УДК 351.86:004.8:004.056; JEL classification: H56, H83, O33 DOI: https://doi.org/10.36887/2415-8453-2026-3-90

Федоренко Тетяна Вікторівна[1],
кандидат юридичних наук, доцент, доцент кафедри галузевого права та загальноправових дисциплін, Директор Інституту права та суспільних відносин

Дабіжа Віра Василівна[1],
кандидат наук з державного управління, доцент, доцент кафедри міжнародних відносин та політичного консалтингу Інститут права та суспільних відносин
[1]*ЗВО «Відкритий міжнародний університет розвитку людини «Україна», м. Київ*

Fedorenko Tetiana[1], PhD in Law, Associate Professor, Associate Professor of the Department of Industry Law and General Legal Disciplines, Director of the Institute of Law and Public Relations, https://orcid.org/0000-0002-3447-9078

Dabizha Vira[1], PhD in Public Administration, Associate Professor, Associate Professor of the Department of International Relations and Political Consulting, Institute of Law and Public Relations, https://orcid.org/0000-0002-7000-4635
[1]*HEI "Open International University of Human Development "Ukraine", Kyiv, Ukraine*

ДЕРЖАВНЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ ОБОРОНИ УКРАЇНИ: СУЧАСНИЙ СТАН, ВИКЛИКИ ТА НАПРЯМИ ВДОСКОНАЛЕННЯ

STATE REGULATION OF ARTIFICIAL INTELLIGENCE USE IN UKRAINE'S DEFENSE SECTOR: CURRENT STATE, CHALLENGES, AND DIRECTIONS FOR IMPROVEMENT

Федоренко Т. В., Дабіжа В. В. Державне регулювання використання штучного інтелекту у сфері оборони України: сучасний стан, виклики та напрями вдосконалення. *Український журнал прикладної економіки та техніки*. 2026. Том 11. № 3. С. 503 – 508.

Fedorenko T., Dabizha V. State regulation of artificial intelligence use in Ukraine's defense sector: current state, challenges, and directions for improvement. *Ukrainian Journal of Applied Economics and Technology*. 2026. Volume 11. № 3. pp. 503 – 508.

У статті досліджено сучасний стан державного регулювання використання технологій штучного інтелекту в оборонній сфері України. Встановлено, що в умовах повномасштабної збройної агресії штучний інтелект перетворюється на стратегічний ресурс для зміцнення обороноздатності держави. Його застосування охоплює аналіз великих масивів даних, розвідку, управління військами, функціонування безпілотних і автономних систем, кіберзахист, моделювання бойової обстановки, оборонну логістику, прогнозування загроз і підтримку ухвалення управлінських рішень. Проаналізовано законодавчі та стратегічні документи України, що визначають засади функціонування сектору безпеки й оборони, а також розвитку технологій штучного інтелекту. З'ясовано, що чинне нормативно-правове регулювання має переважно рамковий, фрагментарний і реактивний характер, а практичне впровадження технологій ШІ відбувається швидше, ніж формування відповідних правових та інституційних механізмів. Виявлено недостатню визначеність порядку застосування автономних систем, меж допустимого використання ШІ, механізмів людського контролю, оцінювання ризиків і відповідальності за рішення, прийняті із застосуванням алгоритмічних систем. Обґрунтовано необхідність запровадження ризик-орієнтованого підходу, чіткого розподілу повноважень між органами державної влади, посилення міжвідомчої координації, забезпечення людського контролю, створення механізмів оцінювання та мінімізації технологічних ризиків, а також визначення відповідальності за наслідки використання систем штучного інтелекту. Наголошено на необхідності дотримання балансу між прискореним упровадженням оборонних інновацій і забезпеченням законності, підзвітності, безпеки та захисту прав людини.
Ключові слова: *державне регулювання, штучний інтелект, оборонна сфера, обороноздатність держави, національна безпека, сектор безпеки і оборони, державна політика, нормативно-правове регулювання, автономні системи, людський контроль, технологічні ризики, ризик-орієнтований підхід, державне управління.*

