УДК 004.8:351.86(477)"20"
DOI https://doi.org/10.32782/2786-9385/2025-6-14

ШТУЧНИЙ ІНТЕЛЕКТ І НАЦІОНАЛЬНА БЕЗПЕКА: АНАЛІЗ ВЗАЄМОВПЛИВУ

Хома Наталія Михайлівна,
доктор політичних наук, професор,
професор кафедри політології та міжнародних відносин
Національного університету «Львівська політехніка»
ORCID ID: 0000-0002-2507-5741
Scopus-Author ID: 57224475851
Researcher ID: AAX-4615-2021

У статті досліджено взаємовплив ШІ та сфери національної безпеки. Аргументовано, що ШІ здатен як посилити стійкість безпекових систем, так і створити нові виклики для них. Відзначено, що загрози для національної безпеки генерують запити держави й інших зацікавлених а́кторів на технологічні рішення машинного інтелекту. Поставлено завдання з'ясувати: 1) як ШІ на сучасному етапі його розвитку слугує безпековим цілям; 2) як ШІ може підривати національну безпеку; 3) як сучасні держави підходять до використання ШІ у сфері національної безпеки.

Розгляд взаємозв'язку ШІ та національної безпеки дав змогу зробити висновок про формування нової парадигми безпекового мислення, у якій ШІ поступово стає стратегічним чинником. Авторка доводить, що можливості машинного інтелекту здатні посилити стійкість держави у сферах оборони, розвідки, кібербезпеки, управління кризами, захисту критичної інфраструктури та ін. Високий рівень автоматизації, аналітики й адаптивності, притаманний ШІ, суттєво розширює інструментарій забезпечення національної безпеки. Водночас авторка звернула увагу, що стрімкий і недостатньо контрольований розвиток ШІ може створити нові безпекові загрози. Наголошено на зростанні ризиків того, що ШІ-технології можуть вийти за межі державного управління або потрапити під контроль недружніх а́кторів. Підкреслено, що політика у сфері національної безпеки має спрямовувати розвиток ШІ у конструктивному напрямі, це забезпечить баланс між інноваційністю й контролем. Указано на важливість: 1) ухвалення нормативно-правової бази функціонування ШІ у сферах, що становлять стратегічний інтерес для держави; 2) створення інституційного середовища для моніторингу інтеграції ШІ у сферу національної безпеки.

Ключові слова: *штучний інтелект (ШІ), цифрова трансформація, інформаційно-комунікаційні технології, національна безпека, національна безпека та обороноздатність України.*

Khoma N. M. Artificial Intelligence and National Security: Analysis of Mutual Influence

This article examines the interplay between AI and national security. It argues that AI can both strengthen the stability of security systems and create new challenges for them. It is also noted that threats to national security generate demand from states and other interested parties for technological solutions based on machine intelligence. The following three tasks are set: (1) determining how AI serves security purposes at its current stage of development; (2) identifying how AI can undermine national security; (3) examining how modern states approach the use of AI in national security.

Examining the connection between AI and national security reveals that a new security mindset is emerging, in which AI is gradually becoming a strategic factor. The author argues that machine intelligence can strengthen the state's resilience in areas such as defence, intelligence, cybersecurity, crisis management and critical infrastructure protection. The high level of automation, analytics, and adaptability inherent in AI significantly expands the range of tools available for ensuring national security. However, the author notes that the rapid and insufficiently controlled development of AI may create new security threats. She emphasises the growing risk that AI technologies may exceed the scope of state control or fall under the control of hostile actors. The importance of national security policy guiding the constructive development of AI was stressed, as this will ensure a balance between innovation and control. The importance of the following is emphasised: (1) the adoption of a regulatory framework for

AI in areas of strategic interest to the state, and (2) the creation of an institutional environment for monitoring the integration of AI into the sphere of national security.

Key words: *artificial intelligence (AI), digital transformation, information and communication technologies, national security, Ukraine's national security and defence capabilities.*

Актуальність дослідження. У сучасному світі, що характеризується водночас стрімким технологічним розвитком та зростанням глобальних загроз, штучний інтелект (ШІ) щобільше впливає на всі сфери, зокрема й на національну безпеку. Розроблення та впровадження новітніх технологій докорінно змінює аналіз даних, кібербезпеку, охорону кордонів, системи прийняття стратегічних рішень, методи ведення війни, розвідку, протидію дезінформації і т. ін. З одного боку, ШІ відкриває нові можливості для ефективного захисту інтересів держави та її громадян, оперативного реагування на загрози, підвищення точності прогнозування й аналітики. З іншого – створює нові виклики та ризики, пов’язані з неконтрольованим використанням технологій, автономними озброєннями, кібератаками та потенційним порушенням прав людини.

