УДК: 35:004.8:351.862 *DOI: https://doi.org/10.32631/vca.2025.2.82*

Віктор Михайлович ВАСИЛЕНКО,
доктор юридичних наук, доцент
(Харківський національний університет внутрішніх справ, м. Харків)

ІНТЕГРАЦІЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ В ДЕРЖАВНЕ УПРАВЛІННЯ: РИЗИКИ, ПРАВОВІ ВИКЛИКИ ТА БЕЗПЕКОВІ ГАРАНТІЇ

У статті здійснено комплексний аналіз інтеграції систем штучного інтелекту у сферу державного управління з урахуванням сучасних трансформацій публічного сектору та зростання технологічної залежності інституцій влади від алгоритмічних рішень. Розкрито теоретичні та концептуальні засади використання інтелектуальних технологій у діяльності органів державної влади, окреслено ключові ризики, що виникають внаслідок алгоритмічної автономності, непрозорості та потенційних помилок в ухваленні управлінських рішень. Особливу увагу приділено правовим викликам, пов'язаним із визначенням відповідальності за функціонування та наслідки застосування систем штучного інтелекту, захистом персональних даних, забезпеченням прав людини та необхідністю гармонізації національного законодавства зі стандартами Європейського Союзу. Проаналізовано безпекові аспекти впровадження інтелектуальних технологій, зокрема загрози кібербезпеці, ризики зовнішнього втручання, маніпулювання даними та залежність від іноземних технологічних платформ. Обґрунтовано необхідність формування цілісної системи правових та організаційних гарантій, спрямованих на забезпечення прозорості, підзвітності та безпечної роботи інтелектуальних систем у державному секторі. Результати дослідження можуть бути використані для розроблення національної моделі регулювання штучного інтелекту та удосконалення стратегій цифрової трансформації України.

Ключові слова: *штучний інтелект, державне управління, правові виклики, алгоритмічна безпека, цифрова трансформація, публічна політика, кібербезпека, алгоритмічна підзвітність.*

Постановка проблеми. Стрімке впровадження систем штучного інтелекту в державне управління створює одночасно нові можливості та

комплекс викликів, що безпосередньо впливають на якість, прозорість і безпеку публічних рішень. Алгоритмічні технології дедалі глибше інтегруються у процеси прогнозування, надання адміністративних послуг, розподілу ресурсів і підтримки управлінських рішень, що формує залежність державних інституцій від цифрових інструментів. Проте зростання цієї залежності супроводжується появою ризиків, пов'язаних із непрозорістю алгоритмів, ймовірністю технічних збоїв, можливістю маніпулювання даними та складністю контролю за функціонуванням автономних систем. Проблема ускладнюється тим, що нормативно-правове регулювання в більшості країн, зокрема й в Україні, не встигає за темпами технологічного розвитку. Відсутність чітко визначених стандартів відповідальності та механізмів підзвітності створює правові прогалини, які можуть призвести до порушення прав громадян, дискримінаційних рішень або неналежної обробки персональних даних. У сучасних умовах національної безпеки особливу загрозу становить можливість зовнішнього впливу на інтелектуальні системи, їх використання для перекручування інформації, втручання у цифрову інфраструктуру чи ослаблення стійкості державного управління. Крім того, державні органи часто не мають достатнього кадрового та технічного потенціалу для оцінки ризиків, проведення аудиту алгоритмів та контролю за життєвим циклом систем штучного інтелекту. Відсутність таких спроможностей унеможливлює формування належної політики безпеки, що враховує швидку зміну технологічних загроз і зростання обсягів критично важливих даних. Сутність проблеми полягає в необхідності поєднання цифрової модернізації держави з формуванням ефективної системи правових, організаційних та безпекових гарантій, здатних забезпечити відповідальне, контрольоване та безпечне функціонування штучного інтелекту в публічному секторі. Її вирішення потребує міждисциплінарного підходу, адаптації законодавства до сучасних технологічних реалій, а також розвитку інституційної спроможності держави щодо управління ризиками та захисту національних інтересів у цифровому середовищі.

