

**Штучний інтелект у військовій сфері:
міжнародно-правове регулювання та безпекові виклики**

Аблазов Іван Валерійович¹

Опубліковано	Секція	УДК
30.08.2025	Право	34.096+004.89(045)

DOI: <https://doi.org/10.5281/zenodo.21072124>

Анотація. У статті досліджено застосування штучного інтелекту у військовій сфері крізь призму міжнародно-правового регулювання, безпекових викликів та етичних ризиків, котрі спричиняють дані процеси. Актуальність теми зумовлена тим, що в умовах війни Росії проти України ШІ став важливим інструментом розвідки, управління військами, обробки великих масивів даних, логістики, кібербезпеки, моделювання операцій, застосування автономних платформ і підтримання управлінських рішень. Водночас, автономізація військових систем створює ризики втрати людського контролю, помилкової ідентифікації цілей, ескалації конфлікту та ускладнення юридичної відповідальності.

Метою статті є виявлення й аналіз особливостей застосування штучного інтелекту у військовій сфері на основі визначення специфіки міжнародно-правового регулювання використання таких технологій, виділення ключових безпекових, правових та етичних викликів, а також окреслення напрямів удосконалення міжнародного та національного нормативно-правового регулювання військового ШІ.

Методологічну основу дослідження становлять діалектичний метод, системний метод, формально-юридичний метод, порівняльно-правовий метод, метод правового моделювання, метод аналізу міжнародних відносин та етичний підхід.

Розкрито основні напрями використання ШІ у військовій сфері, зокрема, в розвідці, спостереженні, кібербезпеці, автономних і напіваавтономних системах, генеративному ШІ та автоматизованому аналізі бойової обстановки. Проаналізовано застосовність принципів міжнародного гуманітарного права, зокрема, розрізнення, пропорційності, обережності, військової необхідності та заборони надмірних страждань. Особливу увагу приділено змістовному контролю людини, відповідальності держав, командирів, операторів і розробників, а також фрагментарності міжнародного регулювання. Обґрунтовано необхідність формування комплексної нормативної моделі, що поєднуватиме міжнародне право, національне законодавство, технічні стандарти, правові огляди нових систем і гарантії відповідального застосування ШІ.

Ключові слова: штучний інтелект, міжнародне гуманітарне право, міжнародно-правове регулювання, міжнародна безпека, збройний конфлікт, НАТО, технології подвійного використання.

¹ кандидат політичних наук, професор,
начальник кафедри міжнародних відносин і стратегічних комунікацій,
Воєнно-дипломатична академія імені Євгенія Березняка,
04119, Україна, м. Київ, вул. Юрія Іллєнка, 81,
ablazov@ukr.net,
ORCID: <https://orcid.org/0000-0001-6293-8043>

Artificial Intelligence in the Military Sphere: International Legal Regulation and Security Challenges

Abstract. The article examines the use of artificial intelligence in the military sphere through the prism of international legal regulation, security challenges, and ethical risks caused by these processes. The relevance of the topic is determined by the fact that, in the context of Russia's war against Ukraine, AI has become an important tool for intelligence, command and control, processing large amounts of data, logistics, cybersecurity, operational modelling, the use of autonomous platforms, and decision-making support. At the same time, the autonomization of military systems creates risks related to the loss of human control, erroneous target identification, conflict escalation, and the complication of legal responsibility.

The purpose of the article is to identify and analyze the specific features of the use of artificial intelligence in the military sphere on the basis of determining the specific features of international legal regulation of the use of such technologies, identifying key security, legal, and ethical challenges, as well as outlining directions for improving international and national legal regulation of military AI.

The methodological basis of the study consists of the dialectical method, the systemic method, the formal legal method, the comparative legal method, the method of legal modelling, the method of international relations analysis, and the ethical approach.

The article reveals the main areas of AI application in the military sphere, in particular, in intelligence, surveillance, cybersecurity, autonomous and semi-autonomous systems, generative AI, and automated analysis of the battlefield environment. The applicability of the principles of international humanitarian law is analyzed, in particular, the principles of distinction, proportionality, precaution, military necessity, and the prohibition of unnecessary suffering. Particular attention is paid to meaningful human control, the responsibility of states, commanders, operators, and developers, as well as the fragmented nature of international regulation. The need to develop a comprehensive regulatory model combining international law standards, national legislation, technical standards, legal reviews of new systems, and guarantees for the responsible use of AI is substantiated.

Keywords: artificial intelligence, International Humanitarian Law, international legal regulation, international security, armed conflict, NATO, dual-use technologies.

