УДК 342.6
DOI https://doi.org/10.24144/2788-6018.2026.02.2.47

ІНФОРМАЦІЙНА БЕЗПЕКА ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ОРГАНАМИ ВИКОНАВЧОЇ ВЛАДИ

Шопіна І.М.,
доктор юридичних наук, професор,
професор кафедри адміністративно-правових дисциплін,
Львівський державний університет внутрішніх справ
ORCID: 0000-0003-3334-7548

Шопіна І.М. Інформаційна безпека використання штучного інтелекту органами виконавчої влади.

Стаття присвячена дослідженню проблем інформаційної безпеки використання технологій штучного інтелекту органами виконавчої влади України. Проаналізовано наукові підходи до оцінки можливостей і ризиків використання штучного інтелекту в діяльності публічної адміністрації, зокрема у сфері інформаційної безпеки, публічних закупівель та прийняття адміністративних рішень. Встановлено, що сучасні дослідження акцентують увагу як на позитивному потенціалі штучного інтелекту для підвищення ефективності управлінських процесів, так і на наявності значних ризиків, пов'язаних із захистом персональних даних, прозорістю алгоритмів, можливістю виникнення упередженості в даних, а також залежністю державних інституцій від технологічних компаній.

Досліджено сучасний стан правового регулювання використання штучного інтелекту в Україні. Проаналізовано положення Концепції розвитку штучного інтелекту в Україні, плани заходів щодо її реалізації, а також окремі рекомендаційні документи у сфері безпечного використання штучного інтелекту. Встановлено наявність низки організаційно-правових прогалин, зокрема недостатню системність державної політики у сфері інформаційної безпеки застосування штучного інтелекту органами виконавчої влади, відсутність належного рівня правової регламентації діяльності публічних службовців при використанні відповідних інструментів, а також переважання рекомендаційних механізмів регулювання.

Обґрунтовано авторське розуміння інформаційної безпеки використання штучного інтелекту органами виконавчої влади як комплексу правових, організаційно-управлінських, технічних, технологічних, економічних, соціально-психологічних та освітніх заходів, спрямованих на запобігання, виявлення та нейтралізацію ризиків і загроз, пов'язаних із застосуванням систем штучного інтелекту в процесі підготовки, прийняття та реалізації управлінських рішень. Доведено необхідність удосконалення правового регулювання використання штучного інтелекту в системі виконавчої влади шляхом деталізації правил роботи з відповідними технологіями, запровадження механізмів контролю достовірності інформації, а також встановлення обмежень щодо використання певних видів інформації. Зроблено висновок про доцільність прийняття спеціального закону про штучний інтелект, який би закріпив правові засади безпечного використання цих технологій у діяльності органів державної влади.

Ключові слова: інформаційна безпека, кібербезпека, інформаційні технології, органи виконавчої влади, державна служба, публічна служба, публічне управління, державні службовці, публічні службовці, штучний інтелект.

Shopina I.M. Information security of artificial intelligence use by executive authorities.

This article examines the issues of information security related to the use of artificial intelligence technologies by executive authorities of Ukraine. The study analyzes scholarly approaches to assessing the opportunities and risks associated with the use of artificial intelligence in public administration, particularly in the areas of information security, public procurement, and administrative decision-making. It has been established that contemporary research emphasizes both the positive potential of artificial intelligence in enhancing the efficiency of governance processes and the existence of significant risks associated with personal data protection, algorithmic transparency, the possibility of data bias, and the growing dependence of public institutions on technology companies.

The current state of legal regulation governing the use of artificial intelligence in Ukraine is also examined. The provisions of the Concept for the Development of Artificial Intelligence in Ukraine, the action plans for its implementation, and several advisory documents concerning the safe use of artificial intelligence are analyzed. The study identifies a number of organizational and legal gaps, including the

insufficient systemic nature of state policy in ensuring the information security of artificial intelligence use by executive authorities, the lack of an adequate level of legal regulation governing the activities of public servants when using such tools, and the predominance of advisory rather than binding regulatory mechanisms.