Питання використання систем штучного інтелекту (далі – ШІ) у державному управлінні активно досліджується як у міжнародній, так і у вітчизняній науковій літературі. Низка праць присвячена проблемам етичного застосування інтелектуальних технологій, ризикам алгоритмічної непрозорості та формуванню принципів відповідального використання ШІ в публічному секторі. Однією з фундаментальних робіт у цій сфері є праці Л. Флоріді, у яких автор обґрунтовує концепцію етичної рамки ШІ та необхідність формування принципів підзвітності, прозорості та контролю при впровадженні інтелектуальних систем у суспільно важливі процеси[1]. Подібні підходи розвиває Дж. Брісон, наголошуючи на ризиках відтворення соціальних упереджень алгоритмами та необхідності незалежного аудиту

[1] Floridi L., Cowls J. A Unified Framework of Five Principles for AI in Society. *Harvard Data Science Review*. 2019. Iss. 1.1. DOI: https://doi.org/10.1162/99608f92.8cd550d1.

технологій, які використовують державні інституції[1]. Значний внесок у вивчення проблем алгоритмічної підзвітності зробив Ф. Паскуале, який досліджує феномен «чорних скриньок» та наголошує на загрозі, що виникає при застосуванні непрозорих автоматизованих систем у соціально чутливих сферах[2]. Важливий напрям сучасних досліджень також сформований роботами С. Вахтер та Б. Міттельштадта, які аналізують правові аспекти автоматизованого ухвалення рішень у контексті захисту прав людини та підкреслюють необхідність гарантій права на пояснення результатів роботи алгоритмів[3]. Українські дослідники активно вивчають процеси цифрової трансформації публічного сектору та виклики, пов'язані з інтеграцією інтелектуальних технологій у діяльність органів влади. Так, Н. Сорокіна розглядає теоретичні основи цифровізації державного управління, акцентуючи увагу на залежності ефективності цифрових інновацій від рівня інституційної спроможності органів влади та їхньої готовності до роботи з новими технологіями[4]. У дослідженні В. Кучменка та М. Ватульєва проаналізовано специфіку цифрової трансформації у період воєнного стану, визначено ризики, пов'язані з використанням інформаційних систем, та окреслено потребу в посиленні кіберзахисту у структурах державного управління[5].

Проблематика цифрового розвитку публічного управління також висвітлена у дослідженні В. Євдокимова і С. Коломійця, які акцентують увагу на необхідності структурної модернізації державних інституцій, гармонізації національного законодавства з європейськими стандартами та впровадженні принципів відкритості та підзвітності при використанні ШІ у публічних процесах[6]. Окремий дослідницький напрям становлять міжнародні аналітичні матеріали Організації економічного співробітництва та розвитку (далі – OECD), де подано системний набір принципів відповідального застосування ШІ у державному секторі та запропоновано інструменти оцінювання ризиків високого рівня у технологічних системах[7]. Європейські дослідження щодо регуляторної межі Закону про штучний інтелект (Artificial Intelligence Act) також визначають підходи до оцінювання безпеки, інституційної відповідальності та контролю за застосуванням ШІ у

[1] Bryson J. The Past Decade and Future of AI's Impact on Society. ACM Computing Surveys, 2019. 35 p. URL: https://static1.squarespace.com/static/5e13e4b93175437bccfc4545/t/67057b00d95cad198c5575da/1728412417139/the-past-decade-and-future-of-ai-impact-on-society-bbva.pdf

[2] Pasquale F. The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press, 2015. 260 p. // JSTOR: сайт. URL: https://www.jstor.org/stable/j.ctt13x0hch

[3] Wachter S., Mittelstadt B., Floridi L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*. 2017. Vol. 7, Iss. 2. Pp. 76–99. DOI: https://doi.org/10.1093/idpl/ipx005

[4] Сорокіна Н. Цифровізація публічного управління в Україні: теоретичний аспект. *Аспекти публічного управління*. 2021. Т. 13, № 1. С. 77–81. DOI: https://doi.org/10.15421/152509.