Особливої актуальності тема взаємовпливу ШІ та національної безпеки набуває в умовах глобальної нестабільності, гібридних конфліктів та інформаційної війни, коли технологічна перевага стає одним із ключових чинників національної безпеки. Україна як держава, що функціонує в умовах комплексу надзвичайних викликів, стоїть перед завданням ефективного використання потенціалу ШІ для захисту національних інтересів. Щобільше, війна створила такі умови, коли багато технологічних рішень можуть бути одразу апробовані в умовах реальних ситуацій.

Таким чином, дослідження взаємовпливу ШІ та національної безпеки необхідне для розуміння, як машинний інтелект можна використати в інтересах держави та її громадян і водночас – як можна запобігти деструктивному його застосуванню. Нині ШІ щобільше тісно пов’язують із національною безпекою з позиції їх взаємовпливу: 1) ШІ може зміцнювати або ж підривати національну безпеку; 2) державна політика у сфері національної безпеки може сприяти конструктивній ролі ШІ та мінімізувати ризики, зумовлені машинним інтелектом.

Мета статті – з’ясувати характер взаємовпливу ШІ та сфери національної безпеки. За нашою гіпотезою, з одного боку, ШІ впливає на підвищення стійкості безпекових систем або ж, навпаки, створює нові виклики для них. З іншого боку, загрози у сфері національної безпеки генерують запит держави та інших зацікавлених а́кторів на технологічні рішення, реалізація яких можлива саме завдяки ШІ. Тобто припускаємо наявність взаємовпливу ШІ та сфери національної безпеки. Це вимагає розгляду зв’язків, взаємозалежностей, зворотного зв’язку між сучасними технологіями та сферою національної безпеки в умовах нинішніх викликів.

Для досягнення цієї мети нами поставлено **завдання** з’ясувати: 1) як ШІ на сучасному етапі його розвитку слугує цілям національної безпеки; 2) як ШІ може підривати національну безпеку в цілому або ж окремі види безпеки в системі національної безпеки; 3) як держава, виконуючи функцію забезпечення національної безпеки, підходить до використання ШІ, його унормування, діалогу з технологічними компаніями-розробниками і т. ін. Важливо з’ясувати, наскільки нині сильним є взаємовплив ШІ та національну безпеку, а також якими можуть бути наслідки (конструктивні та деструктивні) від такого взаємовпливу.

Аналіз останніх досліджень і публікацій. Кількість досліджень проблематики ШІ в межах соціальних наук стрімко зростає, про що свідчить бібліометричний аналіз [16]. Цьому сприяють зростання безпекових викликів і водночас прискорення технологічного поступу. На перетині цих процесів виявляються нові проблеми та можливості їх розв’язання, які й стають об’єктами міждисциплінарного вивчення.

Останнім часом активізувалося обговорення, як ШІ може вплинути на

національну безпеку в найближчій та довгостроковій перспективі. Ці дискусії відбуваються, найперше, на тлі загострення конкуренції між США та Китаєм за технологічне лідерство.

Ґ. Аллен і Т. Чан довели наявність трансформаційного потенціалу ШІ для національної безпеки [9]. М. Раска, К. Жиск та І. Бауерс дослідили вплив революційних технологій Четвертої промислової революції на військові інновації та застосування сили. Дослідники запропонували авторський прогноз, який вплив ШІ, робототехніка, нанотехнології і т. ін. можуть мати на майбутні конфлікти [17]. Також М. Раска у співавторстві з Р.А. Бітцінґером дослідили роль ШІ для оборонних інновацій [18].

Низка вітчизняних учених із різних галузей знання (політична наука, економічна безпека, державне управління, право та ін.) розглянули значення машинного інтелекту в контексті інноваційних підходів до забезпечення національної безпеки. Так, С. Білоус, Л. Самойленко та Л. Бандунко [1] акцентували на значенні ШІ та інших новітніх технологічних підходів для зміцнення стійкості України в умовах сучасних викликів.

Тематика є у фокусі уваги юридичної науки. Так, Н. Пацурія [5] вивчає правові проблеми впровадження технологій ШІ в забезпечення національної безпеки. Дослідниця слушно відзначає відсутність в Україні документа на зразок Стратегії розвитку ШІ у сфері забезпечення національної безпеки та обороноздатності України попри ухвалення ще наприкінці 2020 р. Концепції розвитку штучного інтелекту в Україні [6]. Зауважимо, що від часу ухвалення згаданої концепції лише затверджувалися плани заходів з її реалізації (на 2021–2024, 2025–2026 рр.), реорганізовано Інститут проблем штучного інтелекту і под. Сьогодні відсутнє національне законодавство, яке б урегульовувало застосування ШІ у сфері забезпечення національної безпеки та обороноздатності України як під час воєнного стану, так і на повоєнному етапі.