Постановка проблеми. В умовах повномасштабної війни Росії проти України штучний інтелект (ШІ) став невід'ємним засобом, що використовується у військовій сфері, адже за його допомогою активно змінюються підходи до розвідки, управління військами, обробки даних, логістики, кібербезпеки, моделювання операцій, застосування автономних платформ і прийняття управлінських рішень під час ведення бойових дій. Якщо на попередніх етапах технологічного розвитку цифрові системи виконували переважно допоміжну функцію, то нині алгоритми машинного навчання, генеративний ШІ, автономні безпілотні апарати, автоматизовані системи управління та засоби прогнозової аналітики стають складовими військового планування і застосування бойових засобів.

Відтак, наразі зростає наукова актуальність розгляду даної проблематики, адже використання ШІ у військовій сфері створює одночасно нові можливості й нові загрози. З одного боку, ШІ здатен значно прискорити обробку великих масивів даних, підвищити точність розвідки, поліпшити логістику, забезпечити швидше виявлення загроз, зменшити ризики для особового складу та посилити ефективність оборонних операцій. З іншого боку, автономізація військових систем породжує низку правових, етичних і безпекових ризиків, пов'язаних із делегуванням алгоритмам функцій, які

можуть координувати застосування сили, ураження цілей чи ідентифікацію цивільних осіб, що в результаті може призвести до ескалації конфлікту або втрати належного контролю над процесами з боку людини.

Особливо гострою є проблема міжнародно-правового регулювання військового використання ШІ. Звісно, міжнародне гуманітарне право містить загальні принципи, які застосовуються для регулювання застосування будь-яких засобів і методів ведення війни, зокрема, принципи розрізнення, пропорційності, запобігання надмірним стражданням, військової необхідності та обережності під час нападу. Водночас, чинні міжнародні договори були введені в дію до появи сучасних автономних систем, генеративного ШІ, алгоритмічної обробки розвідувальних даних і високошвидкісних автоматизованих контурів прийняття рішень, що створює нормативний розрив між технологічною динамікою та правовими механізмами контролю.

Крім того, військовий ШІ не обмежується виключно зброєю, а може застосовуватися у навігації, зв'язку, розвідці, радіоелектронній боротьбі, протидії дезінформації, логістиці, розмінуванні, навчанні військових, моделюванні сценаріїв, автоматизованому аналізі супутникових знімків тощо. Як результат, межа між бойовими та небойовими, летальними й нелетальними, допоміжними та безпосередніми системами ураження з часом стає менш чіткою, а міжнародно-правове регулювання має враховувати не лише летальні автономні системи озброєнь, а й ширший спектр військового застосування ШІ. Тому в умовах сучасної війни, зокрема, повномасштабної агресії Російської Федерації проти України, питання застосування цифрових технологій набуває не теоретичного, а прикладного значення. Для України розвиток ШІ є не лише питанням технологічної модернізації, а й елементом національної безпеки, обороноздатності та адаптації до нових форм ведення війни, адже як демократична держава вона має забезпечити, щоб впровадження таких технологій відповідало міжнародному праву, правам людини, принципам відповідального використання ШІ та вимогам цивільного контролю над сектором безпеки й оборони.

Аналіз останніх досліджень і публікацій. Проблематика ШІ у військовій сфері досліджується в рамках науки міжнародного права, теорії міжнародних відносин, стратегічних студій, кібербезпеки, етики застосування технологій та досліджень озброєнь. Теоретичною основою для аналізу цієї теми є концепції технологічної революції у військовій справі, стратегічної стабільності, гонки озброєнь, міжнародного гуманітарного права, відповідального інноваційного розвитку та нормативного регулювання нових військових технологій.

У класичній теорії міжнародних відносин військові технології розглядаються як один із чинників зміни балансу сил. Реалістична традиція наголошує на тому, що держави прагнуть здобути технологічну перевагу для гарантування власної безпеки, стримування супротивника та посилення військово-політичного впливу [24, с. 118-121]. В контексті ШІ, ця логіка проявляється у технологічному суперництві США, Китаю, Росії, Ізраїлю, Великої Британії, Франції та інших держав, які розглядають військовий ШІ як інструмент майбутньої стратегічної переваги [12, с. 36-40]. Водночас, ліберально-інституційний підхід акцентує увагу на необхідності впровадження міжнародних режимів, норм, прозорості, діалогу та механізмів контролю, які могли б зменшити ризики неконтрольованої гонки військового ШІ.

Важливе місце в науковій дискусії посідають праці, присвячені співвідношенню універсальних прав людини, культурних відмінностей і глобального регулювання ШІ. Так, К. Браун, аналізуючи критику універсалізму прав людини, звертає увагу на те, що наявні інтерпретації прав і свобод залежать від політичного та культурного контексту [3, с. 41-45]. Дж. Чан у межах конфуціанського підходу до прав людини наголошує на значенні колективних інтересів, соціальної гармонії та обов'язків перед спільнотою [6].

