

УДК 341.3:004.8:623.4

DOI <https://doi.org/10.24144/2788-6018.2025.04.3.58>

АДАПТАЦІЯ МІЖНАРОДНОГО ПРАВА ДО ВИКЛИКІВ НОВИХ ТЕХНОЛОГІЙ: ШТУЧНИЙ ІНТЕЛЕКТ, АВТОНОМНІ СИСТЕМИ ОЗБРОЄНЬ ТА ЇХ РЕГУЛЮВАННЯ

Захарчук І.В.,

старший викладач кафедри «Правознавство»,

Північноукраїнський інститут ім. Героїв Крут ПрАТ «ВНЗ «МАУП»

ORCID: 0000-0001-6957-9004

Захарчук І.В. Адаптація міжнародного права до викликів нових технологій: штучний інтелект, автономні системи озброєнь та їх регулювання.

Стаття присвячена аналізу міжнародно-правових аспектів адаптації права до викликів, пов'язаних із розвитком штучного інтелекту (ШІ) та автономних систем озброєнь (АСО). У центрі дослідження – спроба оцінити, наскільки чинні нормативні конструкції міжнародного гуманітарного, безпекового та кримінального права здатні забезпечити ефективне, етичне й юридично обґрунтоване регулювання новітніх технологій у військовій сфері. У статті систематизовано основні типи ризиків, які створюють ШІ та АСО, із фокусом на проблематиці дотримання принципів міжнародного гуманітарного права, юридичної атрибуції дій автономних систем, відповідальності держав і фізичних осіб, а також прогалин у чинних режимах експортного контролю та інституційного нагляду.

Особливу увагу приділено аналізу існуючих міжнародно-правових механізмів, включаючи Конвенцію про конкретні види звичайної зброї (ККЗ), Додатковий протокол I до Женевських конвенцій 1949 року, Римський статут МКС, міжнародні режими контролю за експортом та європейське законодавство у сфері ШІ. Підкреслено, що наявні правові інструменти мають фрагментарний і недостатньо зобов'язуючий характер, особливо у сфері військового застосування новітніх цифрових технологій. Значну увагу приділено аналізу обмежень *soft law*-підходів (етичних декларацій, добровільних стандартів), які не забезпечують належного рівня юридичної визначеності та примусовості.

У заключній частині подано авторські пропозиції щодо адаптації міжнародного права до новітніх викликів. Зокрема, пропонується укладання спеціального багатостороннього договору про автономні системи озброєнь, інституціоналізація незалежного механізму контролю та верифікації, інтеграція принципу «значущого людського контролю» в норми міжнародного гуманітарного права, а також розширення сфери експортного контролю на програмне забезпечення та алгоритми військового призначення. Автор підкреслює, що без формалізованого правового реагування технології ШІ можуть стати чинником руйнування сучасного міжнародного порядку, зокрема у сфері захисту прав людини, безпеки та відповідальності за збройні конфлікти.

Ключові слова: міжнародне гуманітарне право, штучний інтелект, автономні системи озброєнь, юридична відповідальність, експортний контроль, принцип значущого людського контролю, адаптація міжнародного права, м'яке право.

Zakharchuk I.V. Adapting international law to the challenges of new technologies: artificial intelligence, autonomous weapon systems, and their regulation.

The article explores the international legal challenges and required adaptations of international law in response to the rapid development of artificial intelligence (AI) and autonomous weapon systems (AWS). It aims to evaluate the capacity of existing legal frameworks – particularly international humanitarian law, security law, and international criminal law – to ensure effective, ethical, and accountable regulation of military AI technologies. The study presents a systematic typology of legal risks associated with AI and AWS, including potential violations of the principles of distinction and proportionality under international humanitarian law, issues of legal attribution, gaps in state and individual responsibility, and the insufficiency of current export control regimes and institutional oversight mechanisms.