У дослідженні Д. Гребенюка [2] розглянуто проблеми правового регулювання застосування ШІ у сфері національної безпеки. Слушно відзначено, що правові системи не встигають адаптуватися до стрімкого розвитку технологій ШІ, що створює виклики у сфері регулювання використання даного явища в контексті національної безпеки.

Попри доволі широкий спектр наявних досліджень, взаємовпливи ШІ та сфери національної безпеки з позиції політичної науки лише розпочинаються.

Виклад основного матеріалу дослідження. Роль ШІ у системі забезпечення національної безпеки невпинно зростає. Це пояснюється пропозицією нових методів виявлення та прогнозування загроз, більш ефективних та оперативних інструментів протидії різноманітним викликам і т. ін. ШІ автоматизує процеси, швидко та точно аналізує дані, обробляє великі масиви різнорідних даних. Застосування ШІ «дає змогу вдосконалювати процеси моніторингу та аналітики, що забезпечує підвищену готовність до потенційних ризиків» [2, с. 125]. Однак машинний інтелект може як зміцнювати безпеку держави, так і створювати нові складні загрози. Для суб'єктів, відповідальних за сферу національної безпеки, важливо врахувати як позитивні, так і негативні аспекти застосування ШІ.

Потенціал впливу ШІ на національну безпеку фіксується у низці сфер. Звернемо увагу на основні.

1. *Військові технології та оборона.* ШІ переосмислює традиційні методи ведення війни, а також сфери, де ця війна ведеться. Насамперед сюди належать автономні системи озброєння (АСО) на зразок дронів, бойових роботів. Їх застосування не обмежується лише військовою сферою, бо вони «дедалі частіше впроваджуються у прикордонному контролі, діяльності правоохоронних органів, антитерористичних операціях, підтриманні громадського порядку, стеженні за масовими заходами та громадськими зібраннями» [4, с. 190]. Попри численні переваги АСО (швидкість, точність, мінімізація людських утрат і т. ін.), ставиться питання про те, що їх застосування супроводжується істотними юри-

дичними, етичними та технологічними ризиками.

ШІ успішно використовується для розвідки та аналізу даних завдяки здатності швидко обробити великі обсяги інформації, а отже, виявити загрози. Прикладами є супутникові знімки, перехоплені переговори тощо. Розвідка на основі відкритих джерел (OSINT), підсилена ШІ, стає фундаментом національної безпеки багатьох держав. Сучасні розвідки трансформуються шляхом звернення до відкритих джерел, швидкої обробки даних у реальному часі з використанням ШІ, розвитку партнерства між державою та приватним сектором (технологічними компаніями).

Українські технологічні компанії також використовують OSINT та ШІ проти російської агресії для відстеження військових переміщень, викриття дезінформації і т. ін. ШІ-моделі обробляють зображення із супутників або дронів для автоматичного розпізнавання типів техніки, військових об'єктів чи руху колон. Дані з OSINT-джерел і ШІ-аналітики інтегруються у військові системи управління, що допомагає визначити пріоритетні цілі, підвищити точність артилерійських ударів, забезпечують синхронізацію між підрозділами і т. ін.

Під час російсько-української війни вперше відкриті дані та ШІ використовуються для документування воєнних злочинів у режимі реального часу. Сучасні технології дають змогу опрацьовувати супутникові знімки, контент соціальних мереж тощо для збору доказів та подальшого притягнення винних до відповідальності. Osavul, Mantis Analytics як ШІ-аналітики використовуються для швидкого виявлення дезінформації та аналізу великих обсягів даних [14]. Цей напрям активізований практично одразу після початку повномасштабного вторгнення.

2. *Кібероперації та інформаційна безпека.* Значення ШІ є критично важливим, позаяк фальсифіковані відео/аудіо (діпфейки) можуть спричинити дестабілізацію, дискредитацію лідерів, провокації та ін. Також ШІ-боти можуть впливати на вибори, поширювати дезінформацію, розпалювати соціальні конфлікти, поширювати мову ворожнечі. У цьому контексті роль ШІ є деструктивною. Отже, виникає питання про те, чи можна потенціал ШІ використати з протилежною метою, для нейтралізації створеного деструктиву. Образно кажучи, «ШІ проти ШІ». Боротися з діпфейками, створеними ШІ, можна саме за допомогою ШІ [8].

