Intelligence on Human Resources Management, Part B (Emerald Studies in Finance, Insurance, and Risk Management)*. Emerald Publishing Limited, Leeds. 2023. P. 81-109. doi: https://doi.org/10.1108/978-1-80455-662-720230006.
6. Ishengoma F.R., Shao D., Alexopoulos C., Saxena S., Nikiforova A. (), Integration of artificial intelligence of things (AIoT) in the public sector: drivers, barriers and future research agenda. *Digital Policy, Regulation and*

Governance. 2022. Vol. 24, No. 5. P. 449-462. doi: https://doi.org/10.1108/DPRG-06-2022-0067.

7. Halagatti M., Gadag S., Mahantshetti S., Hiremath C.V., Tharkude D., Banakar V. Artificial Intelligence: The New Tool of Disruption in Educational Performance Assessment. Tyagi, P., Grima, S., Sood, K., Balamurugan, B., Özen, E. and Eleftherios, T. (Ed.). *Smart Analytics, Artificial Intelligence and Sustainable Performance Management in a Global Digitalised Economy (Contemporary Studies in Economic and Financial Analysis, Vol. 110A).* Emerald Publishing Limited, Leeds. 2023. P. 261-287. doi: https://doi.org/10.1108/S1569-37592023000110A014.
8. Almheiri H.M., Ahmad S.Z., Abu Bakar A.R., Khalid K. Artificial intelligence capabilities, dynamic capabilities and organizational creativity: contributing factors to the United Arab Emirates Government's organizational performance. *Journal of Modelling in Management*. 2024. Vol. 19, No. 3. P. 953-979. doi: https://doi.org/10.1108/JM2-11-2022-0272.
9. Nzobonimpa S. Artificial intelligence, task complexity and uncertainty: analyzing the advantages and disadvantages of using algorithms in public service delivery under public administration theories. *Digital Transformation and Society*. 2023. Vol. 2, No. 3. P. 219-234. doi: https://doi.org/10.1108/DTS-03-2023-0018.
10. Criado J.I., Gil-Garcia J.R. Creating public value through smart technologies and strategies: From digital services to artificial intelligence and beyond. *International Journal of Public Sector Management*. 2019. Vol. 32, No. 5. P. 438-450. doi: https://doi.org/10.1108/IJPSM-07-2019-0178.
11. Магиляс Ю., Корсун В., Миргородська М. Пріоритетні напрямки впровадження штучного інтелекту в публічне управління. *Аспекти публічного управління*. 2023. Вип. 11(4). С. 97-103. doi: https://doi.org/10.15421/152358.

12. Яровой Т. С. Можливості та ризики використання штучного інтелекту в публічному управлінні. *Economic Synergy*. 2023. Вип. 2. С. 36–47. doi: https://doi.org/10.53920/ES-2023-2-3

References

1. Zaporozhets, T.V. (2020). Zastosuvannya intelektual′nykh tekhnolohiy ta systemy shtuchnoho intelektu dlya pidtrymky pryynyattya upravlins′kykh rishen′ [Application of intelligent technologies and artificial intelligence systems to support management decision-making]. *Vcheni zapysky TNU imeni V.I. Vernads'koho. Seriya: Derzhavne upravlinnya – Academic notes of TNU named after V.I. Vernadskyi. Series: Public administration, 31*(70), 2, 79-85. doi: https://doi.org/10.32838/2663-6468/2020.2/13 [in Ukrainian].
2. Os′mak, A., Karpenko, Yu., & Semenenko, I. (2023). Vykorystannya instrumentiv shtuchnoho intelektu v merezhevomu upravlinni: perevahy, ryzyky ta rozvytok [Use of artificial intelligence tools in network management: advantages, risks and development]. *Aspekty publichnoho upravlinnya – Aspects of public administration, 11*(3), 38-42. doi: https://doi.org/10.15421/152333 [in Ukrainian].
3. Karpenko, O . V., & Karpenko, Yu. V. (2021). Shtuchnyy intelekt yak instrument publichnoho upravlinnya sotsial′no-ekonomichnym rozvytkom: smart-infrastruktura, tsyfrovi systemy biznes-analityky ta transferty [Artificial intelligence as a tool of public management of socio-economic development: smart infrastructure, digital systems of business analytics and transfers]. *Derzhavne upravlinnya: udoskonalennya ta rozvytok – Public administration: improvement and development, 10*. doi: https://doi.org/10.32702/2307-2156-2021.10.2; Retrieved from http://www.dy.nayka.com.ua/?op=1&z=2257 [in Ukrainian].
4. Maksymentseva, N. O., & Maksymentsev, M. H. (2024). Shtuchnyy intelekt u publichnomu upravlinni: perevahy tsyfrovykh tekhnolohiy ta zahrozy