[5] Кучменко В., Ватульєв М. Цифрова трансформація публічного управління в умовах воєнного стану. *Молодий вчений*. 2025. № 4 (135). DOI: https://doi.org/10.32839/2304-5809/2025-4-135-14

[6] Євдокимов В., Коломієць С. Цифрова трансформація публічного управління в Україні: виклики та перспективи. *Актуальні питання у сучасній науці. Серія «Державне управління»*. 2024. № 9 (27). С. 403–415. DOI: https://doi.org/10.52058/2786-6300-2024-9(27)-403-415

[7] Artificial Intelligence in Society // OECD: сайт. 11.06.2019. DOI: https://doi.org/10.1787/eedfee77-en.

державному управлінні[1].

Таким чином, наявні наукові праці формують широку академічну базу щодо етичних, правових та інституційних аспектів впровадження ШІ. Водночас комплексний аналіз взаємозв'язку безпекових, правових та управлінських чинників у процесі інтеграції ШІ в державний сектор у контексті українських реалій потребує подальшого теоретичного й практичного опрацювання.

Метою статті є комплексне дослідження процесів інтеграції систем ШІ в державне управління з акцентом на виявленні основних ризиків, правових викликів та безпекових загроз, що супроводжують використання інтелектуальних технологій у публічному секторі. У межах цієї мети передбачається проаналізувати теоретичні та нормативні підходи до регулювання ШІ, оцінити сучасний стан технологічної трансформації державного управління, а також визначити напрями формування ефективної системи правових і організаційних гарантій, здатних забезпечити відповідальне та безпечне застосування ШІ в умовах цифрової модернізації України.

Виклад основного матеріалу. Стрімке поширення технологій ШІ стало одним із ключових чинників трансформації сучасних систем державного управління. Інтелектуальні алгоритми дедалі частіше застосовуються для аналізу великих масивів даних, прогнозування суспільних процесів, оптимізації адміністративних процедур та підтримки управлінських рішень. Наведена інтеграція відкриває нові можливості для підвищення ефективності роботи державних інституцій, розширення їхніх аналітичних спроможностей та удосконалення взаємодії з громадянами. Водночас широке впровадження ШІ формує складний комплекс викликів, що стосується як правових аспектів, так і питань прозорості, довіри та безпеки. Цифрова трансформація державного сектору супроводжується зростанням залежності управлінських рішень від алгоритмічних інструментів, які, попри високу функціональність, можуть містити помилки, упередження або вразливості. Застосування таких систем у сферах, що безпосередньо впливають на права та свободи громадян, вимагає не лише технологічної модернізації, а й формування нових підходів до регулювання, оцінювання ризиків та забезпечення відповідальності. Особливої актуальності ці питання набувають для України, яка одночасно розвиває цифрову інфраструктуру, модернізує публічне управління й функціонує в умовах посилених безпекових загроз.

У таких обставинах державне управління стикається з потребою збалансувати інноваційність і безпеку, забезпечити контроль над алгоритмічними процесами, створити умови для захисту даних та запобігти технічним або управлінським помилкам, що можуть мати масштабні наслідки. Використання ШІ в публічному секторі потребує комплексного осмислення – від етичних та правових засад до оцінювання ризиків і

[1] European Commission. Artificial Intelligence Act: Proposal for a Regulation. Brussels, 2021.

формування механізмів гарантування безпеки. Саме тому дослідження інтеграції систем ШІ в державне управління стає важливим завданням сучасної науки та практики, які орієнтовані на побудову ефективної, надійної й стійкої моделі цифрової держави.