Також ШІ може застосовуватися для виявлення уразливостей в енергетичних системах, транспорті, банках, аеропортах, телекомунікації, системі охорони здоров'я та ін., тобто йдеться про зміцнення стійкості критичної інфраструктури. Зокрема, ENISA (Агентство ЄС із кібербезпеки) у звіті за 2024 р. [11] рекомендує інтегрувати ШІ-інструменти у системи захисту критичної інфраструктури (особливо енергетики, транспорту та охорони здоров'я). До прикладу, щоб запобігти кібератакам на сервери українських освітніх установ, ШІ може здійснювати постійний моніторинг мережевої інфраструктури закладів освіти і своєчасно виявляти й блокувати загрози. Системи на основі ШІ та обробки Big Data можуть розпізнавати патерни атак і аномальну активність, що може свідчити про спроби несанкціонованого доступу до систем [3]. Водночас атаки на базі машинного інтелекту здатні виводити з ладу енергетичні та транспортні мережі, чим підривається безпека держави та її громадян. Низка кіберінцидентів порушувала роботу енергетики, транспорту, аеропортів, залізниць, портів. Прикладом є атака у вересні 2025 р. на американського IT-провайдера Collins Aerospace, яка на кілька днів зупинила системи реєстрації в аеропортах Європи.

ШІ може посилити безпеку критичної інфраструктури, використовуючи передові механізми виявлення та реагування на загрози. Системи виявлення та запобігання вторгненням на основі ШІ здатні розпізнавати і запобігати деструктивній діяльності, а також перехоплювати спроби несанкціонованого доступу. Також дослідники [7] відзначають потенціал ШІ у забезпеченні кібербезпеки військових мереж.

3. *Безпека державних інституцій.* Тут ідеться передусім про прогнозування криз або певних подій, що підривають стійкість системи національної безпеки. Аналітика на основі ШІ допомагає передбачити соціальні заворушення, економічні потрясіння, загрози тероризму [12]. Наприклад, ШІ можна використовувати для прогнозування тероризму шляхом аналізу метаданих комунікацій, інформації про фінансові операції, активності на вебсторінках. Величезні обсяги особистої та професійної інформації, оброблені ШІ, можуть виявити зміни у моделях поведінки та взаємодіях людей, прогнозування їхньої поведінки [13]. У сфері безпеки ШІ працює у напрямі виявлення внутрішніх загроз у державних інституціях. Машинний інтелект здатен аналізувати поведінку співробітників державних органів, виявлення тих, хто може співпрацювати з ворогом. AI-системи сигналізують про підозрілі дії працівників, що мають доступ до державної чи військової таємниці. Системи відеоспостереження з ШІ використовуються для захисту стратегічних об'єктів, контролю за периметром у режимі 24/7. Також ШІ забезпечує біометричну систему доступу до низки державних установ, щоб мінімізувати ризики несанкціонованого проникнення.

4. *Охорона державних кордонів.* Технологія комп'ютерного зору (Computer Vision) допомагає автоматичному відстеженню потоків людей, транспортних засобів, змін у поведінці на кордоні завдяки системі камер. Це стосується як пунктів пропуску на кордоні, так і портів, залізниці і т. ін. Також ШІ здатен збирати та аналізувати інформацію зі соціальних мереж, форумів, чатів тощо про підготовку незаконних перетинів, контрабанду і т. ін.; прикладами є європейські програми моніторингу soft intelligence.

Машинний інтелект використовується для ідентифікації осіб, виявлення контрабанди через кордони [19]. Використовується комп'ютерний зір (для сканерів багажу), який дає змогу отримувати корисну інформацію із цифрових зображень або відео. AI аналізує рентген-зображення у пошуках зброї, наркотиків, незадекларованої готівкової валюти та банківських металів і т. ін. ШІ може «бачити» підозрілі форми, навіть приховані у пакуванні. Це цінні в безпековому аспекті технології, які використовуються не лише на транспортних об'єктах, а й в урядових і дипломатичних установах, судах, місцях масових заходів, релігійних та історичних місцях тощо.

Також ШІ автоматично порівнює обличчя з базами даних паспортів, віз, «чорних списків», виявляє спроби використати чужі документи. Коли йдеться про відбитки пальців, то сенсор з ШІ-алгоритмами порівнюють відбитки із базою даних. Окремі аеропорти в США, державах Азії, Близького Сходу, впровадили технологію іридіальної (сітківкової) біометрії. Також прикордонні пункти послуговуються різними інструментами на базі ШІ, щоб виявляти підробку паспортів, візових етикеток, заяв-дозволів на вивезення дітей за кордон, документів, які дають в умовах воєнного стану право на виїзд за кордон та ін.

Досягнення в галузі камер безпеки зі ШІ трансформували виявлення загроз у режимі реального часу на лінії державного кордону. Ці системи інтегрують машинне навчання та комп'ютерний зір для виявлення підозрілої поведінки, відстеження несанкціонованого доступу та миттєвого надсилання сповіщень до центрів прийняття рішень.