П. Г. Вонг, досліджуючи культурні відмінності у глобальній етиці та врядуванні щодо ШІ, підкреслює, що різні політико-культурні системи можуть по-різному тлумачити поняття людської гідності, безпеки, автономії та відповідальності [25, с. 705-715], оскільки глобальні правила використання ШІ формуються в умовах різних нормативних традицій.

Окремий блок досліджень у рамках даної проблематики стосується автономних систем озброєнь. Міжнародна неурядова організація *Human Rights Watch* у доповіді *Losing Humanity: The Case against Killer Robots* ще у 2012 році обґрунтовувала необхідність превентивної заборони повністю автономної зброї, наголошуючи на ризиках для принципу розрізнення між комбатантами та цивільними особами, а також на проблемі відповідальності за рішення, прийняті машиною [13]. Ця доповідь стала одним із важливих імпульсів для подальших міжнародних дискусій щодо положень Конвенції про заборону або обмеження застосування конкретних видів звичайної зброї, які можуть вважатися такими, що завдають надмірних ушкоджень або мають не вибірково, дію від 10 жовтня 180 року [7].

Міжнародний Комітет Червоного Хреста послідовно розглядає автономні системи озброєнь як виклик міжнародному гуманітарному праву. У позиційному документі 2026 року МКЧХ підкреслює необхідність збереження контролю людини над застосуванням сили, забезпечення передбачуваності, обмеження автономії у виборі й ураженні цілей, а також відповідності принципам МГП [14]. Такий підхід є одним із ключових у сучасній дискусії щодо *meaningful human control*, тобто змістовного людського контролю над автономними системами.

Значну увагу дослідники приділяють національним моделям регулювання військового ШІ. США формують власний підхід через Директиву Міністерства оборони 3000.09 *Autonomy in Weapon Systems*, яка окреслює політику щодо застосування автономних і напіваавтономних функцій у системах озброєнь; вимоги до тестування, перевірки, управління ризиками та мінімізації ймовірності небажаного ураження [10]. НАТО, в свою чергу, розробила принципи відповідального використання ШІ в обороні, серед яких – законність, відповідальність і підзвітність, пояснюваність і простежуваність, надійність, керованість і мінімізація упереджень [16; 17].

Китайська модель розвитку ШІ у військовій сфері аналізується через концепцію «інтелектуалізованої війни», військово-цивільної інтеграції, централізованої державної координації технологічного розвитку та активної ролі Народно-визвольної армії Китаю у фінансуванні відповідних досліджень. У цьому контексті, важливими є положення Закону КНР про кібербезпеку 2017 року, етичні документи щодо ШІ нового покоління та дослідження І. Дмитровича, Я. Мао і К. Ши-Купфер щодо регуляторних та етичних засад розвитку ШІ в азійських країнах [9; 15].

На міжнародному рівні особливе значення має Резолюція Генеральної Асамблеї ООН 79/239 від 24 грудня 2024 року *Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security*, що стала першою резолюцією ГА ООН, спеціально присвяченою ШІ у військовій сфері, підтвердивши застосовність міжнародного права на всіх етапах життєвого циклу ШІ [21]. Подальша Доповідь Генерального Секретаря ООН А/80/78 систематизувала можливості й виклики, які створює військове застосування ШІ для міжнародного миру та безпеки, зробивши особливий акцент на сферах, що знаходяться поза межами летальних автономних систем озброєнь [22].

В Україні нормативною основою розвитку ШІ є Концепція розвитку штучного інтелекту в Україні, схвалена Розпорядженням Кабінету Міністрів України від 2 грудня 2020 року № 1556-р. Вона визначає ШІ як організовану сукупність інформаційних технологій, котра дає змогу виконувати складні комплексні завдання шляхом використання алгоритмів обробки інформації, моделей прийняття рішень і баз знань

[1]. Хоча дана Концепція має загальний характер і не створює спеціального режиму військового ШІ, вона закладає основу для подальшої правової політики у цій сфері в нашій державі.

Виділення невирішених раніше частин загальної проблеми. Попри достатньо інтенсивне вивчення питань ШІ та активізацію відповідних міжнародних дискусій, низка питань щодо застосування машинних систем прийняття рішень у військовій сфері, залишається недостатньо врегульованою та потребує подальшого наукового аналізу. Наразі відсутній універсальний міжнародний договір, який міг би врегулювати застосування ШІ у військовій сфері. Загальні принципи МГП поширюються на всі засоби й методи ведення війни, однак не завжди дають однозначні відповіді щодо автономних систем, алгоритмічного таргетингу, машинного прийняття рішень і відповідальності за помилкові дії ШІ. Недостатньо визначеним залишається відповідний понятійний апарат, оскільки в міжнародних документах і науковій літературі паралельно використовуються поняття «штучний інтелект у військовій сфері», «автономні системи озброєнь», «летальні автономні системи озброєнь», «військовий ШІ» тощо, що ускладнює правове регулювання, контроль і міжнародні переговори. Також невирішеною залишається проблема відповідальності, адже в разі заподіяння автономною системою шкоди, складно визначити, хто саме має нести відповідальність – держава, командир, оператор, розробник програмного забезпечення, виробник платформи, постачальник даних або особа, яка затвердила застосування системи. Недостатньо дослідженим є питання співвідношення військового ШІ та кібербезпеки, а правове регулювання військового ШІ має охоплювати не тільки застосування сили, а й захист даних, стійкість систем, контроль доступу, перевірку алгоритмів і кібернетичну безпеку. І, зрештою, залишається відкритим питання участі України у формуванні міжнародних норм відповідального застосування військового ШІ та недопущення воєнних злочинів.