Теоретичні засади застосування систем ШІ в державному управлінні формуються на перетині декількох наукових напрямів, зокрема публічного адміністрування, інформаційного права, цифрової етики та технологічних досліджень. Штучний інтелект у сучасній науковій традиції визначається як сукупність алгоритмів і моделей, здатних виконувати функції аналізу, прогнозування, класифікації та ухвалення рішень, що раніше вимагали участі людини. Однією з найбільш ґрунтовних праць у цьому контексті є дослідження С. Рассела та П. Норвіга, у якому автори обґрунтовують концептуальні підходи до створення інтелектуальних систем і визначають їхній потенціал для автоматизації складних управлінських процесів[1]. Аналогічні підходи містяться в дослідженнях Л. Флоріді, який підкреслює соціальне значення ШІ та його вплив на структуру державного управління в умовах цифрової трансформації[2].

У публічному секторі технології ШІ дедалі частіше використовують для підсилення управлінських рішень, оптимізації адміністративних процедур, цифровізації державних сервісів і забезпечення аналітичної підтримки політичних процесів. Згідно з аналітичними матеріалами OECD, застосування алгоритмічних рішень у публічній політиці сприяє підвищенню ефективності державних інституцій, скороченню часу на обробку даних та підвищенню точності прогнозування суспільно значущих процесів. Проте міжнародні дослідження також свідчать про зростання ризику алгоритмічного упередження та помилок, якщо державні органи не здійснюють належного контролю за навчанням моделей, їх оновленням та використанням.

Особливого значення теоретичні принципи регулювання ШІ набувають у державному секторі України, який одночасно проходить етап цифрової модернізації та стикається з підвищеним рівнем безпекових загроз. У нормативних документах Міністерства цифрової трансформації України визначено пріоритетність впровадження інтелектуальних технологій у державні процеси, але при цьому наголошено на необхідності дотримання етичних стандартів, прозорості алгоритмів, захисту персональних даних та недопущення дискримінаційних рішень[3]. Ці положення корелюють із міжнародними підходами, які надають перевагу так званому відповідальному ШІ, що передбачає поєднання технологічної

[1] Russell S., Norvig P. Artificial Intelligence: A Modern Approach. Hoboken: Pearson, 2021. 18 p

[2] Floridi L. The Logic of Information: A Theory of Philosophy as Conceptual Design. Oxford University Press, 2019. DOI: https://doi.org/10.1093/oso/9780198833635.001.0001.

[3] Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р

інноваційності зі стабільністю та безпекою управлінських процесів[1]. Концептуальні основи застосування ШІ в публічному управлінні також охоплюють питання інституційної готовності держави до роботи з інтелектуальними технологіями.

Узагальнюючи наукові підходи, можна стверджувати, що інтеграція ШІ в державне управління потребує чіткого теоретичного обґрунтування, яке поєднує технічні можливості ШІ з вимогами правової визначеності, етичної відповідальності та гарантування безпеки громадян. Сучасні дослідження демонструють, що потенціал інтелектуальних систем може реалізовуватися лише за наявності комплексного підходу, який охоплює аналіз технологічних ризиків, формування регуляторних меж та розвиток інституційної спроможності держави.

Правові аспекти впровадження систем ШІ в публічне адміністрування стали ключовим напрямом досліджень у європейській та світовій юридичній науці. Одним із центральних документів, що формує сучасну нормативну основу, є Закон ЄС про штучний інтелект (Artificial Intelligence Act), який визначає класифікацію технологій за рівнем ризику та встановлює вимоги до їхньої безпеки, прозорості, контролю та підзвітності державних органів[2]. Цей документ є першим у світі комплексним регуляторним підходом, спрямованим на забезпечення відповідального використання ШІ у сферах, що безпосередньо впливають на права громадян.