AI для дронів і автономних патрулів нині має особливе значення для патрулювання важкодоступних ділянок кордону та передачі відеопотоку для автоматичного аналізу. Постійний моніторинг великих ділянок можливий без залучення великої кількості людей та з вищою точністю. Це підвищує ефективність охорони кордону. Нині це дуже важливо, особливо для держав, які межують із державами-агресорами чи їхніми союзниками. До прикладу, рішення у цьому напрямі пропонує ізраїльська компанія Mer Group [10]. ШІ використовується для класифікації прикордонних інцидентів у режимі реального часу та захисту прикордонних периметрів.

Технології спостереження (оптичні системи, радари, датчики тощо) розгортаються вздовж кордонів, ідентифікують та відстежують будь-який рух і передають дані безпосередньо алгоритмам машинного навчання, які інтегровані в національний центр управління та контролю прикордонного захисту.

Ми вказали лише на кілька напрямів у системі національної безпеки, де роль ШІ посилюється. Поза межами залишено біо- та санітарно-епідеміологічну, екологічну, техногенну, енергетичну та інші види безпеки. Водночас події довкола пандемії COVID-19, блекаутів на Запорізькій АЕС, численних наслідків кліматичних змін, DDoS-атак і т. ін. демонструють перспективи ШІ у різних сферах національної безпеки.

ШІ отримує дуже суперечливі оцінки, особливо у сфері національної безпеки. До прикладу, Дж. Салліван, радник Дж. Байдена з національної безпеки, назвав ШІ найбільшою загрозою національній безпеці США [15]. Відзначимо, що за нинішньої адміністрації Д. Трампа у питаннях регулювання ШІ на перше місце поставлено саме національну безпеку та інтереси ІТ-індустрії, а не користувачів (як у ЄС). Про це можна зробити висновок на основі Плану дій США щодо ШІ [21].

ШІ трансформують міжнародне безпекове середовище. Однак, як машинний інтелект це робить і які наслідки цього процесу, має широкий спектр оцінок – від здатності посилювати національну безпеку до, навпаки, створення нових загроз. За нашою оцінкою, для тих держав, які активно інвестують у технології на основі ШІ, його вплив на національну безпеку продовжує зростати і при цьому створює як можливості, так і виклики.

Щоб ШІ став партнером, а не проблемою для національної безпеки, необхідний системний підхід. Прикладом можна назвати Лабораторію досліджень безпеки на основі штучного інтелекту (Laboratory for AI Security Research, LASR). Вона функціонує від кінця 2024 р. у Великій Британії завдяки урядовій ініціативі для захисту від руйнівного використання технологій ШІ ворожими державами, передусім Росією. Також LASR спрямована з'ясувати, як можна зменшити ризики від машинного інтелекту. LASR аналізує вплив ШІ на національну безпеку та має завданням системно вивчати, як його можливості використовують держави-агресори.

Упровадження ШІ у сферу національної безпеки має труднощі, які відсутні в недержавному секторі. Зокрема: 1) ризики вищі, а наслідки невдачі – серйозніші. Якщо помилка в комерційному чат-боті може призвести до плутанини чи певних фінансових втрат, то помилка у зведеній розвідувальній інформації – до цілковитого провалу місії; 2) інструменти ШІ повинні інтегруватися із застарілими системами у сфері національної безпеки, які, своєю чергою, можуть не підтримувати сучасне програмне забезпечення; 3) багато даних у сфері національної безпеки та оборони є закритими. Їх треба зуміти захистити на всіх етапах життєвого циклу ШІ [20].

Системи ШІ є динамічними за природою. Тож одночасно з тестуванням та оцінюванням вони потребують постійного моніторингу в такому середовищі, як сфера національної безпеки через підвищені ризики, чутливість, закритість інформації. Важливо вбудовувати нагляд із боку людини. ШІ не замінить прийняття рішення людиною, але може покращити та доповнити процес ухвалення рішень. Для сфери національної безпеки ШІ може бути корисний тим, що дає змогу відповідним організаціям приймати рішення за менший час, зменшити рутинну роботу персоналу, підвищити обізнаність про складні середовища з багатьма складниками.

Перспективи ШІ у сфері національної безпеки узалежнені від поєднання інновації з обережністю, а також використання адаптивних стратегій, чіткої підзвітності та постійної взаємодії між людьми та ШІ для ефективного досягнення цілей у сфері національної безпеки.