Метою статті є виявлення й аналіз особливостей застосування штучного інтелекту у військовій сфері на основі визначення специфіки міжнародно-правового регулювання використання таких технологій, виділення ключових безпекових, правових та етичних викликів, а також окреслення напрямів удосконалення міжнародного та національного нормативно-правового регулювання військового ШІ.

Методологічну основу дослідження становить поєднання загальнонаукових, спеціально-юридичних і міждисциплінарних методів. Діалектичний метод використано для аналізу суперечливого характеру військового ШІ, який одночасно підвищує ефективність оборонних можливостей і створює нові правові та безпекові ризики. Системний метод дав змогу розглянути військовий ШІ як елемент ширшої системи міжнародної безпеки, військово-технічного розвитку, міжнародного гуманітарного права, кібербезпеки та державної оборонної політики.

Формально-юридичний метод застосовано для аналізу міжнародних договорів, резолюцій ООН, документів МКЧХ, НАТО, ЄС, Міністерства оборони США та нормативних актів України. Порівняльно-правовий метод використано для зіставлення підходів США, Китаю, НАТО, ЄС та України до правового регулювання ШІ. Метод правового моделювання дозволив визначити можливі напрями майбутнього регулювання порядку застосування автономних систем озброєнь, включаючи вимоги щодо людського контролю, тестування, відповідальності й оцінки їх відповідності міжнародному гуманітарному праву.

Метод аналізу міжнародних відносин застосовано для вивчення військового ШІ як чинника стратегічної конкуренції, гонки озброєнь, технологічного стримування та міжнародного нормотворення. Етичний підхід використано для аналізу проблем делегування машинам рішень щодо застосування сили, ризику алгоритмічної помилки, дискримінації, непрозорості та втрати людської відповідальності.

Виклад основного матеріалу дослідження. Зрозуміло, що наразі штучний інтелект у військовій сфері охоплює широкий комплекс технологій, спрямованих на автоматизацію, прискорення та оптимізацію військових процесів. При цьому, йдеться не лише про роботизовані бойові системи, а й про програмні комплекси, які аналізують розвідувальні дані, обробляють зображення і відеоматеріали, виявляють аномалії, прогнозують розвиток операційної обстановки, підтримують логістику, забезпечують кіберзахист, моделюють бойові сценарії та допомагають командирам у прийнятті рішень.

Одним із ключових напрямів використання ШІ є обробка великих масивів даних у режимі реального часу. Сучасне поле бою генерує величезний обсяг інформації із супутників, безпілотників, сенсорів, радарів, кіберсистем, соціальних мереж, засобів радіоелектронної розвідки та відкритих джерел. Людина не здатна самотійно швидко обробити такий обсяг інформації, тому алгоритми машинного навчання стають інструментом прискореного аналізу, виявлення закономірностей і формування варіантів дій, що підвищує швидкість командування, однак, водночас, створює ризик надмірної залежності від алгоритмічних рекомендацій [8, с. 7-11; 12, с. 46-49].

Другим важливим напрямом є використання ШІ в розвідці, спостереженні та рекогноситуванні. Безпілотні літальні апарати, наземні роботи, морські автономні платформи та сенсорні мережі можуть виявляти рух, теплові сигнатури, військову техніку, інженерні споруди, позиції противника й маршрути його переміщення. Системи комп'ютерного зору здатні автоматично класифікувати об'єкти, порівнювати їх із базами даних і формувати аналітичні звіти [8, с. 6-9; 12, с. 48-50]. У військовому сенсі це створює перевагу у швидкості реагування, але в правовому сенсі потребує особливої уваги до точності ідентифікації, перевірки цілей і недопущення помилкового ураження цивільних осіб.

Третім напрямом є впровадження автономних і напівавтономних систем, до яких належать безпілотні літальні апарати, наземні роботизовані платформи, морські дрони, системи патрулювання, роботизовані засоби розмінування, автоматизовані оборонні комплекси та потенційно летальні автономні системи озброєнь. У логістиці такі системи можуть доставляти вантажі, евакуювати поранених або працювати в небезпечних зонах. У розмінуванні вони здатні зменшити ризики для саперів. У бойовому застосуванні вони можуть підтримувати розвідку, коригування вогню або безпосередньо уражати цілі [10; 14; 20, с. 27-35].