The article substantiates the author's understanding of the information security of artificial intelligence use by executive authorities as a set of legal, organizational and managerial, technical, technological, economic, socio-psychological, and educational measures aimed at preventing, detecting, and neutralizing risks and threats associated with the application of artificial intelligence systems in the preparation, adoption, and implementation of managerial decisions. The necessity of improving the legal regulation of artificial intelligence use within the system of executive authorities is demonstrated through the specification of rules for working with relevant technologies, the introduction of mechanisms for verifying the reliability of information, and the establishment of restrictions on the use of certain types of information. The article concludes that it is advisable to adopt a special law on artificial intelligence that would establish the legal framework for the safe use of these technologies in the activities of public authorities.

Key words: information security, cybersecurity, information technologies, executive authorities, civil service, public service, public administration, civil servants, public servants, artificial intelligence.

Постановка проблеми. Технології штучного інтелекту (далі – ШІ) протягом останніх років набули в Україні надзвичайно широкого розповсюдження. Не є винятком органи виконавчої влади, деякі з яких вже почали впроваджувати базовані на технологіях ШІ платформи та інструменти, призначені для підвищення ефективності виконання публічними службовцями своїх функцій та завдань. Однак, як свідчить практика застосування ШІ і як визначено, зокрема, у Регламенті (ЄС) 2024/1689 Європейського Парламенту і Ради [1], використання ШІ пов'язано із виникненням різноманітних ризиків. Це уявляється особливо небезпечним для України під час воєнного стану. Вказане обумовлює доцільність визначення сучасного стану розбудови системи інформаційної безпеки використання штучного інтелекту органами виконавчої влади і слугує підтвердженням актуальності цієї статті.

Мета статті – визначити сутність та особливості інформаційної безпеки використання штучного інтелекту органами виконавчої влади.

Стан опрацювання проблематики. Динамічний розвиток технологій ШІ, конкуренція між його розробниками, суттєве підвищення ефективності рутинної праці під час користування продуктами ШІ сприяли його проникненню у всі сфери суспільного життя. Особливості застосування ШІ останнім часом привертають увагу багатьох українських та зарубіжних вчених.

О. Дубовський вказує, що використання надійного та етичного ШІ посилює інформаційну безпеку, збільшує довіру суспільства та зменшує невизначеність. Як технологія дії та протидії, штучний інтелект дозволяє підвищити об'єктивність, швидкість формування та повноту ситуаційної обізнаності. Ефективність використання моделей ШІ залежить від збереженості людського компонента, розробка «спільних когнітивних систем» є оптимальним балансом між аналітиками та алгоритмами [2]. Повністю погоджуючись з науковцем щодо можливості зміцнення інформаційної безпеки завдяки використанню технологій ШІ, зауважимо, однак, що якістю етичності може володіти лише людина. Аналіз визначення поняття ШІ, під яким у Концепції розвитку штучного інтелекту в Україні розуміється «організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації…» (і далі за текстом) [3], свідчить про належність його до категорії технологій інформаційного характеру. Такі технології як сукупність інформаційних процесів не володіють якістю суб'єктності та не здатні до етичних або неетичних дій чи поведінки. Отже, з огляду на оновлення термінології інформаційного права і появи нової і більш широкої за змістом категорії «цифрові технології», проблеми етичних бар'єрів при використання ШІ потребують свого подальшого вивчення.

О. Карпенко, Ю. Карпенко та Д. Герман дослідили можливості ШІ для зниження корупційних ризиків у сфері публічних закупівель. Автори дійшли висновку, що запровадження нових можливостей ШІ завдяки встановленим перевагам (належному інформуванню потенційних учасників закупівельного процесу; моніторингу великих масивів даних відкритих тендерів; плануванню, здійсненню аналітичної та прогностичної діяльності; роботизації трудомістких, рутинних, стандартних, типових та повторюваних операцій; оптимізації та/або узгодженню внутрішніх операцій закупівельного процесу; розробці стратегій з управління закупівельним процесом) та наданим практичним рекомендаціям для максимізації рівня впровадження його алгоритмів й технологій дасть можливість суттєво спростити та покращити результативність функціонування державної системи