Висновки. Розгляд взаємозв'язку між ШІ та національною безпекою дає змогу зробити висновок про формування нової парадигми безпекового мислення, у якій

ШІ поступово стає одним із ключових стратегічних чинників. ШІ має потенціал змінювати баланс сил. З одного боку, можливості, які відкриває застосування ШІ, створюють умови для якісного посилення стійкості держави в таких сферах, як оборона, розвідка, кібербезпека, управління кризами та захист критичної інфраструктури тощо. Високий рівень автоматизації, аналітики й адаптивності, притаманний ШІ, суттєво розширює інструментарій забезпечення національної безпеки.

Водночас швидкий і недостатньо контрольований розвиток ШІ може не лише знецінити традиційні підходи до безпеки, а й створити нові технологічно складні загрози. До таких загроз належать використання ШІ для здійснення кібератак, маніпуляцій інформаційним простором, поширення дезінформації, розроблення автономних озброєнь без чіткого регуляторного контролю. У перспективі зростає ризик, що ШІ-технології можуть вийти за межі державного управління, потрапити під контроль ворожих а́кторів.

У цьому контексті особливого значення набуває державна політика у сфері національної безпеки, яка має виконувати регулятивну, стратегічну й етичну функції. Саме ця політика здатна спрямовувати розвиток ШІ у безпечний формат, забезпечуючи баланс між інноваційністю й контролем. Ідеться про потребу формування комплексної нормативно-правової бази, створення інституційного середовища для моніторингу і відповідальності, стимулювання розвитку вітчизняних ШІ-рішень, а також активну участь у міжнародному діалозі щодо глобального регулювання цих технологій.

Отже, ефективне поєднання технологічного потенціалу ШІ з чіткою державною політикою у сфері національної безпеки є необхідною умовою збереження суверенітету, стабільності та стійкості держави в умовах цифрової трансформації. Успішне розв’язання цього завдання передбачає не лише технологічну модернізацію, а й оновлення стратегічного бачення безпеки, адаптованого до викликів і можливостей нової цифрової доби.

ЛІТЕРАТУРА:

1. Білоус С., Самойленко Л., Бандунко Л. Інноваційні підходи до забезпечення національної безпеки: міжнародний досвід та перспективи впровадження. *Public Networks and Communications*. 2024. № 2. С. 19–24. DOI: 10.31558/3083-5895.2024.2.3

2. Гребенюк Д. Використання штучного інтелекту в системі забезпечення національної безпеки: перспективи, виклики та правові аспекти. *Національні інтереси України*. 2024. № 5(5). С. 121–128. DOI: 10.52058/3041-1793-2024-5(5)-121-128

3. Дорогий Я., Цуркан В., Дорога-Іванюк О. Використання штучного інтелекту під час захисту критичної інфраструктури установ освітньої галузі. *Інформаційна безпека та інформаційні технології* : зб. доп. V Міжн. наук.-практ. конф., м. Львів, 27 листопада 2024 р. Львів : ЛДУ БЖД, 2024. С. 296–298.

4. Кутовий О., Бурма С. Автономні системи озброєнь і штучний інтелект як виклик міжнародному гуманітарному праву та правам людини. *Науковий вісник Ужгородського національного університету*. *Серія «Право»*. 2025. № 90(5). С. 185–194. DOI: 10.24144/2307-3322.2025.90.5.22

5. Пацурія Н. Упровадження технологій штучного інтелекту в забезпечення національної безпеки та обороноздатності України: правові проблеми і перспективи повоєнного періоду. *Теорія і практика інтелектуальної власності*. 2023. № 3. С. 68–78. DOI: 10.34142/23121661.2023.38.05

6. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220 (дата звернення: 17.10.2025).

7. Трофименко О., Соколов А., Чикунов П., Ахмаметьєва Г., Манаков С. ШІ у військовій кібернетичній сфері. *Технології та інженерія*. 2024. № 4(21). С. 85–92. DOI: 10.30857/2786-5371.2024.4.8

8. Abbas F., Taeihagh A. Unmasking Deepfakes: A Systematic Review of Deepfake Detection and Generation Techniques Using Artificial Intelligence. *Expert Systems with Applications*. 2024. № 252 (B), article 124260. DOI: 10.1016/j.eswa.2024.124260

9. Allen G., Chan T. Artificial Intelligence and National Security. *Belfer Center for Science and International Affairs. Harvard Kennedy School.* URL: https://www.belfercenter.org/publication/artificial-intelligence-and-national-security (дата звернення: 18.10.2025).

10. AI-driven Border Security. *MER Group.* URL: https://mer-group.com/ai-driven-border-security/ (дата звернення: 18.10.2025).

11. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity, 2024. DOI: 10.2824/0710888

12. Koutidis G., Loumponias K., Tsikrika T., Vrochidis S., Kompatsiaris I. Towards AI-Driven Prediction of Terrorism Risk Based on the Analysis of Localized Web News. IEEE Access. 2024. № 12. P. 167288–167299. DOI: 10.1109/ACCESS.2024.3485913

13. Madaoui N. The Role of Artificial Intelligence in Combating Cyber Terrorism. Ius Et Scientia. 2023. № 9 (2). P. 221–227. DOI: 10.12795/IESTSCIENTIA.2023.i02.10

14. OSINT та ШІ: як технології допомагають документувати воєнні злочини. *Quo Vadis* URL: https://quovadis.in.ua/biznes/dim/3211-o (дата звернення: 17.10.2025).

15. Press Briefing by Press Secretary Karine Jean-Pierre and National Security Advisor Jake Sullivan. *The White House*. URL: https://bidenwhitehouse.archives.gov/briefing-room/press-briefings/2025/01/13/press-briefing-by-press-secretary-karine-jean-pierre-and-national-security-advisor-jake-sullivan-20/ (дата звернення: 17.10.2025).

16. Prieto-Gutierrez J.-J., Segado-Boj F., Da Silva França F. Artificial Intelligence in Social Science: A Study Based on Bibliometrics Analysis. *Human Technology.* 2023. № 19(2). P. 149–162. DOI: 10.48550/arXiv.2312.10077

17. Raska M., Bitzinger R.A. The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories (1st ed.). London: Routledge, 2023. 284 p.

18. Raska M., Zysk K., Bowers I. Defence Innovation and the 4th Industrial Revolution: Security Challenges, Emerging Technologies, and Military Implications (1st ed.). London: Routledge, 2022. 202 p.

19. Rinaldi A., Teo S.A. The Use of Artificial Intelligence Technologies in Border and Migration Control and the Subtle Erosion of Human Rights. *International and Comparative Law Quarterly*. 2025. № 74(1). P. 61–89. DOI:10.1017/S0020589325000090

20. Rishel P., Smith C., O'Hearn B., Creel R. Artificial Intelligence in National Security: Acquisition and Integration. *Carnegie Mellon University*. URL: https://doi.org/10.58012/gfnb-pr02 (дата звернення: 12.10.2025).

21. Winning the race: America's AI action plan. *The White House*. URL: https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf (дата звернення: 17.10.2025).

REFERENCES:

1. Bilous, S., Samoilenko, L., & Bandunko, L. (2024). Innovatsiini pidkhody do zabezpechennia natsionalnoi bezpeky: mizhnarodnyi dosvid ta perspektyvy vprovadzhennia [Innovative Approaches to Ensuring National Security: International Experience and Perspectives of Implementation]. *Public Networks and Communications*, *2*, 19–24. DOI: 10.31558/3083-5895.2024.2.3 [in Ukrainian].

2. Hrebeniuk, D. (2024). Vykorystannia shtuchnoho intelektu v systemi zabezpechennia natsionalnoi bezpeky: perspektyvy, vyklyky ta pravovi aspekty [The Application of artificial intelligence in the national security system: Prospects, Challenges and Legal Aspects]. *Natsionalni interesy Ukrainy* [*National Interests of Ukraine*], *5*(5), 121–128. DOI: 10.52058/3041-1793-2024-5(5)-121-128 [in Ukrainian].

3. Dorohyi, Ya., Tsurkan, V., & Doroha-Ivaniuk, O. (2024). Vykorystannia shtuchnoho intelektu pry zakhysti krytychnoi infrastruktury ustanov osvitnoi haluzi [The Use of Artificial Intelligence in Protecting Critical Infrastructure in Educational Institutions]. In: *Informatsiina bezpeka ta informatsiini tekhnolohii*: zbirnyk dopovidei V Mizhnarodnoi naukovo-praktychnoi konferentsii [Information Security and Information Technology:

Proceedings of the V International Scientific and Practical Conference] (Lviv, 27.11.2024). Lviv: Lvivskyi derzhavnyi universytet bezpeky zhyttiediialnosti, 296–298 [in Ukrainian].

4. Kutovyi, O., & Burma, S. (2025). Avtonomni systemy ozbroien i shtuchnyi intelekt yak vyklyk mizhnarodnomu humanitarnomu pravu ta pravam liudyny [Autonomous weapon systems and artificial intelligence as a challenge to international humanitarian law and human right]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo* [*Uzhhorod National University Herald. Series: Law*], *90*(5), 185–194. DOI: 10.24144/2307-3322.2025.90.5.22 [in Ukrainian].

5. Patsuriia, N. (2023). Uprovadzhennia tekhnolohii shtuchnoho intelektu v zabezpechennia natsionalnoi bezpeky ta oboronozdatnosti Ukrainy: pravovi problemy i perspektyvy povoiennoho periodu [Implementation of Artificial Intelligence Technologies for Ensuring National Security and Defense Capability of Ukraine: Legal Issues and Prospects for the Post-War Period]. *Teoriia i praktyka intelektualnoi vlasnosti* [*Theory and Practice of Intellectual Property*], *3*, 68–78. DOI: 10.34142/23121661.2023.38.05 [in Ukrainian].