На нашу думку, саме бойове застосування автономних систем нині породжує найбільші правові та етичні дискусії: якщо система здатна самотійно обирати й уражати ціль без безпосереднього втручання людини, виникає питання відповідності такої системи міжнародному гуманітарному праву. Принцип розрізнення вимагає, щоб сторони конфлікту відрізняли комбатантів від цивільних осіб та військові об'єкти – від цивільних. Принцип пропорційності забороняє напади, у яких очікувана шкода цивільному населенню буде надмірною порівняно з конкретною і безпосередньою військовою перевагою. Принцип обережності вимагає вживати всіх практично можливих заходів для мінімізації шкоди цивільним. Відтак, питання полягає в тому, чи здатна автономна система адекватно оцінювати контекст, намір, поведінку осіб, змінну бойову обстановку та складні гуманітарно-правові критерії її оцінювання [13; 14; 19].

Міжнародне право не містить загальної заборони на використання ШІ у військовій сфері. Водночас, право сторін збройного конфлікту обирати засоби й методи ведення війни не є необмеженим. Конвенції про заборону або обмеження застосування конкретних видів звичайної зброї, які можуть вважатися такими, що завдають надмірних ушкоджень або мають не вибірккову, закріплює підхід, відповідно до якого можуть заборонятися або обмежуватися види озброєнь, що спричиняють надмірні ушкодження або мають не вибірккову дію [7]. Додатковий протокол I до Женевських

конвенцій також передбачає зобов'язання держав оцінювати нову зброю, засоби або методи ведення війни на відповідність міжнародному праву [19]. Саме цей підхід є основою для правових оглядів автономних систем і військового ШІ, проте існує важлива проблема: не всі системи ШІ є зброєю у класичному розумінні. Алгоритм, який аналізує розвідувальні дані, прогнозує переміщення противника або оптимізує логістику, не є зброєю, але його помилка може призвести до прийняття неправомірного рішення про застосування сили. Система генеративного ШІ, яка створює дезінформаційні повідомлення або імітує голос командира, також не є традиційною зброєю, але може спричинити дезорганізацію управління, паніку або ескалацію. Відтак, правове регулювання використання ШІ у військовій сфері має охоплювати не тільки матеріальні платформи, а й алгоритмічні функції, дані, програмне забезпечення та канали управління.

Згідно з нормами традиційного міжнародного права, держава несе відповідальність за міжнародно-протиправні діяння, а фізичні особи можуть нести кримінальну відповідальність за воєнні злочини. Однак, у випадку автономних систем виникає складний ланцюг відповідальності: командир ухвалює рішення про застосування системи, оператор активує її, розробник створює алгоритм, виробник інтегрує сенсори, постачальник даних формує навчальний масив, а сама система діє в непередбачуваному середовищі. У такій ситуації необхідно зберегти принцип, за яким відповідальність не може бути перекладена на машину: ШІ не є суб'єктом міжнародного права і не може нести юридичну відповідальність, адже відповідальними залишаються люди, держави та організації, які розробляють, тестують, закуповують, санкціонують і застосовують такі системи. Тому маємо відзначити, що вагоме значення також має змістовний людський контроль, який означає не просто формальну присутність людини в ланцюгу прийняття рішень, а реальну можливість розуміти функціонування системи, оцінювати її рекомендації, контролювати межі застосування, втручатися в роботу, зупиняти дію і нести відповідальність за її наслідки [14; 20, с. 195-213].

У даному контексті, пропонуємо розглянути досвід застосування ШІ у військовій сфері низкою ключових суб'єктів міжнародних відносин та відповідне нормативно-правове регулювання цих процесів. Так, США вважається одним із провідних акторів у сфері застосування військового ШІ, оскільки їхній підхід поєднує активний розвиток автономних і напіваавтономних систем із внутрішніми політико-правовими обмеженнями. Директива Міністерства оборони США 3000.09 встановлює вимоги до розробки й застосування автономних систем озброєнь, зокрема, щодо мінімізації ризиків ненавмисного ураження, тестування, перевірки, кібербезпеки, навчання персоналу та управління життєвим циклом системи [10]. У 2023 році США також ініціювали схвалення Політичної декларації про відповідальне військово-використання ШІ та автономії, яка передбачає, що військові системи ШІ мають відповідати міжнародному праву, проходити належне тестування, мати зрозумілі межі застосування та бути побудованими з урахуванням відповідальності людини [23].