Special attention is given to existing legal instruments such as the Convention on Certain Conventional Weapons (CCW), Additional Protocol I of the Geneva Conventions 1949, the Rome Statute of the International Criminal Court, various international export control regimes, and recent European legal initiatives such as the EU AI Act and the Council of Europe's AI Framework Convention. The article concludes that the current legal architecture is fragmented, non-binding in many critical areas, and largely inapplicable to the military use of emerging AI technologies. It also emphasizes the limitations

of soft law approaches (such as ethical guidelines and political declarations), which lack enforceability and legal certainty.

In the final section, the author proposes a set of legal and institutional reforms to adapt international law to new technological threats. These include: the adoption of a dedicated multilateral treaty on AWS; the establishment of an independent monitoring and verification mechanism; the formal integration of the «meaningful human control» principle into international humanitarian law; and the expansion of export control regimes to cover military-grade AI software, algorithms, and training datasets. The article ultimately argues that, without proactive and structured legal adaptation, the unchecked development and deployment of military AI could undermine the fundamental principles of international law, including human rights protection, accountability for armed conflict, and global security.

Key words: international humanitarian law, artificial intelligence, autonomous weapon systems, legal responsibility, export control, meaningful human control, legal adaptation, soft law.

Постановка проблеми. Стрімкий розвиток штучного інтелекту (ШІ) та автономних систем озброєнь (АСО) ставить під сумнів здатність існуючих норм міжнародного публічного права, насамперед, міжнародного гуманітарного права (МГП) та права міжнародної безпеки, забезпечити належний рівень запобігання шкоді, підзвітності та захисту прав людини. Незважаючи на те, що низка універсальних (в рамках ООН) та регіональних (в рамках ЄС та Ради Європи) ініціатив пропонують нові регуляторні рамки, між ними залишаються прогалини та колізії: відсутність спеціальної заборонної чи обмежувальної угоди щодо летальних автономних систем, нечіткий розподіл відповідальності між державою-розробником і державою-користувачем таких або аналогічних систем, а також складність застосування принципу «значущого людського контролю» в умовах високого рівня автономії систем.

Мета дослідження: систематизувати поточні міжнародно-правові підходи до регулювання ШІ та АСО, виявити ключові прогалини й запропонувати концептуальні напрями щодо їх усунення, спираючись на новітні нормативні й політичні ініціативи 2024-2025 рр.

Стан опрацювання проблематики. Дослідження адаптації міжнародного права до викликів нових технологій, зокрема ШІ та АСО, є актуальним напрямком як у світовій, так і в українській науковій спільноті. В Україні ця проблематика перебуває на стадії активного розвитку, враховуючи інтеграцію країни до європейських правових стандартів та виклики, пов'язані з національною безпекою, зокрема в контексті російсько-української війни.

На протязі останніх років науковці досліджували окремі аспекти використання та правового регулювання ШІ та АСО у військовій сфері та сфері оборони. Серед них варто зазначити таких як С.М. Бортник, О.М. Борщевська, С.В. Грузій, А.А. Завадський, О.А. Задихайло, Т.Г. Каткова, С.Ю. Козьяков, Р.Г. Меликов, Д.І. Прокопович-Ткаченко, Т.Ю. Федчук.

Окремо слід виділити Р.Г. Меликова, який провів ґрунтовне комплексне дослідження питань правового регулювання автономних систем озброєнь (АСО) як важливої частини міжнародного гуманітарного права ХХІ століття [1].

Загалом, більшість науковців погоджуються, що правове регулювання штучного інтелекту як в Україні, так і на міжнародному рівні перебуває на етапі становлення. Це обумовлює високу актуальність подальших досліджень в цій сфері. Поки в міжнародному праві не існує єдиного нормативного підходу до правового регулювання використання систем ШІ та АСО, а також до визначення відповідальних суб'єктів або відповідних механізмів контролю за прозорістю рішень, які можуть прийматися алгоритмами та нейромережами. Все це зумовлює необхідність більш глибокої теоретико-правової розробки зазначеної сфери, із врахуванням міжнародного та вітчизняного досвіду.