The article examines the current state of governmental regulation of artificial intelligence technologies in Ukraine's defense sector. It is established that, amid full-scale armed aggression, artificial intelligence is becoming a strategic resource for strengthening the country's defense capabilities. Its applications include big data analysis, intelligence, command and control, unmanned and autonomous systems, cyber defense, combat-environment modeling, defense logistics, threat forecasting, and decision-making support. The legislative and strategic documents governing Ukraine's security and defense sector, as well as the development of artificial intelligence technologies, are analyzed. It is determined that the existing legal framework remains predominantly general, fragmented, and reactive, while the practical implementation of AI technologies is advancing faster than the development of the corresponding legal and institutional mechanisms. Insufficient regulation has been identified regarding the use of autonomous systems, permissible limits of AI deployment, human oversight, risk assessment, and responsibility for decisions made with the assistance of algorithmic systems. The need to establish a comprehensive model of governmental regulation that combines legal, institutional, organizational, personnel, and resource mechanisms is well-substantiated. The article proposes introducing a risk-based approach, clearly allocating powers among public authorities, strengthening interagency coordination, establishing procedures for testing and evaluating AI systems, ensuring meaningful human oversight, and defining responsibility for the consequences of their use. Particular emphasis is placed on maintaining a balance between the rapid implementation of defense innovations and compliance with the principles of legality, accountability, security, and human rights protection.
Keywords: *governmental regulation, artificial intelligence, defense sector, national defense capability, national security, security and defense sector, public policy, legal regulation, autonomous systems, human oversight, technological risks, risk-based approach, public administration.*

Вступ

В умовах повномасштабної війни проти України, активного поширення цифрових технологій та постійних змін у сфері безпеки одним із важливих напрямів державної політики є зміцнення обороноздатності країни шляхом впровадження сучасних інноваційних рішень. Значну роль у цьому процесі відіграє штучний інтелект, який поступово перетворюється з окремого технологічного інструменту на важливий стратегічний ресурс для підвищення спроможностей сектору безпеки та оборони. Застосування технологій штучного інтелекту відкриває широкі можливості для обробки та аналізу значних обсягів інформації, удосконалення процесів прийняття управлінських рішень, створення й використання безпілотних та автономних систем, посилення кіберзахисту, оптимізації оборонної логістики, прогнозування потенційних загроз, а також протидії дезінформації та інформаційно-психологічним операціям.

Разом із тим результативність використання штучного інтелекту залежить не лише від рівня розвитку відповідних технологій. Важливе значення мають ефективність державного управління, сформованість цілісної державної політики у цій сфері, належне нормативно-правове регулювання, достатнє фінансове та кадрове забезпечення, налагоджена взаємодія між державними органами та дієві механізми контролю.

Отже, використання штучного інтелекту у сфері безпеки й оборони не можна розглядати виключно як технологічне питання. Воно є комплексним завданням державного управління, що передбачає формування ефективних механізмів розроблення, впровадження та реалізації державної політики у сфері застосування технологій штучного інтелекту. Саме тому виникає необхідність у його всебічному науковому дослідженні та визначенні

This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

© Федоренко Тетяна Вікторівна, Дабіжа Віра Василівна, 2026

оптимальних підходів до застосування відповідних технологій для зміцнення обороноздатності України.

Важливість досліджуваної проблематики визначається потребою подальшого вдосконалення системи публічного управління України відповідно до нових викликів і загроз у сфері національної безпеки. Особливого значення набуває вивчення та використання міжнародного досвіду застосування технологій штучного інтелекту у сфері оборони, поглиблення цифрової трансформації сектору безпеки й оборони, а також формування необхідних умов для забезпечення технологічної спроможності держави в умовах сучасної війни. Подолання зазначених викликів безпосередньо пов'язане з реалізацією стратегічних пріоритетів державної політики у сфері національної безпеки та оборони, підвищенням обороноздатності України, удосконаленням роботи органів публічної влади та подальшим упровадженням цифрових технологій у систему державного управління.

У зв'язку з цим дослідження державної політики у сфері застосування штучного інтелекту для посилення обороноздатності України має вагоме наукове та прикладне значення. Отримані результати можуть бути використані для вдосконалення управлінських механізмів, нормативно-правової бази та організаційних підходів до впровадження технологій штучного інтелекту й цифрової трансформації сектору безпеки та оборони України.

Питання застосування технологій штучного інтелекту у сфері публічного управління, національної безпеки та оборони протягом останніх років привертає дедалі більше уваги науковців. Дослідницький інтерес зосереджується на широкому спектрі проблем, зокрема на державному регулюванні використання штучного інтелекту, цифровій модернізації системи публічного управління, управлінні технологічними ризиками, забезпеченні кібербезпеки, розвитку автономних систем, а також на використанні алгоритмічних технологій під час підготовки та ухвалення управлінських рішень.