Китайський підхід до застосування військового ШІ формується в межах ширшої стратегії технологічного суверенітету, кібербезпеки та військово-цивільної інтеграції. Народньо-визвольна армія Китаю розглядає ШІ як ключовий елемент майбутньої «інтелектуалізованої» війни, що охоплює автономні безпілотні системи, обробку великих масивів даних, моделювання операцій, командування, навчання, інформаційну війну та кіберпростір. Китайське регулювання ШІ пов'язане з нормами кібербезпеки, захисту даних, етичними принципами нового покоління ШІ та контролем над генеративними сервісами [9; 15]. Водночас, відмінності між західним і китайським розумінням прав людини, колективної безпеки та ролі держави в суспільстві та

міжнародних відносинах ускладнюють формування універсального режиму військового ШІ [3; 6; 25].

У свою чергу, НАТО формує нормативну рамку відповідального використання ШІ в обороні через принципи законності, відповідальності, надійності, керованості та мінімізації упереджень [16; 17]. Такий підхід важливий для держав-членів Альянсу та його партнерів, оскільки військовий ШІ має не лише бути ефективним, а й забезпечувати сумісність, довіру, контроль, прозорість і відповідність нормам міжнародного права. Для України, яка поглиблює взаємодію з НАТО, ці принципи можуть бути орієнтиром для побудови національної політики у сфері оборонного ШІ в майбутньому. Європейський Союз у 2024 році ухвалив Акт про штучний інтелект (англ. – *AI Act*), який став першою комплексною горизонтальною моделлю регулювання ШІ. Водночас, цей документ прямо не застосовується до систем ШІ, які використовуються виключно для військових, оборонних або національно-безпекових цілей [11], що демонструє важливу особливість: навіть найрозвинутіші цивільні моделі регулювання ШІ залишають військову сферу переважно у площині міжнародного права, національної безпеки та спеціальних оборонних режимів, тому принципи ризик-орієнтованого підходу, прозорості, управління даними, оцінки відповідності та нагляду можуть бути корисними і для військової сфери.

Для України питання ШІ у військовій сфері має особливе значення. Концепція розвитку ШІ в Україні визначає загальні засади державної політики у цій сфері [1], а Закон України «Про національну безпеку України» закріплює, що державна політика у сферах національної безпеки й оборони спрямовується, зокрема, на забезпечення воєнної, державної, економічної, інформаційної безпеки, безпеки критичної інфраструктури та кібербезпеки [2]. З огляду на це, розвиток військового ШІ в Україні має бути інтегрований у ширшу систему оборонного планування, кіберзахисту, інновацій, правового контролю та міжнародного співробітництва. Водночас, Україна потребує більш спеціалізованої нормативної рамки, що повинна включати визначення військового ШІ, класифікацію автономних і напіваавтономних систем, порядок правового огляду нових засобів і методів ведення війни, вимоги до тестування, кіберстійкості, контролю людини, відповідальності командирів і операторів, захисту даних, взаємодії з приватними розробниками та міжнародного обміну технологіями. Особливу увагу слід звернути на те, щоб військові інновації не виходили за межі міжнародного гуманітарного права.

Нині кібербезпека є одним із ключових вимірів військового ШІ, адже автоматизовані системи можуть виявляти кібератаки, аналізувати аномалії, прогнозувати поведінку противника, захищати критичну інфраструктуру та підтримувати інформаційну безпеку. Водночас, самі системи ШІ можуть бути об'єктом атак: противник може намагатися спотворити навчальні дані, підмінити сигнали сенсорів, ввести систему в оману, порушити канал зв'язку або змусити алгоритм неправильно класифікувати ціль. Тому відповідальне військове застосування ШІ передбачає не лише його ефективність, а й стійкість до втручання [10; 23].

Ще одним безпековим викликом є швидкість ескалації. Автоматизація прийняття рішень може скоротити час між виявленням загрози і відповіддю на неї. У певних ситуаціях це може бути перевагою, але в стратегічному вимірі надмірне прискорення військових процесів може зменшити простір для політичного контролю, дипломатії, перевірки інформації та деескалації. Особливо небезпечним є застосування ШІ в ядерній сфері, системах раннього попередження, протиракетній обороні та командно-контрольних структурах. Відтак, міжнародні документи дедалі частіше наголошують на тому, що людина повинна зберігати відповідальність за критично важливі рішення щодо застосування сили [22; 23].

Окрему увагу слід приділити генеративному ШІ, військове використання якого може охоплювати створення синтетичних зображень, відео, голосових повідомлень, фальшивих наказів, дезінформаційних кампаній, психологічних операцій і автоматизованого аналізу текстових даних. У воєнних умовах імітація голосу командира або створення переконливої фальшивої інформації може мати безпосередні наслідки для бойового управління, морального стану військ і цивільного населення. Тому правове регулювання військового ШІ має враховувати не лише фізичне ураження, а й інформаційно-психологічний вплив, котрий він може чинити під час ведення бойових дій [22; 23].