Виклад основного матеріалу. Історично міжнародне право формувалося як реакція на політичні, воєнні або гуманітарні потрясіння. Однак з розвитком технологій, особливо у ХХ-ХХІ століттях, стало очевидним, що технологічні інновації самі по собі можуть становити виклик для наявної системи норм. Цей феномен поступово оформився як поняття технологічного виклику (technological challenge), що потребує як концептуального осмислення, так і практичного реагування у сфері права.

Першим масштабним технологічним викликом, який поставив під сумнів ефективність наявного міжнародного права, став розвиток ядерної зброї в середині ХХ століття. Міжнародне право тих часів не передбачало:

- контролю над руйнівною силою масового знищення, що перевищувала можливості традиційного збройного конфлікту;
- режиму нерозповсюдження;
- механізмів моніторингу, верифікації та санкцій.

Це спровокувало появу прецедентної технологічної прогалини, яку довелося заповнювати екстраординарними заходами (створення МАГАТЕ, прийняття Договору про нерозповсюдження ядерної зброї та Договору про всеосяжну заборону ядерних випробувань тощо).

З кінця XX століття правові системи зіткнулися з новим поколінням технологічних загроз, пов'язаних із нематеріальними і децентралізованими феноменами – кіберзлочинністю, кібервійною, цифровими платформами. Основними характеристиками нової хвилі викликів стали:

- невизначеність суб'єкта. Винакає питання, хто несе відповідальність за такі дії – держава, приватна компанія чи конкретна особа-хакер;
- транскордонність. Такі атаки або порушення не обмежуються територією однієї держави;
- асиметричність шкоди. Один суб'єкт може завдати надмірної шкоди системі без прямого застосування зброї.

Це породило появу так званих актів «м'якого права» (soft-law) (наприклад, Будапештська конвенція про кіберзлочинність 2001 р.) та доктрин, серед яких можна відзначити «Талліннський посібник щодо міжнародного права, що може бути застосоване до кібервійни», виданий в 2013 році робочою комісією під егідою Центру кіберзахисту НАТО (CCDCoE), розміщеного в Таллінні (Естонія) [2, с. 248].

У XXI столітті перед міжнародним правом постала якісно нова категорія технологічного виклику – системи ШІ та автономні системи, зокрема в сфері озброєнь. На відміну від попередніх викликів, що були масштабними, але зрозумілими, ШІ-системи створюють правову невизначеність на рівні базових понять, серед яких:

- намір (mens rea);
- агентність;
- контроль;
- відповідальність.

До особливості цього виклику можна віднести:

- непередбачуваність поведінки систем (особливо тих, що навчаються). Вони можуть ухвалювати рішення на основі непередбачених зв'язків у даних;
- відсутність єдиного центру контролю (розробник ≠ користувач ≠ держава);
- ефект «чорної скриньки», що означає неможливість пояснити логіку ухваленого рішення (особливо в deep learning-моделях);
- технологічна універсальність. Одна й та сама система може мати цивільне, комерційне і військове застосування – виникає проблема dual-use (подвійного призначення) [3, с. 798].

У сучасному світі технології перестають бути просто засобом ведення війни – вони самі стають полем бою. ШІ, автономні дрони, цифрові близнюки, моделі поведінки – усе це створює нові структури впливу, які виходять за межі класичних юридичних категорій.

Таким чином, технологічні виклики XXI століття змушують переосмислити саме поняття збройного конфлікту, відповідальності, порушення суверенітету тощо.

Традиційно міжнародне право формувало відповіді реактивно – лише після появи певної загрози чи катастрофи. Проте з розвитком автономних і систем із ШІ потрібен проактивний підхід:

- передбачення потенційних сценаріїв зловживань;
- впровадження етичних фільтрів до розробки технологій (ethics by design);
- створення превентивних регуляторних інструментів (реєстри, обмеження, аудит, інспекції тощо).

Інакше кажучи, поняття технологічного виклику поступово трансформується з інцидентного фактору (загроза, на яку треба реагувати) в структурний фактор міжнародної безпеки, що потребує постійної нормативної підтримки.