Важливе місце у формуванні наукових підходів до державного управління технологіями штучного інтелекту посідають дослідження зарубіжних учених С. А. Барката та М. Бусідоса [1], у працях яких розглядаються особливості застосування алгоритмічних систем органами публічної влади та наслідки використання автоматизованих рішень для функціонування державного управління.

Проблематика використання штучного інтелекту у військовій та оборонній сферах представлена у роботах М. Драсара, А. Котта, П. Лебланка, П. Терона [2] та інших дослідників. У рамках наукових програм НАТО ними було розроблено концептуальні засади створення автономних інтелектуальних агентів кібероборони (AICA), визначено основні елементи відповідної архітектури та окреслено перспективи використання штучного інтелекту для захисту військових інформаційних систем від кіберзагроз.

Окремий пласт наукових праць присвячений питанням формування державної політики та міжнародних підходів до регулювання штучного інтелекту. Зокрема, В. Хардінг акцентує увагу на необхідності забезпечення балансу між технологічним розвитком і принципами демократичного врядування, прозорості, відповідальності та підзвітності державних інституцій під час упровадження систем штучного інтелекту [3].

В українському науковому просторі проблематику цифровізації, застосування сучасних технологій, кібербезпеки та інновацій у секторі безпеки й оборони досліджували, зокрема, В. Савченко, О. Шаповаленко [4], С. Шумлянський [5, 6], Є. Хоменко [5] та інші науковці.

Водночас проведений аналіз наукових праць свідчить, що, попри значну кількість досліджень у галузях цифрової трансформації, кібербезпеки, технологічних інновацій та оборонних технологій, питання публічно-управлінського забезпечення застосування штучного інтелекту для зміцнення обороноздатності України ще не отримало достатньо комплексного висвітлення. Зокрема, потребують подальшого дослідження механізми формування та реалізації цілісної державної політики у цій сфері, розподіл повноважень між органами публічної влади, інституційні засади впровадження технологій штучного інтелекту, міжвідомча координація, підготовка та розвиток відповідних кадрів, фінансове й ресурсне забезпечення, а також механізми державного нагляду та контролю за використанням таких технологій у секторі безпеки й оборони.

Формулювання цілей статті

Метою статті є аналіз сучасного стану державного регулювання використання технологій штучного інтелекту в оборонній сфері України, виявлення основних нормативно-правових, інституційних, організаційних і технологічних викликів, а також обґрунтування напрямів удосконалення державної політики щодо впровадження ШІ з урахуванням потреб національної безпеки, необхідності людського контролю та ризик-орієнтованого підходу.

Виклад основного матеріалу дослідження

Україна сьогодні активно розвиває та впроваджує технології штучного інтелекту, розглядаючи їх як один із важливих напрямів модернізації Збройних Сил України та оборонно-промислового комплексу. Така увага до ШІ значною мірою зумовлена необхідністю пошуку нових технологічних можливостей для ефективної протидії повномасштабній збройній агресії російської федерації [5].

На відміну від попередніх періодів, коли Україна переважно орієнтувалася на запозичення технологічних розробок, створених за кордоном, в умовах повномасштабної війни ситуація суттєво змінилася. Необхідність протистояти технологічно потужному противнику стала стимулом для прискореного розвитку власних військових інновацій, безпілотних систем, цифрових рішень і технологій штучного інтелекту [5]. Унаслідок цього Україна перетворилася на одного з активних учасників процесу створення й практичного випробування новітніх військових технологій, фактично ставши одним із найбільш масштабних середовищ для застосування ШІ в умовах реальних бойових дій [7].

Водночас процес упровадження штучного інтелекту в Україні поки що не має повністю сформованого централізованого й системного характеру. Значною мірою він розвивається через окремі ініціативи, проєкти та практичні розробки, що виникають безпосередньо в умовах воєнних потреб.

Політика України у сфері штучного інтелекту наразі переважно має реактивний характер. Її розвиток на національному рівні не встигає за стрімким технологічним прогресом і темпами впровадження ШІ на практиці. Особливо помітним цей розрив є у військовій сфері, зокрема у застосуванні штучного інтелекту в озброєнні та військовій техніці, а також під час виконання бойових завдань в умовах збройної агресії російської федерації [8].