6. Pro skhvalennia Kontseptsii rozvytku shtuchnoho intelektu v Ukraini: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 02.12.2020 № 1556-r. [On approval of the Concept for the development of artificial intelligence in Ukraine: Resolution of the Cabinet of Ministers of Ukraine dated December 2, 2020, No. 1556-r.] *Uriadovyi portal* [*Government Portal*]. Retrieved from https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220 [in Ukrainian].

7. Trofymenko, O., Sokolov, A., Chykunov, P., Akhmametieva, H., & Manakov, S. (2024). AI u viiskovii kibernetychnii sferi [AI in the Military Cyber Domain]. *Tekhnolohii ta inzheneriia* [*Technologies and Engineering*], *4*(21), 85–92. DOI: 10.30857/2786-5371.2024.4.8 [in Ukrainian].

8. Abbas, F., & Taeihagh, A. (2024). Unmasking Deepfakes: A Systematic Review of Deepfake Detection and Generation Techniques Using Artificial Intelligence. *Expert Systems with Applications*, *252*(B), article 124260. DOI: 10.1016/j.eswa.2024.124260 [in English].

9. Allen, G., & Chan, T. (2017)/ Artificial Intelligence and National Security. Belfer Center for Science and International Affairs, Harvard Kennedy School. Retrieved from https://www.belfercenter.org/publication/artificial-intelligence-and-national-security [in English].

10. AI-driven Border Security (2025). *MER Group.* Retrieved from https://mer-group.com/ai-driven-border-security/ [in English].

11. ENISA Threat Landscape 2024 (2024). Brussels: European Union Agency for Cybersecurity. DOI: 10.2824/0710888 [in English].

12. Koutidis, G., Loumponias, K., Tsikrika, T., Vrochidis. S., & Kompatsiaris, I. (2024). Towards AI-Driven Prediction of Terrorism Risk Based on the Analysis of Localized Web News. IEEE Access, *12*, 167288–167299. DOI: 10.1109/ACCESS.2024.3485913 [in English].

13. Madaoui, N. (2023). The Role of Artificial Intelligence in Combating Cyber Terrorism. Ius Et Scientia, *9*(2), 221–227. DOI: 10.12795/IESTSCIENTIA.2023.i02.10 [in English].

14. OSINT ta AI: yak tekhnolohii dopomahaiut dokumentuvaty voienni zlochyny [OSINT and AI: how technology helps document war crimes] (2025). *Quo Vadis*. Retrieved from https://quovadis.in.ua/biznes/dim/3211-o [in Ukrainian].

15. Press Briefing by Press Secretary Karine Jean-Pierre and National Security Advisor Jake Sullivan (2025). *The White House*. Retrieved from https://bidenwhitehouse.archives.gov/briefing-room/press-briefings/2025/01/13/ press-briefing-by-press-secretary-karine-jean-pierre-and-national-security-advisor-jake-sullivan-20/ [in English].

16. Prieto-Gutierrez, J.-J., Segado-Boj, F., & Da Silva França, F. (2023). Artificial Intelligence in Social Science: A Study Based on Bibliometrics Analysis. *Human Technology, 19*(2), 149–162. DOI: 10.48550/arXiv.2312.10077 [in English].

17. Raska, M., & Bitzinger, R.A. (Eds.) (2023). The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories (1st ed.). London: Routledge. 284 p. [in English].

18. Raska, M., Zysk, K., & Bowers, I. (Eds.) (2022). Defence Innovation and the 4th Industrial Revolution: Security Challenges, Emerging Technologies, and Military Implications (1st ed.). London: Routledge, 202 p. [in English].

19. Rinaldi, A., & Teo, S.A. (2025). The Use of Artificial Intelligence Technologies in Border and Migration Control and the Subtle Erosion of Human Rights. *International and Comparative Law Quarterly*, *74*(1), 61–89. DOI:10.1017/S0020589325000090 [in English].

20. Rishel, P., Smith, C., O'Hearn, B., & Creel, R. (2025). Artificial Intelligence in National Security: Acquisition and Integration. *Carnegie Mellon University*. Retrieved from https://doi.org/10.58012/gfnb-pr02 [in English].

21. Winning the race: America's AI action plan (2025). *The White House*. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2025/07/ Americas-AI-Action-Plan.pdf [in English].

Стаття надійшла до редакції 20.10.2025
Стаття прийнята 15.11.2025
Статтю опубліковано 30.12.2025