Еволюція технологічного виклику у міжнародному праві – це поступовий перехід від поодиноких правових криз (як у випадку ядерної зброї) до постійної адаптації нормативної системи до умов невизначеності та високої складності. ШІ та автономні системи – лише чергова, але принципово якісно нова фаза цієї трансформації. Вони ставлять перед міжнародним правом питання не лише що регулювати, але й як і коли це робити. Розробка відповідей на ці питання стане одним із ключових викликів міжнародної правової науки та практики в найближчі десятиліття.

ШІ та АСО виводять міжнародне право за межі звичних моделей регулювання засобів і методів ведення війни. Правові ризики, які постають у зв'язку з їх розробкою, використанням та експортом, можна умовно поділити на кілька ключових типів.

1. Проблема відповідності автономних систем нормам МГП.

АСО мають потенціал порушувати базові принципи МГП, зокрема:

- принцип розрізнення [4, с. 317]. Автономна система може не мати достатньої здатності відрізнити комбатанта від цивільної особи або військовий об'єкт від цивільної інфраструктури, що суперечить ст. 48 Додаткового протоколу I до Женевських конвенцій 1949 р.;

- принцип пропорційності. Відповідно до ст. 51(5)(b) того ж Протоколу, напад є незаконним, якщо очікувана побічна шкода цивільному населенню є надмірною порівняно з очікуваною військовою перевагою. Алгоритмічні рішення можуть ігнорувати або неправильно оцінювати такі співвідношення;
- обов'язок вживати запобіжних заходів. Ст. 57 все того ж Протоколу зобов'язує командирів мінімізувати шкоду цивільним. Якщо ж управління системою здійснюється автономно, здатність вживати адекватних запобіжних заходів ставиться під сумнів [5].

Ці порушення можуть спричинити державну відповідальність (як міжнародно-протиправні діяння), а також індивідуальну кримінальну відповідальність у випадку серйозних порушень МГП (наприклад, за воєнні злочини).

2. Атрибуція дій автономних систем державі та суб'єктам.

Одним із фундаментальних правових ризиків є проблема атрибуції, тобто як пов'язати дії АСО з відповідною державою чи особою. З одного боку порушення є міжнародно-протиправним лише тоді, коли його можна приписати державі, але автономна система може діяти без прямого людського контролю або навіть усупереч намірам держави [1, с. 137].

Таким чином, непередбачувана поведінка АСО може залишити певні дії поза сферою атрибуції, що ускладнює притягнення держави до відповідальності, навіть якщо було порушено МГП.

Крім того, відсутність юридичного суб'єкта у вигляді ШІ робить неможливим традиційне покарання системи – це створює «вакуум відповідальності».

3. Ризик порушення МГП.

Застосування автономних систем може призвести до:

- ненавмисної або автоматизованої ескалації збройного конфлікту без політичного рішення чи мандату на застосування сили;
- порушення п. 4 ст. 2 Статуту ООН (заборона погрози силою та її застосування проти територіальної цілісності чи політичної незалежності іншої держави);
- невідповідності принципу необхідності та пропорційності у рамках права на самооборону згідно зі ст. 51 Статуту ООН [6].

Отже, навіть якщо ШІ-система «самостійно» відповідає на провокацію, дії все одно можуть вважатися незаконним застосуванням сили з боку держави, що її використовує.

4. Пробіли у міжнародному договірному регулюванні.

На сьогодні відсутній універсальний міжнародно-правовий договір, який безпосередньо регулював би розробку, використання або заборону АСО та військового ШІ [7, с. 92].

Конвенція про конкретні види звичайної зброї (ККЗ) не містить спеціального протоколу щодо АСО, хоча Група урядових експертів з летальної автономної зброї (LAWS) працює в цьому напрямі з 2016 року. Але поки що без результатів.

Деякі міжнародні ініціативи (наприклад, політична Декларація Ірландії про «забезпечення гуманного контролю над системами озброєнь») є *soft law*, тобто не мають обов'язкової юридичної сили.

Римський статут Міжнародного кримінального суду не передбачає спеціальних положень для злочинів, пов'язаних із використанням автономних технологій.

У результаті на міжнародному рівні існує нормативний вакуум, який дозволяє державам діяти на власний розсуд без прямого порушення обов'язкових норм, але із серйозними правовими ризиками.