У межах дослідження було проаналізовано основні нормативно-правові акти України у сфері національної безпеки та оборони, зокрема Закони України «Про національну безпеку України» [9], «Про мобілізаційну підготовку та мобілізацію» [10] , «Про правовий режим надзвичайного стану» [11] , «Про оборону України» [121] , «Про Раду національної безпеки і оборони України» [13] та «Про правовий режим воєнного стану» [14]. Проведений аналіз засвідчив, що чинне законодавство України не містить комплексного нормативного регулювання питань, пов’язаних із застосуванням технологій штучного інтелекту у сфері оборони. Зазначені законодавчі акти визначають загальні

правові засади функціонування сектору безпеки й оборони, однак не встановлюють спеціальних норм щодо порядку, умов та обмежень використання систем ШІ, розподілу відповідальності за рішення, прийняті із застосуванням таких систем, а також механізмів управління пов'язаними з ними ризиками. Наявність нормативно-правового вакууму та певних прогалин у законодавстві, свідчить про потребу подальшого врегулювання досліджуваної проблематики з урахуванням специфіки застосування ШІ в умовах збройного конфлікту.

Важливу роль у реалізації завдань у сфері оборони відіграють органи місцевого самоврядування та військово-цивільні адміністрації, які в межах визначених законом повноважень здійснюють низку заходів, пов'язаних із забезпеченням обороноздатності та функціонуванням відповідних територій в умовах воєнного стану. Водночас аналіз чинного законодавства свідчить про відсутність належного нормативного визначення питань застосування технологій штучного інтелекту на цьому рівні.

Зокрема, у статті 36 «Повноваження в галузі оборонної роботи» глави 2 «Повноваження виконавчих органів сільських, селищних, міських рад» Закону України «Про місцеве самоврядування в Україні» відсутні положення, які б безпосередньо регулювали використання технологій штучного інтелекту під час виконання органами місцевого самоврядування завдань у сфері оборони [15]. Аналогічна ситуація спостерігається і в Законі України «Про військово-цивільні адміністрації», який також не містить спеціальних норм щодо застосування, контролю або відповідальності за використання систем штучного інтелекту у діяльності військово-цивільних адміністрацій [16].

Отже, на місцевому рівні також простежується нормативна прогалина щодо використання штучного інтелекту у сфері оборони.

Водночас окремі аспекти застосування штучного інтелекту у сфері оборони вже знайшли певне відображення у підзаконному нормативно-правовому регулюванні, зокрема в положеннях відповідних концепцій, стратегій та інших програмних документів. Водночас таке регулювання має переважно рамковий і концептуальний характер та не забезпечує комплексного врегулювання практичних питань використання технологій ШІ в оборонній сфері.

Важливим етапом формування державної політики України у сфері штучного інтелекту стало розпорядженням Кабінету Міністрів України від 2 грудня 2020 року № 1556-р про затвердження Концепції розвитку штучного інтелекту в Україні. Вищезазначений документ визначив основні напрями та пріоритети державної політики щодо впровадження технологій ШІ. Зокрема, відповідно до абзацу 13 розділу «Мета, принципи та строки реалізації Концепції», одним із ключових напрямів передбачено інтеграцію технологій штучного інтелекту в основні сфери суспільного життя, зокрема в економіку, освіту, публічне управління, сектор безпеки й оборони та кіберпростір. Метою такого впровадження визначено, зокрема, підвищення конкурентоспроможності України та зміцнення її позицій у міжнародному середовищі [17].

Окрему увагу в Концепції приділено забезпеченню інформаційної безпеки держави. Так, абзац 17 відповідного розділу передбачає захист національного інформаційного простору від протиправного втручання, а також забезпечення належного та безперебійного функціонування інформаційно-телекомунікаційних систем [17]

Щодо сектору безпеки й оборони Концепція визначає низку напрямів, у яких технології штучного інтелекту можуть бути інтегровані в процеси військового управління та забезпечення обороноздатності держави. Зокрема, йдеться про застосування ШІ у системах командування, управління, зв'язку та розвідки, сучасних зразках озброєння і військової техніки, а також під час збору, систематизації та аналізу великих масивів даних в умовах бойових дій [17].

Перспективними напрямами також визначено використання технологій ШІ у розвідувальній діяльності, спеціальній розвідці та обробленні просторово-картографічної інформації. Важливе місце відведено кібербезпеці, зокрема застосуванню алгоритмів штучного інтелекту для оперативного виявлення кібератак, аналізу шкідливого програмного забезпечення та виявлення аномальної поведінки в інформаційних системах [17].