У науковій літературі дедалі більше уваги приділяється проблемі юридичної відповідальності за рішення, ухвалені на основі алгоритмічних моделей. Дослідження К. Кат доводять, що складність автономного функціонування ШІ створює ситуації, за яких неможливо однозначно визначити суб'єкт відповідальності, оскільки рішення часто формуються на основі непрозорих або частково навчальних моделей[3]. Ця проблема є особливо актуальною для публічного сектору, де помилки автоматизованих систем можуть спричинити порушення соціальних, майнових та адміністративних прав. Окремий пласт правових викликів стосується дотримання прав людини під час використання алгоритмічних технологій. За даними Human Rights Watch, автоматизовані системи здатні відтворювати упередженість щодо окремих груп громадян, створювати ризики надмірного спостереження та обмежувати свободу особи через

[1] Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2030 року та затвердження плану заходів щодо її реалізації : розпорядження Кабінету Міністрів України від 17.11.2021 № 1467-р. URL: https://zakon.rada.gov.ua/laws/show/1467-2021-p#Text

[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

[3] Cath C. Governing artificial intelligence: ethical, legal and technical opportunities and challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*. 2018. Vol. 376, Iss. 2133. 20180080. DOI: https://doi.org/10.1098/rsta.2018.0080

помилкову класифікацію даних[1]. Особливо критичними є випадки, коли ШІ застосовують у правоохоронній діяльності, системах соціального забезпечення та механізмах оцінювання ризиків, оскільки результати роботи алгоритмів у цих сферах мають безпосередній вплив на життя людей. Українське законодавство також стикається з низкою викликів, пов'язаних із регулюванням ШІ. Зокрема, чинний Закон України «Про захист персональних даних» не враховує специфіку автоматизованої обробки великих масивів інформації, особливо в разі застосування технологій машинного навчання, що створює прогалини у сфері захисту приватності та інформаційної безпеки. Додаткові труднощі виникають через відсутність законодавчих норм щодо аудиту алгоритмів, процедур оцінювання ризиків та механізмів забезпечення прозорості у використанні ШІ державними органами. Євроінтеграційний курс України потребує поступової гармонізації національного законодавства з нормативними актами ЄС, насамперед у частині алгоритмічної підзвітності, відкритості критеріїв оцінювання рішень та стандартів недискримінації. Міжнародні рекомендації вказують на те, що впровадження ШІ в публічне адміністрування повинно супроводжуватися чітким визначенням меж відповідальності, впровадженням механізмів людиноорієнтованого контролю та створенням правових гарантій, які забезпечать можливість оскарження автоматизованих рішень і перевірки логіки їх формування.

Таким чином, правові виклики інтеграції ШІ в державне управління охоплюють питання захисту прав людини, забезпечення прозорості алгоритмів, недопущення дискримінації, визначення юридичної відповідальності та адаптацію законодавства до сучасних технологічних умов. Ефективне правове регулювання має ґрунтуватися на поєднанні національних інтересів, міжнародних стандартів та науково обґрунтованих підходів, що дозволить забезпечити зважене, безпечне та контрольоване використання інтелектуальних технологій у публічному секторі.

Використання систем ШІ в державному управлінні створює фундаментально нове середовище, у якому цифрові технології отримують доступ до критичних процесів, що впливають на якість публічних послуг, економічну стабільність, обороноздатність та загальнодержавну безпеку. Штучний інтелект здатний значно пришвидшити обробку інформації та підвищити точність аналізу, однак водночас він формує багаторівневі ризики, які потребують усвідомленої державної політики та системних механізмів контролю. Одним із ключових викликів є складність та непрозорість алгоритмічних рішень, що можуть формуватися без можливості повної інтерпретації їхньої логіки людиною. Алгоритми, що працюють на основі великих масивів даних, здатні відтворювати упередження, які містяться в цих даних, або генерувати хибні прогнози