5. Експортний контроль і міжнародна передача технологій подвійного призначення.

ШІ-системи часто мають подвійне призначення – цивільне та військове. Це створює серйозні ризики незаконної передачі технологій у збройні конфлікти або до авторитарних режимів.

Регулювання міжнародної передачі автономних військових технологій фактично є правовою «сірою зоною», що сприяє неконтрольованому поширенню ризиків.

6. Ризики порушення прав людини під час застосування АСО поза умовами збройного конфлікту.

У випадках, коли АСО застосовуються поза активною фазою воєнних дій, наприклад для прикордонного патрулювання, у контртерористичних операціях чи під час поліцейських місій:

- діє міжнародне право прав людини (зокрема, Міжнародний пакт про громадянські та політичні права);
- будь-яке позасудове вбивство автономною системою, навіть з міркувань безпеки, може бути розцінене як порушення права на життя (ст. 6 Міжнародного пакту про громадянські та політичні права), права на правовий захист, права на людську гідність.

Особливо це стосується ситуацій, де:

- система діє на основі розпізнавання облич чи біометрії;

- вживаються попереджувальні удари без конкретного мандату чи розслідування;
- не передбачено належного контролю з боку людини.

Типологізація правових ризиків ШІ та АСО демонструє, що ці системи:

- порушують базові принципи міжнародного гуманітарного права та прав людини;
- ускладнюють юридичну відповідальність та атрибуцію дій;
- не вписуються в наявну договірну базу, що робить їх правовим прецедентом без чітких обмежень;
- створюють нові прогалини в експортному контролі та транснаціональному регулюванні.

Для забезпечення правового контролю над ШІ та АСО потрібне створення окремого правового режиму, який би:

- доповнив існуючі міжнародні договори (ККЗ, Римський статут, Женевські конвенції);
- чітко регулював використання, передачу, аудит і відповідальність у сфері автономних військових технологій.

Це стане основою для підвищення правової визначеності, передбачуваності та захисту прав людини в умовах технологічної трансформації воєнної справи.

До існуючих міжнародно-правових механізмів, які на сьогоднішній день регулюють сферу ШІ можна віднести:

1) Регламент Європейського Союзу AI Act (Регламент (ЄС) 2024/1689), що є обов'язковим нормативним актом для держав-членів Європейського Союзу. Він регулює цивільне використання систем штучного інтелекту, класифікуючи їх за рівнем ризику. Водночас сфера оборони прямо виключена з його дії. Таким чином, попри високий рівень деталізації й правову зобов'язаність, цей акт не охоплює військові аспекти ШІ, залишаючи вразливим питання автономних систем озброєнь [8];

2) Рамкову конвенцію Ради Європи про ШІ, права людини, демократію та верховенство права (відкрита для підписання у 2024 р.), яка є багатостороннім міжнародним договором, відкритим не лише для членів Ради Європи. Вона має міжгалузевий характер і спрямована на забезпечення прав людини та етичних стандартів у сфері ШІ. Водночас, з міркувань політичного компромісу, сфера оборони та військового застосування ШІ винесена за межі Конвенції. Україна приєдналась до конвенції у травні 2025 року;

3) Політичну декларацію про відповідальне використання ШІ у військових цілях, яка була оприлюднена США у 2023 році. Її вже підписали 52 країни. Але вона є прикладом «м'якого права», тобто не має обов'язкової сили, проте встановлює принципи належного поведіння з автономними військовими системами. Основним її недоліком є добровільність виконання положень, а також відсутність контрольного механізму чи санкцій у разі порушень;

4) Резолюцію Генеральної Асамблеї ООН A/78/L.49 (2024 р.), що має декларативний характер. Вона зосереджена переважно на аспектах безпечного, відповідального й етичного розвитку ШІ, підкреслює необхідність міжнародного співробітництва, але не містить зобов'язальних норм. Це політичний сигнал, а не юридичний механізм;

5) Групу урядових експертів (GGE) з питань летальних автономних озброєнь (LAWS), яка функціонує в рамках Конвенції ООН про конкретні види звичайної зброї (ККЗ) і є консультативним органом. Її мандат обмежений, оскільки вона працює на основі консенсусу, а отже не може ухвалювати обов'язкові рішення. Група продовжує обговорення можливості розробки нового Протоколу щодо автономних систем, але наразі не має чіткого доручення на укладення такого документа.