Крім того, документ передбачає можливість використання ШІ для імітаційного та когнітивного моделювання оперативної обстановки, а також оцінювання бойових спроможностей і потенціалу військових підрозділів. Концепція розвитку штучного інтелекту в Україні фактично заклала нормативно-стратегічні передумови для використання ШІ в оборонній сфері. Водночас її положення мають переважно концептуальний характер і не встановлюють детальних правових механізмів застосування систем штучного інтелекту під час виконання оборонних завдань [17].

Подальший розвиток нормативно-стратегічних засад державної політики у цій сфері пов'язаний із розпорядженням Кабінету Міністрів України від 13 квітня 2024 р. № 320-р «Про схвалення Концепції Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року» [18]. Вищевказаний документ визначає основні стратегічні орієнтири, принципи та пріоритетні напрями розвитку і використання технологій штучного інтелекту в Україні. Водночас положення Концепції охоплюють не лише економічну сферу, а й питання національної безпеки та оборони, що свідчить про поступове розширення державного підходу до використання ШІ.

У безпековому та оборонному вимірі документ акцентує увагу на доцільності інтеграції технологій штучного інтелекту у системи управління військами, озброєння та військову техніку, розвідувальну діяльність, кіберзахист, а також засоби імітаційного моделювання. Все вищевказане спрямоване саме на підвищення ефективності прийняття управлінських рішень, оперативності оброблення інформації, бойових спроможностей та загальної обороноздатності держави .

Зокрема, аналіз зазначених концептуальних документів дає підстави стверджувати, що в Україні вже сформовано певне нормативно-стратегічне підґрунтя для впровадження штучного інтелекту у сфері національної безпеки та оборони. Водночас ці документи переважно визначають загальні напрями, пріоритети та перспективи застосування ШІ, не встановлюючи детальних правових механізмів його використання у військовій сфері. Зокрема, недостатньо врегульованими залишаються питання відповідальності за рішення, прийняті із використанням систем ШІ, контролю за автономними системами, оцінювання та мінімізації ризиків, а також визначення меж допустимого застосування таких технологій під час бойових дій. Це, своєю чергою, актуалізує необхідність подальшого розвитку спеціального нормативно-правового регулювання та формування ризик-орієнтованого підходу до застосування штучного інтелекту в секторі безпеки й оборони.

Окремим напрямом нашого дослідження стало вивчення положень стратегічних документів України, що визначають пріоритети у сфері національної безпеки та оборони, зокрема Стратегії розвитку оборонно-промислового комплексу України [19], Стратегії кібербезпеки України [20] та Стратегії національної безпеки України [21], Стратегії воєнної безпеки України [22]. Проведений аналіз засвідчив, що питання застосування технологій штучного інтелекту в зазначених документах залишається недостатньо деталізованим.

Найбільш виразно згадка про штучний інтелект простежується у Стратегії національної безпеки України [21]. Водночас і в цьому документі ШІ не розглядається як самостійний напрям державної політики у сфері безпеки та оборони. Зокрема, його використання лише опосередковано згадується у пункті 9 розділу ІІ «Поточні та прогнозовані загрози національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов». Отже, на стратегічному рівні технології штучного інтелекту поки що не отримали належного концептуального та нормативного визначення як окремого фактора розвитку оборонних спроможностей і потенційного джерела нових ризиків для національної безпеки.

Висновки та перспективи подальших розвідок

Проведене дослідження засвідчило, що штучний інтелект поступово перетворюється з окремого технологічного інструменту на важливий фактор розвитку спроможностей сектору безпеки й оборони України. В умовах повномасштабної війни його застосування охоплює широкий спектр напрямів — від аналізу великих масивів даних, розвідки та управління військами до використання безпілотних і автономних систем, кіберзахисту, моделювання бойової обстановки та оптимізації оборонної логістики. Водночас ефективність такого впровадження залежить не лише від технологічних можливостей, а й від якості державного управління, нормативно-правового, кадрового та фінансового забезпечення, міжвідомчої координації й механізмів контролю.

Аналіз сучасного стану державної політики України у сфері штучного інтелекту дає підстави визначити її як таку, що значною мірою має реактивний і фрагментарний характер. Практичне впровадження ШІ, особливо у військовій сфері, відбувається швидше, ніж формування відповідної державної регуляторної системи. У результаті виникає розрив між технологічним розвитком і нормативно-інституційними можливостями держави щодо належного його врегулювання.