публічних закупівель, збільшити конкурентоспроможність учасників торгів, підвищити ефективність діяльності тендерних комітетів, знизити ймовірність помилок, забезпечити прозорість процедур відкритих торгів [4, с. 134]. Позитивно оцінюючи отримані науковцями результати, які можуть бути корисними для правової теорії і практики, слід звернути увагу на потребу у більш детальному аналізі можливих негативних наслідків використання ШІ в сфері публічних закупівель, а також створенні моделі контролю за його використанням. Метою функціонування такої моделі могло б бути попередження помилок та неточностей генерованих ШІ даних, а також (і це найголовніше) зниження ймовірності прийняття помилкових управлінських рішень, прийнятих з урахуванням отриманої від ШІ інформації.

Досить цікавою є робота О. Автономова, який виокремлює такі групи ризиків використання ШІ у публічній службі: 1) конфіденційність та безпека персональних даних приватних осіб під час прийняття адміністративних рішень адміністративними органами; 2) непрозорість і алгоритмічна «справедливість» під час прийняття адміністративних рішень; 3) втрата робочих місць і соціальні наслідки для публічних службовців; 4) залежність від технологічних компаній і монополізація ринку цифрових трансформацій; 5) етичні та правові виклики збалансування публічного та приватного інтересів у діяльності суб'єктів публічної адміністрації [5]. Додамо, що робота із попередження негативного впливу цих та інших ризиків, пов'язаних із процесами широкого впровадження технологій ШІ у систему публічного управління потребує зміцнення системи інформаційної безпеки. Рішення та заходи, пов'язані із використанням означених технологій, можуть бути успішними лише за умови їх системного характеру та усвідомлення органічного зв'язку між публічним управлінням та його інформаційною складовою. Помилки під час моніторингу даних та їх інтерпретації можуть спотворювати інформаційну базу управлінських рішень органів виконавчої влади та утворювати нові загрози національній безпеці. У сукупності ці фактори підтверджують важливість подальшого наукового пошуку.

Виклад основного матеріалу. Ситуація у сфері правового регулювання використання технологій ШІ органами виконавчої влади в нашій державі характеризується нерівномірністю. З одного боку, Україна однією з перших держав Центрально-Східної Європи сформувала стратегічне бачення розвитку ШІ. Ключові чинники, загрози та ризики, пов'язані з технологіями ШІ знайшли своє правове закріплення у Концепції розвитку штучного інтелекту в Україні, схваленої розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. У вказаному правовому документі було проголошено, що реалізація державної політики у галузі штучного інтелекту впливатиме на ключові інтереси таких заінтересованих сторін, як громадяни, заклади освіти, суб'єкти господарської діяльності, органи виконавчої влади та місцевого самоврядування. У Концепції знайшли відображення і питання інформаційної безпеки. Так, відзначалося, що застосування технологій штучного інтелекту в забезпеченні інформаційної безпеки є одним із факторів, що сприятиме забезпеченню національних інтересів. Зокрема, моніторинг соціальних мереж та інтернет-ресурсів електронних медіа з використанням технологій штучного інтелекту дає можливість виявляти системні тренди і проблематику, діяти на випередження, аналізувати цільову аудиторію [2]. На виконання вказаного правового документу було затверджено План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021-2024 роки, відповідно до якого мали бути розроблені Концепція законопроекту про розвиток штучного інтелекту, система показників для оцінки стану інформаційної безпеки з використанням технологій штучного інтелекту, забезпечено використання технологій штучного інтелекту для проведення аналізу та оцінки, прогнозування та моделювання показників ефективності системи державного управління [6]. Однак, як і багато інших планів в сфері інформаційного забезпечення публічного управління, цей план залишився не повною мірою реалізованим. Почасти цьому сприяв початок повномасштабної російської збройної агресії, почасти – певна нереалістичність його положень та недостатність коштів для виконання його заходів. Від центральних органів виконавчої влади щодо виконання Плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021-2024 роки мала щорічно надходити інформація до Міністерства цифрової трансформації інформацію про стан виконання зазначеного плану. У свою чергу, цей орган після узагальнення вказаних заходів мав подавати її Кабінетові Міністрів України. На жаль, на офіційному вебсайті Міністерства цифрової трансформації станом на 3 березня 2026 року нам не вдалося знайти звітних документів з цього приводу. Так само не вдалося знайти звітну інформація про виконання означеного Плану на офіційному вебсайті Кабінету Міністрів України.