[1] Human Rights Watch. Automated Neglect: How the World Bank's Push to Allocate Cash Assistance Using Algorithms Threatens Rights // Human Rights Watch: сайт. 13.06.2023. URL: https://www.hrw.org/report/2023/06/13/automated-neglect/how-world-banks-push-allocate-cash-assistance-using-algorithms

внаслідок некоректного навчання. Такі проблеми потенційно загрожують порушенням прав громадян, особливо у сферах соціального забезпечення, контролю ризиків чи розподілу державних ресурсів. У наукових роботах наголошується, що непрозорі алгоритми можуть стати чинником управлінської помилки, яку важко виявити без спеціальних інструментів аналізу[1]. Ще один важливий ризик пов'язаний із вразливістю ШІ до кібератак і зовнішніх втручань. Зважаючи на те, що значна частина моделей ШІ працює з даними в режимі реального часу, будь-яке втручання в ці дані здатне модифікувати результати роботи системи. У контексті гібридної війни проти України ця загроза набуває особливої ваги: зміна алгоритмічних параметрів чи отруєння навчальних наборів даних (*data poisoning*) може спричинити хибне моделювання загроз, порушення логістичних процесів, збій у роботі електронних сервісів або ослаблення системи державної кібербезпеки. Дослідження українських фахівців свідчать, що алгоритмічні системи можуть стати не лише об'єктом атаки, а й інструментом її поширення в умовах масштабних інформаційних та кібернетичних операцій. Правові ризики також набувають дедалі більшого значення. Проблема відповідальності за алгоритмічні рішення досі не врегульована ані в українському законодавстві, ані в більшості світових правових систем. Питання про те, хто має відповідати за наслідки автоматизованих дій – розробник, адміністратор, державний орган чи сама система – лишається відкритим. Зазначене створює правові прогалини, які можуть призвести до зловживань або втрати довіри суспільства до цифрових державних рішень. У працях українських дослідників наголошується, що нечіткість відповідальності у сфері ШІ формує ризик управлінських помилок, які неможливо оскаржити або відкоригувати традиційними юридичними інструментами[2].

Значної уваги потребує і ризик залежності від іноземних технологій. Україна активно використовує хмарні рішення, інструменти обробки даних та програмне забезпечення, значна частина якого розроблена за кордоном. Це збільшує ризик того, що у критичний момент держава може опинитися перед обмеженим доступом до технологій, змінами в політиці компаній-постачальників або технічними обмеженнями, які унеможливлять безперервне функціонування державних сервісів. Наукові й аналітичні висновки підтверджують необхідність розвитку власних технологічних компетенцій, які забезпечать стійкість систем ШІ до зовнішніх впливів. Окремим викликом є питання інформаційної конфіденційності. Оскільки ШІ працює з великими обсягами персональних і службових даних, будь-який витік або неправомірне використання цих даних стає чинником загрози. Гарантії недоторканності приватності мають бути закріплені на законодавчому рівні та технічно забезпечені, адже алгоритмічні системи

[1] Дубовський О. Інформаційна безпека: суб'єктність і штучний інтелект. *Journal of Innovations and Sustainability*. 2024. Vol. 8, No. 2. DOI: https://doi.org/10.51599/is.2024.08.02.09

[2] Ваврик Ю. Л., Опірський І. Р. Штучний інтелект: кібербезпека нового покоління. *Безпека інформації*. 2024. Т. 30, № 2. С. 244–255. DOI: https://doi.org/10.18372/2225-5036.30.19235

здатні не лише фіксувати, а й аналізувати поведінкові моделі громадян, що робить необхідним суворий контроль обробки інформації. Попри всю складність ризиків, сучасні дослідження демонструють, що ефективні безпекові механізми існують. До них належать: а) створення систем регулярного аудиту алгоритмів; б) тестування моделей перед впровадженням; в) забезпечення технічної пояснюваності рішень ШІ; г) впровадження національних центрів оцінки та моніторингу ШІ; д) підготовка фахівців у сфері алгоритмічної безпеки; е) формування нормативно-правових меж, що регулюють відповідальність і прозорість використання ШІ.