На міжнародному рівні поступово формується консенсус щодо застосування норм міжнародного права під час регулювання процесів використання ШІ у військовій сфері. Резолюція ГА ООН 79/239 прямо підтверджує застосовність міжнародного права на всіх етапах життєвого циклу військового ШІ [21]. Доповідь Генерального Секретаря ООН A/80/78 наголошує на потребі аналізу не лише летальних автономних систем, а й ширших можливостей та ризиків військового ШІ для міжнародного миру й безпеки [22]. На нашу думку, це важливий крок, оскільки глобальна дискусія наразі виходить за межі вузьких питань, охоплюючи розвідку, командування, кіберпростір, логістику, інформаційні операції та стратегічну стабільність.

Разом із цим, міжнародне регулювання використання ШІ у військовій сфері залишається фрагментарним. Частина держав виступає за юридично обов'язкові заборони або обмеження летальних автономних систем, інші наполягають, що чинного міжнародного права достатньо, а нові норми можуть обмежити технологічний розвиток [13; 14; 21; 22]. Така розбіжність пояснюється не лише правовими аргументами, а й стратегічною конкуренцією, адже провідні військові держави не бажають втрачати потенційну технологічну перевагу. Така ситуація створює класичну проблему безпекової дилеми: навіть якщо держави визнають ризики військового ШІ, вони побоюються, що одностороннє обмеження поставить їх у невигідне становище. Отже, військовий ШІ є не просто новим технологічним інструментом, а фактором трансформації сучасної безпекової архітектури. Він впливає на баланс сил, характер війни, швидкість прийняття рішень, міжнародне гуманітарне право, кібербезпеку, стратегічну стабільність і відповідальність держав. Його регулювання не може бути зведене лише до заборони окремих видів озброєнь. Потрібна комплексна модель, яка поєднує міжнародне право, національне законодавство, технічні стандарти, етичні принципи, контроль людини, прозорість, правові огляди та міжнародну співпрацю.

Висновки. Отже, в результаті проведеного дослідження встановлено, що штучний інтелект став одним із ключових чинників трансформації сучасної військової сфери. Його застосування охоплює розвідку, спостереження, аналіз даних, логістику, кібербезпеку, автономні платформи, моделювання операцій, підготовку рішень і потенційне застосування сили, що створює значні переваги для держав, які володіють відповідними технологіями, але, водночас, породжує нові правові, етичні та безпекові виклики.

Чинне міжнародне гуманітарне право поширюється на військове використання ШІ, однак його загальні принципи потребують конкретизації щодо автономних систем, алгоритмічного прийняття рішень, машинного таргетингу, кібероперацій, генеративного ШІ та відповідальності за помилки систем. Відсутність спеціального універсального міжнародного договору у цій сфері створює нормативну невизначеність, яка може бути використана державами для прискореної розробки військових ШІ-систем без належного контролю. Центральними правовими проблемами в даному сенсі є забезпечення принципів розрізнення, пропорційності, обережності, військової необхідності, заборони надмірних страждань, відповідальності та змістовного контролю людини. При цьому, ШІ не може бути суб'єктом юридичної

відповідальності. Відповідальність за розробку, закупівлю, тестування, санкціонування та застосування таких систем мають нести держави, командири, оператори, розробники та інші причетні суб'єкти залежно від характеру вчиненого порушення.

Міжнародне регулювання військового ШІ має розвиватися у кількох напрямках: по-перше, через уточнення дефініцій і класифікації автономних та напіваавтономних систем; по-друге, через закріплення вимоги змістовного контролю людини; по-третє, через обов'язкові правові огляди нових засобів і методів ведення війни; по-четверте, через вимоги до тестування, валідації, кіберстійкості й простежуваності рішень; по-п'яте, через міжнародну прозорість і обмін кращими практиками; по-шосте, через заборону або суворе обмеження систем, які не можуть бути застосовані відповідно до міжнародного гуманітарного права.

Для України розвиток військового ШІ має важливе значення з огляду на війну з РФ, потребу в технологічній перевазі, кіберзахисті, ефективному управлінні ресурсами та захисті цивільного населення. Водночас, Україна має розвивати цю сферу в межах міжнародного права, демократичного цивільного контролю, партнерства з НАТО та ЄС, а також власної нормативної політики у сфері ШІ. Доцільним є розроблення спеціальних стандартів для військового ШІ, які охоплювали б правовий огляд систем, контроль людини, кібербезпеку, відповідальність, етичні принципи та взаємодію з приватними технологічними компаніями.