Розпорядженням від 9 травня 2025 р. № 457-р Кабінет Міністрів України затверджує новий План у досліджуваній сфері – на 2025-2026 роки. Він менший за обсягом запланованих заходів, ніж попередній, деякі його пункти дублюють положення Плану на 2021-2024 роки, але в іншій редакції. Зокрема, це стосується розроблення та подання Кабінетові Міністрів України законо-

проекту щодо правового врегулювання у сфері розвитку штучного інтелекту, що Міністерство цифрової трансформації має здійснити у IV кварталі 2026 року. Разом з тим, із нового Плану [7] зникли будь-які згадування про інформаційну безпеку, присутні у п. 7 Плану на 2021-2024 роки [6].

Розбудова і зміцнення систем інформаційної безпеки на рівні виконавчої влади має носити цілеспрямований характер, що повинно знаходити своє відображення у програмних і планових документах, затверджених Урядом. Інакше така діяльність стає хаотичною, неефективною, утруднюється контроль та інтерпретація його результатів. На жаль, аналіз правових та організаційних передумов зміцнення інформаційної безпеки за досліджуваним напрямом не дозволяє зробити висновок про системність, цілеспрямованість та послідовність у здійсненні вказаних заходів. Проте слід позитивно відзначити деякі досягнення у галузі кібербезпеки як складової інформаційної безпеки, зокрема, виконання п. 2 Плану на 2025-2026 роки, яким передбачалося розроблення, затвердження і оприлюднення на офіційному вебсайті Адміністрації Держспецзв'язку Рекомендацій з кіберзахисту інформаційно-комунікаційних систем, які використовують технології штучного інтелекту, затверджених наказом Адміністрації Держспецзв'язку від 23.02.2026 року № 154 [7]. Рекомендації можуть використовуватися власниками та/або розпорядниками інформаційних, електронних комунікаційних, інформаційно-комунікаційних і технологічних систем, які використовують технології штучного інтелекту, під час розробки плану кіберзахисту. Рекомендації стосуються специфічної сфери правового регулювання (кіберзахисту) і наповнені технічними термінами, розуміння яких державними службовцями органів виконавчої влади без спеціальної освіти, скоріше за все, буде викликати труднощі (перехресна валідація, федеративне навчання, комплексна видимість тощо). Однак багато положень вказаних Рекомендацій є надзвичайно корисними для побудови систем інформаційної безпеки органів виконавчої влади. Зокрема, це стосується п. 7, відповідно до якого у процесі забезпечення якості та релевантності даних власник та/або розпорядник ІКС із ШІ враховує ризики виникнення упередженості у даних та моделях ШІ включно з упередженістю, що може: бути наслідком навмисного або ненавмисного «отруєння» даних; спричиняти некоректні рішення моделей та технологій ШІ, які впливають на безпеку ІКС із ШІ; знижувати стійкість моделі ШІ та ІКС із ШІ відповідно до деструктивного впливу та загроз; створювати передумови для компрометації ІКС із ШІ через спрямовані маніпуляції набором даних; бути наслідком використання іноземних продуктів, які не є адаптованими до українських реалій [7].