Побудова безпечного середовища для роботи інтелектуальних систем має базуватися на принципах людського контролю, прозорості, захисту даних і технологічного суверенітету. У державному секторі ШІ може бути ефективним лише в тому разі, якщо його впровадження супроводжується глибоким аналізом ризиків, багаторівневими гарантіями та системним нормативним забезпеченням.

Висновки. Дослідження концептуальних і практичних засад інтеграції систем ШІ в державне управління надало змогу сформулювати такі узагальнення. Застосування ШІ стає ключовим чинником модернізації публічної сфери, оскільки забезпечує новий рівень аналітичних можливостей, підвищує швидкість обробки інформації та сприяє формуванню більш адаптивних управлінських рішень. Проте одночасно з технологічними перевагами виникає комплекс ризиків, що охоплює правові невизначеності, загрози інформаційній безпеці, етичні дилеми та потенційне зростання залежності державних інституцій від алгоритмічних рішень. У процесі дослідження було встановлено, що ефективне впровадження ШІ неможливе без формування надійної системи правових гарантій, яка забезпечуватиме підзвітність алгоритмів, захист персональних даних, дотримання прав людини та можливість людського контролю за критичними рішеннями. Саме неврегульованість цих аспектів створює найбільші виклики для держав, що перебувають у стані активної цифрової трансформації, зокрема й для України, яка додатково стикається з небезпеками гібридної війни та зростанням інтенсивності кібератак. Забезпечення безпечного функціонування систем ШІ потребує поєднання технологічних та інституційних рішень, а саме: розвитку національних експертних центрів, впровадження механізмів аудиту та моніторингу алгоритмів, створення умов для прозорої роботи систем і контролю за якістю даних. Важливою умовою є також підготовка фахівців, здатних здійснювати оцінку ризиків, управління інцидентами та аналіз поведінки інтелектуальних систем.

Формування ефективної моделі державного управління з використанням ШІ можливе лише за наявності збалансованої нормативної бази, відповідальної інституційної політики та високого рівня інформаційної стійкості. Орієнтація на міжнародні стандарти, інтеграція наукових досягнень та використання практик демократичного врядування

забезпечать технологічний розвиток Україні без втрати контролю над ключовими державними процесами. У результаті ШІ може стати не лише інструментом оптимізації, а й основою для зміцнення національної безпеки та підвищення довіри громадян до діяльності держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ваврик Ю. Л., Опірський І. Р. Штучний інтелект: кібербезпека нового покоління. *Безпека інформації*. 2024. Т. 30. № 2. С. 244–255. DOI: https://doi.org/10.18372/2225-5036.30.19235.

2. Дубовський О. Інформаційна безпека: суб'єктність і штучний інтелект. *Journal of Innovations and Sustainability*. 2024. Vol. 8. No. 2. DOI: https://doi.org/10.51599/is.2024.08.02.09.

3. Євдокимов В., Коломієць С. Цифрова трансформація публічного управління в Україні: виклики та перспективи. *Актуальні питання у сучасній науці. Серія «Державне управління»*. 2024. № 9 (27). С. 403–415. DOI: https://doi.org/10.52058/2786-6300-2024-9(27)-403-415.

4. Кучменко В., Ватульєв М. Цифрова трансформація публічного управління в умовах воєнного стану. *Молодий вчений*. 2025. № 4 (135). DOI: https://doi.org/10.32839/2304-5809/2025-4-135-14.

5. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р

6. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2030 року та затвердження плану заходів щодо її реалізації : розпорядження Кабінету Міністрів України від 17.11.2021 № 1467-р. URL: https://zakon.rada.gov.ua/laws/show/1467-2021-р#Text

7. Сорокіна Н. Цифровізація публічного управління в Україні: теоретичний аспект. *Аспекти публічного управління*. 2021. Т. 13, № 1. С. 77–81. DOI: https://doi.org/10.15421/152509.