Дослідження чинного законодавства засвідчило наявність нормативно-правового вакууму щодо безпосереднього застосування технологій штучного інтелекту у сфері оборони. Базові закони у сфері національної безпеки й оборони визначають загальні засади функціонування відповідного сектору, однак не встановлюють спеціальних правил використання систем ШІ, вимог до контролю за ними, розподілу відповідальності за рішення, прийняті із застосуванням таких технологій, а також механізмів управління технологічними ризиками. Аналогічна проблема простежується і на місцевому рівні: законодавство про місцеве самоврядування та військово-цивільні адміністрації не містить спеціального регулювання застосування ШІ під час виконання завдань у сфері оборони.

Водночас в Україні вже сформовано певне нормативно-стратегічне підґрунтя для розвитку технологій штучного інтелекту. Концепція розвитку штучного інтелекту в Україні та подальші програмні документи визначають можливості використання ШІ у військовому управлінні, розвідці, системах командування, управління та зв'язку, озброєнні та військовій техніці, кібербезпеці, аналізі даних і імітаційному моделюванні. Проте ці документи переважно мають рамковий і концептуальний характер та не забезпечують необхідного рівня деталізації практичних процедур і правових гарантій.

Особливої уваги потребує ризик-орієнтований підхід до державного регулювання ШІ у сфері оборони. На сучасному етапі недостатньо лише стимулювати технологічні інновації; необхідно одночасно визначити допустимі межі використання систем ШІ, механізми людського контролю, процедури оцінювання та мінімізації ризиків, правила використання автономних систем, а також відповідальність посадових осіб і операторів за наслідки застосування таких технологій. Саме поєднання технологічного розвитку з належним рівнем державного контролю має стати одним із ключових принципів формування майбутньої політики у цій сфері.

Література

1. Alon-Barkat, S., Busuioc, M. Human-AI Interactions in Public Sector Decision-Making: "Automation Bias" and "Selective Adherence" to Algorithmic Advice. 2021. DOI: https://doi.org/10.1093/jopart/muac007.
2. Kott A., Théron P., Drašar M., Dushku E., LeBlanc B., Losiewicz P., et al. Autonomous Intelligent Cyber-defense Agent (AICA) Reference Architecture. Release 2.0. NATO Research Task Group IST-152. 2018. DOI: https://doi.org/10.48550/arXiv.1803.10664.
3. Harding V. AI Needs You: How We Can Change AI's Future and Save Our Own. Princeton University Press. 2024. URL: https://press.princeton.edu/books/hardcover/9780691244570/ai-needs-you.
4. Савченко В. А., Шаповаленко О. Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. *Сучасний захист інформації.* 2020. № 4(44), С. 6–11. DOI: https://doi.org/10.31673/2409-7292.2020.040611.
5. Шумлянський С. В., Хоменко Є. В., Попрієнко С. В. Ризикоорієнтований підхід до впровадження штучного інтелекту у сфері оборони України: концептуальні засади. *Military Science,* 2025. №3(3), 1С. 47–161. DOI: https://doi.org/10.62524/msj.2025.3.3.11.
6. Краснов Р. В., Шумлянський С. В., Свєтлічний І. В. Використання штучного інтелекту у військовій галузі: ризики та загрози для особового складу. *Human Rights and Public Governance*. Scientific monograph. Riga, Latvia: Baltija Publishing, 2025. С. 356–376. DOI: https://doi.org/10.30525/978-9934-26-608-9-19.
7. Fontes R., Kamminga J. Ukraine a living lab for AI warfare. *National Defense Magazine*. URL: https://www.nationaldefensemagazine.org/articles/2023/3/24/ukraine-a-living-lab-for-ai-warfare.
8. Як ШІ допомагає ефективно бити по ворожому тилу засобами middle strike. Міністерство оборони України. URL: https://mod.gov.ua/explanation/yak-shi-dopomahaie-efektyvno-byty-po-vorozhomu-tylu-zasobamy-middle-strike.
9. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.
10. Про мобілізаційну підготовку та мобілізацію : Закон України від 21.10.1993 № 3543-XII. URL: https://zakon.rada.gov.ua/laws/show/3543-12#Text.
11. Про правовий режим надзвичайного стану : Закон України від 16.03.2000 № 1550-III. URL: https://zakon.rada.gov.ua/laws/show/1550-14#Text.
12. Про оборону України : Закон України від 06.12.1991 № 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text.
13. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998 № 183/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text.
14. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text.
15. Про місцеве самоврядування в Україні : Закон України від 21.05.1997 № 280/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/280/97-%D0%B2%D1%80#Text.
16. Про військово-цивільні адміністрації : Закон України від 03.02.2015 № 141-VIII. URL: https://zakon.rada.gov.ua/laws/show/141-19#Text.
17. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 13.04.2024 р. № 320-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text.