Слід також відзначити наявність низки документів, підготовлених Міністерством цифрової трансформації України. Перш за все слід сказати, що вказаним центральним органом виконавчої влади підготовлено і розміщено на своєму офіційному вебсайті Дорожню карту з регулювання штучного інтелекту в Україні [8]. На жаль, у тексті цього документу відсутні відомості про його офіційне затвердження. Поряд з безумовно позитивною оцінкою намагань авторів Дорожньої карти створити модель дій для безпечного використання технологій ШІ у всіх сферах життєдіяльності держави, слід відзначити недостатньо професійний рівень підготовки цього тексту. По-перше, викликає питання назва документу, оскільки регулювати ШІ можуть його розробники, розпорядники або власники технології. На сьогоднішній день в Україні розробляються деякі інструменти ШІ, але така розробка здійснюється переважно приватними ІТ-компаніями і орієнтована здебільшого на міжнародний ринок. Головні офіси розробників найбільш відомих українських продуктів ШІ – Grammarly і People.ai знаходяться у м. Сан-Франциско (США) і здійснюють свою діяльність відповідно до норм американського законодавства. Безумовно, в Україні існують деякі власні розробки ШІ, у тому числі у військовій сфері, однак масштаб їх застосування в нашій державі є значно меншим, ніж інструментів іноземних розробників. За результатами соціологічних досліджень, найбільш часто використовуваними в Україні моделями ШІ станом на жовтень 2025 року є наступні: ChatGPT – 85%; Google Gemini – 64%; Microsoft Copilot – 20%; Midjourney – 11%; Claude – 8%; інше – 8%; DALL-E – 7%; Perplexity AI – 5%; жодна – 3% [9]. Як відомо, розробниками і власниками вказаних моделей є компанії, розташовані на території США. Отже, Україна позбавлена можливості впливати на архітектуру та алгоритми цих моделей, однак може регулювати порядок їх використання на національному рівні саме у сфері інформаційної безпеки: зокрема, регулювати поведінку користувачів технологій ШІ (наприклад, державних службовців органів виконавчої влади) або заходи інформаційної безпеки, які мають вживати розробники продуктів, які використовують можливості ШІ, тощо.

Недостатня увага до правової складової використання ШІ у Дорожній карті з регулювання штучного інтелекту в Україні притаманна й деяким положенням цього документу. Так, наприклад, простежується відхилення від усталеної юридичної лексики у формулюванні «Впровадження (на кінцевому етапі) регуляції, яка пропонує найвищий у світі рівень захисту прав людини від

ризиків та злонаміреного використання ШІ» [8]. Можливо, під регуляцією мався на увазі Закон України «Про штучний інтелект», під його впровадженням на кінцевому етапі – прийняття такого закону Верховною Радою України, а під пропонуванням найвищого в світі захисту – включення до цього правового документу норм про інформаційну безпеку, однак це скоріше припущення, і таких неконкретизованих положень у цьому документі ще багато.

Окремо слід зупинити увагу на підготовлених Міністерством цифрової трансформації України Порадах з відповідального використання штучного інтелекту публічними службовцями (розробники та особливості затвердження цього документу також не знайшли в ньому відображення). Не зважаючи на те, що термін «Поради» є дещо незвичним для українських правових документів рекомендаційного характеру, сумнівів в існуванні нагальної потреби для його розробки і широкого впровадження не виникає. Водночас, в аспекті інформаційної безпеки спостерігається наявність численних прогалин. Так, публічному службовцю, який взаємодіє із системами ШІ, рекомендується звертати увагу на політику конфіденційності сервісу до використання у взаємодії з ним персональних даних. Це пояснюється тим, що в умовах війни росії проти України особливу увагу варто приділяти країнам походження ШІ інструмента, зокрема тим, які підтримують агресію, та враховувати безпекову репутацію розробника [10]. Але, як відомо, моделі ШІ, які проголосили політику прозорості для користувача, не приховують, що їх безкоштовні версії збирають надану користувачами інформацію, у тому числі персональні дані, і використовують її для фільтрації шкідливого контенту, навчання нових моделей ШІ, а також, з використанням певного ступеня анонімізації, ця інформація може бути доступною для рецензентів. Вказане викликає питання: а чи може взагалі публічний службовець органу виконавчої влади надавати інструментам ШІ доступ до публічної інформації або персональних даних, що стали йому відомі у зв'язку з його професійною діяльністю? Щодо країни-лідера у розробці ШІ і її позиції щодо повномасштабної російської збройної агресії проти України також виникають певні питання, пов'язані із забезпеченням національної, інформаційної та воєнної безпеки.