Практичне значення нашого дослідження, таким чином, полягає в можливості використання його висновків для формування державної політики у сфері оборонного ШІ, підготовки нормативних актів, розроблення внутрішніх військових стандартів, удосконалення правових оглядів нових систем озброєнь, підготовки фахівців у сфері міжнародного гуманітарного права та підвищення рівня участі України у міжнародних дискусіях щодо відповідального військового використання ШІ. Перспективи подальших досліджень можуть окреслюватися в глибшому аналізі відповідальності за шкоду, заподіяну автономними системами; розробленні критеріїв змістовного контролю людини; дослідженні військового застосування генеративного ШІ; порівнянні моделей регулювання США, Китаю, НАТО, ЄС та України; а також у формуванні пропозицій щодо міжнародного договору або протоколу, який би спеціально регулював найбільш ризиковані для застосування форми військового ШІ.

Список використаних джерел

1. Концепція розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. Дата оновлення: 29.12.2021. *Верховна Рада України: Офіційний вебпортал Парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text> (дата звернення: 12.01.2025).
2. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. Дата оновлення: 09.08.2024. *Верховна Рада України: Офіційний вебпортал Парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (дата звернення: 18.01.2025).
3. Brown C. Universal Human Rights: A Critique. *The International Journal of Human Rights*. 1997. Vol. 1, No. 2. P. 41-65. DOI: 10.1080/13642989708406666.
4. Buzan B. People, States and Fear: The National Security Problem in International Relations. Brighton: Wheatsheaf Books, 1983. 262 p.
5. Buzan B., Wæver O., de Wilde J. Security: A New Framework for Analysis. Boulder; London: Lynne Rienner Publishers, 1998. 239 p.

6. Chan J. C. W. A Confucian Perspective on Human Rights for Contemporary China. The East Asian Challenge for Human Rights / ed. by J. R. Bauer, D. A. Bell. Cambridge: Cambridge University Press, 1999.
7. Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects of 10 October 1980. URL: <https://treaties.unoda.org/t/ccwc> (дата звернення: 07.02.2025).
8. Cummings M. L. Artificial Intelligence and the Future of Warfare / Chatham House. London: Chatham House, 2017. 18 p. URL: <https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf> (дата звернення: 15.02.2025).
9. Cybersecurity Law of the People's Republic of China of 1 June 2017. *DigiChina*. 29.06.2018. URL: <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/> (дата звернення: 21.02.2025).
10. Directive 3000.09: Autonomy in Weapon Systems of 25 January 2023 / Department of Defense. URL: <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf> (дата звернення: 05.03.2025).
11. European Parliament and Council. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. *Official Journal of the European Union*. 2024. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (дата звернення: 12.03.2025).
12. Horowitz M. C. Artificial Intelligence, International Competition, and the Balance of Power. *Texas National Security Review*. 2018. Vol. 1, No. 3. P. 36-57. DOI: 10.15781/T2639KP49.
13. Human Rights Watch. Losing Humanity: The Case against Killer Robots. New York: Human Rights Watch, 2012. URL: <https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots> (дата звернення: 20.03.2025).
14. ICRC Position on Autonomous Weapon Systems. Geneva: ICRC, 2021. URL: <https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems> (дата звернення: 27.03.2025).
15. Mao Y., Shi-Kupfer K. Online Public Discourse on Artificial Intelligence and Ethics in China: Context, Content, and Implications. *AI & Society*. 2023. Vol. 38. P. 373-389. DOI: 10.1007/s00146-021-01309-7.
16. NATO. Summary of the NATO Artificial Intelligence Strategy. URL: https://www.nato.int/cps/en/natohq/official_texts_187617.htm (дата звернення: 03.04.2025).
17. NATO. Summary of NATO's Revised Artificial Intelligence Strategy. URL: https://www.nato.int/cps/en/natohq/official_texts_227237.htm (дата звернення: 10.04.2025).
18. Nye J. S. Soft Power: The Means to Success in World Politics. New York: PublicAffairs, 2004. 191 p.
19. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts of 8 June 1977. URL: <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977> (дата звернення: 16.04.2025).
20. Scharre P. Army of None: Autonomous Weapons and the Future of War. New York; London: W. W. Norton & Company, 2018. 448 p.
21. United Nations General Assembly. Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security: Resolution A/RES/79/239. New York: United Nations, 2024. URL: <https://digitallibrary.un.org/record/4071348> (дата звернення: 22.04.2025).
22. United Nations Secretary-General. Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security: Report A/80/78. New York: United

- Nations, 2025. URL: <https://digitallibrary.un.org/record/4086346> (дата звернення: 15.06.2025).
23. United States Department of State. Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy. URL: <https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy/> (дата звернення: 25.06.2025).
24. Waltz K. N. Theory of International Politics. Reading, Massachusetts: Addison-Wesley Publishing Company, 1979. 251 p.
25. Wong P. H. Cultural Differences as Excuses? Human Rights and Cultural Values in Global Ethics and Governance of AI. *Philosophy & Technology*. 2020. Vol. 33, No. 4. P. 705-715. DOI: 10.1007/s13347-020-00413-8.