18. Про схвалення Концепції Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року : Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://www.kmu.gov.ua/npas/pro-skhvalennia-kontseptsii-derzhavnoi-tsilovoi-naukovo-tekhnichnoi-prohramy-z-vykorystannia-s320130424.
19. Про рішення Ради національної безпеки і оборони України від 18 червня 2021 року «Про Стратегію розвитку оборонно-промислового комплексу України» : Указ Президента України від 20.08.2021 № 372/2021. URL: https://zakon.rada.gov.ua/laws/show/372/2021#Text.
20. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.
21. Про Стратегію національної безпеки України : РНБО; Рішення від 14.09.2020. URL: https://zakon.rada.gov.ua/laws/show/n0005525-20#Text.
22. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України»: Указ Президента України; Стратегія від 25.03.2021 № 121/2021. URL: https://zakon.rada.gov.ua/laws/show/121/2021#Text.

References

1. Alon-Barkat, S. & Busuioc, M. (2021) Human-AI Interactions in Public Sector Decision-Making: "Automation Bias" and "Selective Adherence" to Algorithmic Advice, *Journal of Public Administration Research and Theory*, vol. 33, no. 1, pp. 153–169. https://doi.org/10.1093/jopart/muac007.
2. Kott, A., Théron, P., Drašar, M., Dushku, E., LeBlanc, B., Losiewicz, P. et al. (2018) *Autonomous Intelligent Cyber-defense Agent (AICA) Reference Architecture*. Release 2.0. NATO Research Task Group IST-152. https://doi.org/10.48550/arXiv.1803.10664.
3. Harding, V. (2024) *AI Needs You: How We Can Change AI's Future and Save Our Own*. Princeton: Princeton University Press. Available at: https://press.princeton.edu/books/hardcover/9780691244570/ai-needs-you.
4. Savchenko, V. A. & Shapovalenko, O. D. (2020) Osnovni napriamy zastosuvannia tekhnolohii shtuchnoho intelektu u kiberbezpetsi [Main areas of application of artificial intelligence technologies in cybersecurity], *Suchasnyi zakhyst informatsii*, no. 4 (44), pp. 6–11. https://doi.org/10.31673/2409-7292.2020.040611.
5. Shumlianskyi, S. V., Khomenko, Ye. V. & Popriienko, S. V. (2025) Ryzykooriientovanyi pidkhid do vprovadzhennia shtuchnoho intelektu u sferi oborony Ukrainy: kontseptualni zasady [Risk-based approach to the implementation of artificial intelligence in the defense sector of Ukraine: Conceptual foundations], *Military Science*, no. 3 (3), pp. 147–161. https://doi.org/10.62524/msj.2025.3.3.11.
6. Krasnov, R. V., Shumlianskyi, S. V. & Svitlychnyi, I. V. (2025) Vykorystannia shtuchnoho intelektu u viiskovii haluzi: ryzyky ta zahrozy dlia osobovoho skladu [The use of artificial intelligence in the military sphere: Risks and threats to personnel], in *Human Rights and Public Governance*. Scientific monograph. Riga: Baltija Publishing, pp. 356–376. https://doi.org/10.30525/978-9934-26-608-9-19.
7. Fontes, R. & Kamminga, J. (2023) Ukraine a living lab for AI warfare, *National Defense Magazine*. Available at: https://www.nationaldefensemagazine.org/articles/2023/3/24/ukraine-a-living-lab-for-ai-warfare.
8. Ministry of Defense of Ukraine (2024) *Yak ShI dopomahaie efektyvno byty po vorozhomu tylu zasobamy middle strike* [How AI helps effectively strike the enemy behind lines using middle strike means]. Official portal. Available at: https://mod.gov.ua/explanation/yak-shi-dopomahaie-efektyvno-byty-po-vorozhomu-tylu-zasobamy-middle-strike.
9. Verkhovna Rada of Ukraine (2018) *Pro natsionalnu bezpeku Ukrainy* [On the national security of Ukraine]. Law of Ukraine of June 21, 2018, No. 2469-VIII. Available at: https://zakon.rada.gov.ua/laws/show/2469-19#Text.
10. Verkhovna Rada of Ukraine (1993) *Pro mobilizatsiinu pidhotovku ta mobilizatsiiu* [On mobilization preparation and mobilization]. Law of Ukraine of October 21, 1993, No. 3543-XII. Available at: https://zakon.rada.gov.ua/laws/show/3543-12#Text.