Слід також звернути увагу на неконкретність багатьох положень Порад, що не дає змоги публічному службовцю органу виконавчої влади побудувати власну модель правомірної поведінки при використанні ШІ. З одного боку, з огляду на надання в аналізованому документі достатньої інформації щодо помилок (т.зв. галюцинацій) ШІ, певна частина користувачів, здатних до самонавчання і мотивованих до постійного професійного самовдосконалення, зможе побудувати власні стратегії поводження з ШІ (зокрема, шляхом самостійного розроблення і коректного використання промтів). Однак слід пам'ятати, що, за даними досліджень, більша частина дорослого населення світу не має мотивації до постійного самонавчання. Так, за даними звіту Організації економічного співробітництва та розвитку 2025 року, прагнення до самонавчання залежить від розвитку навичок особи: 70 % людей з добре розвиненими навичками активно беруть участь у навчанні; тоді як серед людей з низько розвиненими навичками таких лише 26 % [11]. Вказане свідчить про необхідність більш високого рівня регламентації та стандартизації дій персоналу – комплаєнс у сфері інформаційної безпеки під час збройного конфлікту високої інтенсивності, на нашу думку, є недоречним.

Ми високо оцінюємо внесок Міністерства цифрової трансформації України у розвиток передумов правового регулювання використання штучного інтелекту органами виконавчої влади та іншими суб'єктами. За кілька років зроблено масштабну роботу, спрямовану на убезпечення публічних службовців та інших осіб від ризиків, які супроводжують використання ШІ. Але стратегічна лінія на саморегулювання не забезпечує належного рівня правової визначеності діяльності органів виконавчої влади (хоча для суб'єктів підприємницької діяльності такий підхід є більш виправданим). Відповідно до ч. 2 ст. 6 Конституції України органи законодавчої, виконавчої та судової влади здійснюють свої повноваження у встановлених цією Конституцією межах і відповідно до законів України [12]. Це обумовлює високий ступень правової регламентації дій публічних службовців, зменшення частки їх дискреційних повноважень. У сфері інформаційної безпеки, як одного із видів національної безпеки, необхідність правової регламентації правил користування інструментами ШІ для персоналу органів виконавчої влади є особливо важливою.

Висновки. Ми обстоюємо позицію, відповідно до якої інформаційна безпека використання штучного інтелекту органами виконавчої влади становить комплекс правових, організаційно-управлінських, технічних, технологічних, економічних, соціально-психологічних та освітніх заходів, спрямованих на запобігання, виявлення та нейтралізацію ризиків і загроз, пов'язаних із застосуванням систем штучного інтелекту в процесі підготовки, прийняття та реалізації управлінських рішень. Особливістю ефективно працюючої системи інформаційної безпеки є її системний характер, за допомогою якого виникає можливість забезпечення сталого функціонування вказаних органів та їх персоналу, здійснення ними діяльності, спрямованої на захист публічних

інтересів, захист прав і свобод громадян відповідно до визначеної законодавством компетенції. Особливо важливим є відстеження можливого впливу ризиків застосування технологій ШІ саме на управлінські рішення, оскільки прийняття їх під впливом помилкової або невірно інтерпретованої інформації може дестабілізувати певні сектори державно-управлінської діяльності.