8. Artificial Intelligence in Society // OECD : сайт. 11.06.2019. DOI: https://doi.org/10.1787/eedfee77-en.

9. Bryson J. The Past Decade and Future of AI's Impact on Society. ACM Computing Surveys, 2019. 35 p. URL: https://static1.squarespace.com/static/5e13e4b93175437bccfc4545/t/67057b00d95cad198c5575da/1728412417139/the-past-decade-and-future-of-ai-impact-on-society-bbva.pdf

10. Cath C. Governing artificial intelligence: ethical, legal and technical opportunities and challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*. 2018. Vol. 376. Iss. 2133. 20180080. DOI: https://doi.org/10.1098/rsta.2018.0080

11. Floridi L. The Logic of Information: A Theory of Philosophy as Conceptual Design. Oxford University Press, 2019. DOI: https://doi.org/10.1093/oso/9780198833635.001.0001.

12. Floridi L., Cowls J. A Unified Framework of Five Principles for AI in Society. *Harvard Data Science Review*. 2019. Iss. 1.1. DOI: https://doi.org/10.1162/99608f92.8cd550d1.

13. Human Rights Watch. Automated Neglect: How the World Bank's Push to Allocate Cash Assistance Using Algorithms Threatens Rights // Human Rights Watch: сайт. 13.06.2023. URL: https://www.hrw.org/report/2023/06/13/automated-neglect/how-world-banks-push-allocate-cash-assistance-using-algorithms

14. Pasquale F. The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press, 2015. 260 p. // JSTOR : сайт. URL: https://www.jstor.org/stable/j.ctt13x0hch

15. Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts : Brussels, 21.4.2021, COM(2021) 206 final2021/0106(COD) // EUR-Lex : сайт. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206/ Russell S., Norvig P. Artificial Intelligence: A Modern Approach. Hoboken : Pearson, 2021. 18 p.

16. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts : Brussels, 21.4.2021, COM(2021) 206 final, 2021/0106(COD) // EUR-Lex : сайт. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206

17. Wachter S., Mittelstadt B., Floridi L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*. 2017. Vol. 7, Iss. 2. Pp. 76–99. DOI: https://doi.org/10.1093/idpl/ipx005.

Стаття надійшла до редакції 30.06.2025

Viktor M. VASYLENKO,
Doctor of Law, Associate Professor
(*Kharkiv National University of Internal Affairs, Kharkiv, Ukraine*)

INTEGRATION OF ARTIFICIAL INTELLIGENCE SYSTEMS INTO PUBLIC GOVERNANCE: RISKS, LEGAL CHALLENGES AND SECURITY GUARANTEES

The article presents a comprehensive analysis of the integration of artificial intelligence systems into public governance, taking into account contemporary transformations of the public sector and the growing technological dependence of state institutions on algorithmic decision-making. The study elaborates on the theoretical and conceptual foundations of employing intelligent technologies in governmental operations, identifying key risks associated with algorithmic

autonomy, opacity, and potential errors in administrative decision-making. Special attention is given to legal challenges, including issues of responsibility for the functioning and consequences of artificial intelligence systems, the protection of personal data, safeguarding human rights, and the need to harmonize national legislation with the regulatory standards of the European Union. The article further examines the security dimension of AI integration, highlighting threats to cybersecurity, risks of external interference, data manipulation, and dependence on foreign technological infrastructures. The research substantiates the necessity of establishing a comprehensive system of legal and organizational safeguards aimed at ensuring transparency, accountability, and the secure operation of AI technologies within the public sector. The findings may serve as a foundation for developing a national regulatory framework for artificial intelligence and improving Ukraine's digital transformation strategies.

Keywords: *artificial intelligence, public governance, legal challenges, algorithmic security, digital transformation, public policy, cybersecurity, algorithmic accountability.*