11. Verkhovna Rada of Ukraine (2000) *Pro pravovyi rezhym nadzvychainoho stanu* [On the legal regime of a state of emergency]. Law of Ukraine of March 16, 2000, No. 1550-III. Available at: https://zakon.rada.gov.ua/laws/show/1550-14#Text.
12. Verkhovna Rada of Ukraine (1991) *Pro oboronu Ukrainy* [On the defense of Ukraine]. Law of Ukraine of December 6, 1991, No. 1932-XII. Available at: https://zakon.rada.gov.ua/laws/show/1932-12#Text.
13. Verkhovna Rada of Ukraine (1998) *Pro Radu natsionalnoi bezpeky i oborony Ukrainy* [On the National Security and Defense Council of Ukraine]. Law of Ukraine of March 5, 1998, No. 183/98-VR. Available at: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text.
14. Verkhovna Rada of Ukraine (2015) *Pro pravovyi rezhym voiennoho stanu* [On the legal regime of martial law]. Law of Ukraine of May 12, 2015, No. 389-VIII. Available at: https://zakon.rada.gov.ua/laws/show/389-19#Text.
15. Verkhovna Rada of Ukraine (1997) *Pro mistseve samovriaduvannia v Ukraini* [On local self-government in Ukraine]. Law of Ukraine of May 21, 1997, No. 280/97-VR. Available at: https://zakon.rada.gov.ua/laws/show/280/97-%D0%B2%D1%80#Text.
16. Verkhovna Rada of Ukraine (2015) *Pro viiskovo-tsyvilni administratsii* [On military-civilian administrations]. Law of Ukraine of February 3, 2015, No. 141-VIII. Available at: https://zakon.rada.gov.ua/laws/show/141-19#Text.
17. Cabinet of Ministers of Ukraine (2024) *Pro skhvalennia Kontseptsii rozvytku shtuchnoho intelektu v Ukraini* [On approval of the Concept for the Development of Artificial Intelligence in Ukraine]. Ordinance of April 13, 2024, No. 320-r. Available at: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text.
18. Cabinet of Ministers of Ukraine (2020) *Pro skhvalennia Kontseptsii Derzhavnoi tsilovoi naukovo-tekhnichnoi prohramy z vykorystannia tekhnolohii shtuchnoho intelektu v priorytetykh haluziakh ekonomiky na mezhuvannia do 2026 roku* [On approval of the Concept of the State Target Scientific and Technical Program for the Use of Artificial Intelligence Technologies in Priority Sectors of the Economy for the Period up to 2026]. Ordinance of December 2, 2020, No. 1556-r. Available at: https://www.kmu.gov.ua/npas/pro-skhvalennia-kontseptsii-derzhavnoi-tsilovoi-naukovo-tekhnichnoi-prohramy-z-vykorystannia-s320130424.
19. President of Ukraine (2021) *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 18 chervnia 2021 roku "Pro Stratehiiu rozvytku oboronno-promyslovoho kompleksu Ukrainy"* [On the decision of the National Security and Defense Council of Ukraine of June 18, 2021 "On the Strategy for the Development of the Defense-Industrial Complex of Ukraine"]. Decree of August 20, 2021, No. 372/2021. Available at: https://zakon.rada.gov.ua/laws/show/372/2021#Text.
20. President of Ukraine (2021) *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy"* [On the decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine"]. Decree of August 26, 2021, No. 447/2021. Available at: https://zakon.rada.gov.ua/laws/show/447/2021#Text.
21. National Security and Defense Council of Ukraine (2020) *Pro Stratehiiu natsionalnoi bezpeky Ukrainy* [On the National Security Strategy of Ukraine]. Decision of September 14, 2020. Approved by Decree of the President of Ukraine of September 14, 2020, No. 392/2020. Available at: https://zakon.rada.gov.ua/laws/show/n0005525-20#Text.
22. President of Ukraine (2021) *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 25 bereznia 2021 roku "Pro Stratehiiu voiennoi bezpeky Ukrainy"* [On the decision of the National Security and Defense Council of Ukraine of March 25, 2021 "On the Military Security Strategy of Ukraine"]. Decree of March 25, 2021, No. 121/2021. Available at: https://zakon.rada.gov.ua/laws/show/121/2021#Text.

Стаття надійшла до редакції / Received 03.08.2026 **Прийнята до друку / Accepted 12.08.2026**
Опубліковано/ Published 04.09.2026