Аналіз сучасного стану інформаційної безпеки використання штучного інтелекту органами виконавчої влади свідчить про наявність прогалин, пов'язаних із недостатнім розвитком правового забезпечення означених процесів. Завдання щодо створення сучасного правового регулювання використання технологій ШІ в Україні були нормативно закріплені ще у 2020 році, але їх ще не можна вважати виконаними. Нині у сфері використання ШІ в системі виконавчої влади використовується переважно метод рекомендацій, який не дозволяє забезпечити належний рівень інформаційної захищеності у воюючій державі. Пропонований для користувачів метод саморегулювання використання ШІ у сфері виконавчої влади має два суттєвих недоліки: 1) не дозволяє повною мірою реалізувати вимоги ч.2 ст.6 Конституції України та забезпечити належний рівень правової визначеності діяльності виконавчої влади; 2) потребує наявності у всіх без винятку користувачів ШІ в органах виконавчої влади прагнення до постійного самонавчання та самовдосконалення, що не завжди відповідає реальному рівню мотивації державних службовців. З огляду на вказане уявляється доцільною детальна регламентація процесів використання інструментів ШІ в органах виконавчої влади, яка дозволила б: 1) знизити ступінь дискреційності процесів надання ШІ відомостей та даних, 2) ввести подвійну систему контролю за достовірністю інформації, що використовується для підготовки аналітичних довідок, прогнозів та прийняття управлінських рішень; 3) знизити ризики несанкціонованого поширення інформації, наданої державними службовцями під час роботи з ШІ (наприклад, шляхом використання корпоративних моделей ШІ, в яких встановлено заборону на використання інформації користувачів для навчальних цілей); 4) ввести обмеження під час надання ШІ інформації, розповсюдження якої може негативно вплинути на стан воєнної безпеки. Вказані положення, на нашу думку, мають знайти своє закріплення у законі України про штучний інтелект, необхідність прийняття якого нині не викликає сумнівів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. 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). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.
2. Дубовський О. Інформаційна безпека: суб'єктність і штучний інтелект. *Journal of Innovations and Sustainability*. 2024. № 8(2). https://doi.org/10.51599/is.2024.08.02.09.
3. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text.
4. Карпенко О., Карпенко Ю., Герман Д. Штучний інтелект як інструмент зниження корупційних ризиків у сфері публічних закупівель. *Аспекти публічного управління.* 2023. Т. 11 № 2 С.129-135. DOI: https://doi.org/10.15421/152328.
5. Автономов О.П. Європейські правові стандарти використання штучного інтелекту у публічній службі: виклики правового регулювання в Україні. *Правова позиція*. 2024. № 2 (43). С. 11-15. DOI https://doi.org/10.32782/2521-6473.2024-2.2.
6. План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021-2024 роки: затверджено розпорядженням Кабінету Міністрів України від 12 травня 2021 р. № 438-р. URL: https://zakon.rada.gov.ua/laws/show/438-2021-%D1%80#Text.
7. Рекомендації з кіберзахисту інформаційно-комунікаційних систем, які використовують технології штучного інтелекту: затверджені наказом Адміністрації Держспецзв'язку від 23.02.2026 року № 154. URL: https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-23-02-2026-154-pro-zatverdzhennya-rekomendacii-z-kiberzakhistu-informaciino-komunikaciinikh-sistem-yaki-vikoristovuyut-tekhnologiyi-shtuchnogo-intelektu.
8. Дорожня карта з регулювання штучного інтелекту в Україні. URL: https://storage.thedigital.gov.ua/files/2/22/363bbcaec30bf9d4e598375fecac3227.pdf.
9. Пилипенко Н. Вже 60% українців використовують ШІ: які моделі і застосунки. URL: https://thepage.ua/ua/news/skilki-ukrayinciv-koristuyutsya-shi-ta-yaki-instrumenti-obirayut.
10. Поради з відповідального використання штучного інтелекту публічними службовцями. URL: https://storage.thedigital.gov.ua/files/f/bf/a9595e0dcd238ab2b3602909107 aabf9.pdf.

11. Education at a Glance 2025 OECD Indicators. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/09/education-at-a-glance-2025_c58fc9ae/1c0d9c79-en.pdf.
12. Конституція України. Закон України 28.06.1996. *Відомості Верховної Ради України*. 1996. №30. Ст.141.

Дата першого надходження рукопису до видання: 2.03.2026
Дата прийняття до друку рукопису після рецензування: 20.03.2026
Дата публікації: 3.04.2026