suverennomu informatsiynomu prostoru [Artificial intelligence in public administration: advantages of digital technologies and threats to the sovereign information space]. *Derzhavne upravlinnya: udoskonalennya ta rozvytok – Public administration: improvement and development, 2*. doi: https://doi.org/10.32702/2307-2156.2024.2.7 [in Ukrainian].

5. Vishwakarma, L.P., & Singh, R.K. (2023). An Analysis of the Challenges to Human Resource in Implementing Artificial Intelligence. Tyagi, P., Chilamkurti, N., Grima, S., Sood, K., & Balusamy, B. (Ed.). *The Adoption and Effect of Artificial Intelligence on Human Resources Management, Part B (Emerald Studies in Finance, Insurance, and Risk Management)*. Emerald Publishing Limited, Leeds, 81-109. doi: https://doi.org/10.1108/978-1-80455-662-720230006.
6. Ishengoma, F.R., Shao, D., Alexopoulos, C., Saxena, S., & Nikiforova, A. (2022). Integration of artificial intelligence of things (AIoT) in the public sector: drivers, barriers and future research agenda. *Digital Policy, Regulation and Governance, 24*(5), 449-462. doi: https://doi.org/10.1108/DPRG-06-2022-0067.
7. Halagatti, M., Gadag, S., Mahantshetti, S., Hiremath, C.V., Tharkude, D., Banakar, V. (2023). Artificial Intelligence: The New Tool of Disruption in Educational Performance Assessment. Tyagi, P., Grima, S., Sood, K., Balamurugan, B., Özen, E. and Eleftherios, T. (Ed.). *Smart Analytics, Artificial Intelligence and Sustainable Performance Management in a Global Digitalised Economy (Contemporary Studies in Economic and Financial Analysis, Vol. 110A)*. Emerald Publishing Limited, Leeds, 261-287. doi: https://doi.org/10.1108/S1569-37592023000110A014.
8. Almheiri, H.M., Ahmad, S.Z., Abu Bakar, A.R., & Khalid, K. (2024). Artificial intelligence capabilities, dynamic capabilities and organizational creativity: contributing factors to the United Arab Emirates Government's

organizational performance. *Journal of Modelling in Management, 19* (3), 953-979. doi: https://doi.org/10.1108/JM2-11-2022-0272.

9. Nzobonimpa, S. (2023). Artificial intelligence, task complexity and uncertainty: analyzing the advantages and disadvantages of using algorithms in public service delivery under public administration theories. *Digital Transformation and Society, 2* (3), 219-234. doi: https://doi.org/10.1108/DTS-03-2023-0018.
10. Criado, J.I., & Gil-Garcia, J.R. (2019). Creating public value through smart technologies and strategies: From digital services to artificial intelligence and beyond. *International Journal of Public Sector Management, 32* (5), 438-450. doi: https://doi.org/10.1108/IJPSM-07-2019-0178.
11. Mahylyas, Yu., Korsun, V., & Myrhorods'ka, M. (2023). Priorytetni napryamky vprovadzhennya shtuchnoho intelektu v publichne upravlinnya [Priority areas of introduction of artificial intelligence in public administration]. *Aspekty publichnoho upravlinnya – Aspects of public administration, 11*(4), 97-103. doi: https://doi.org/10.15421/152358 [in Ukrainian].
12. Yarovoy, T . S. (2023). Mozhlyvosti ta ryzyky vykorystannya shtuchnoho intelektu v publichnomu upravlinni [Opportunities and risks of using artificial intelligence in public administration]. *Economic Synergy, 2,* 36–47. doi: https://doi.org/10.53920/ES-2023-2-3 [in Ukrainian]