Сукупно всі ці ініціативи формують «клаптикову ковдру» норм, де цивільні й військові аспекти регулюються асиметрично.

З огляду на недостатню ефективність чинних міжнародно-правових механізмів у сфері регулювання ШІ та АСО, виникає об'єктивна потреба в оновленні нормативно-правових підходів. Адаптація міжнародного права до новітніх технологічних викликів має здійснюватися на основі принципу збереження балансу між інноваціями та міжнародною безпекою, між суверенітетом держав та універсальними цінностями, такими як людська гідність, гуманність і відповідальність.

У цьому контексті пропонується реалізація таких концептуальних і практичних напрямів:

1. Розробка та ухвалення спеціального міжнародного договору про автономні системи озброєнь.

Зважаючи на відсутність спеціалізованого договірної механізму, доцільним видається започаткування переговорного процесу в рамках Конвенції ООН про заборону або обмеження застосування певних видів звичайної зброї (ККЗ) із метою створення окремого Протоколу щодо автономних систем. Такий протокол повинен містити:

- визначення понять «автономна система озброєння», «передбачуваність дії», «людський контроль» тощо;
- заборону використання систем, які не дозволяють ефективно забезпечити дотримання міжнародного гуманітарного права;
- обов'язок проведення попереднього юридичного аналізу відповідно до ст. 36 Додаткового протоколу I до Женевських конвенцій 1949 р.

2. Інституціоналізація контролю за новими військовими технологіями.

Доцільним є створення постійного спеціалізованого органу під егідою ООН (аналог МАГАТЕ, але у сфері контролю систем ШІ) уповноваженого здійснювати:

- моніторинг нових систем, що розробляються у сфері автономного озброєння;
- методичне забезпечення юридичних оглядів нових систем;
- формування реєстру державних практик і національних підходів до регулювання ШІ в безпековому секторі.

3. Запровадження принципу «значущого людського контролю» (meaningful human control) у міжнародному праві [9, с. 449].

Цей принцип має бути інтегрований у норми МГП як обов'язкова умова законності застосування будь-якої системи, здатної завдавати летальних ударів. Його закріплення може бути здійснене шляхом:

- внесення змін або інтерпретацій до положень чинних протоколів ККЗ;
- ухвалення відповідної резолюції Генеральної Асамблеї ООН;
- включення цього принципу до обов'язкових стандартів експертного огляду систем озброєння.

4. Розширення сфери дії існуючих режимів експортного контролю.

Необхідним є включення до контрольних списків Вассенаарських угод, експортного регламенту Європейського Союзу та інших подібних механізмів не лише апаратного забезпечення (апаратів-дронів, сенсорів), але також:

- програмного забезпечення ШІ;
- моделей машинного навчання військового призначення;
- тренувальних наборів даних для таких систем.

5. Розвиток механізмів індивідуальної кримінальної відповідальності.

З метою уникнення ситуацій правового вакууму в частині персональної підзвітності за порушення, скоєні із використанням АСО, необхідно:

- забезпечити тлумачення положень Римського статуту з урахуванням новітніх технологій;
- внести роз'яснення щодо умов, за яких особа, що застосувала або санкціонувала застосування ШІ-системи, може бути визнана суб'єктом злочину;
- розглянути можливість ухвалення додаткового протоколу до Римського статуту, присвяченого цифровим та автономним технологіям у контексті міжнародних злочинів.

6. Гармонізація «м'якого права» (soft law) з обов'язковими стандартами.

Ініціативи у сфері «м'якого права» (етичні керівні принципи, політичні декларації) мають бути інституційно підкріплені через:

- запровадження механізмів регулярної звітності;
- розробку типових нормативних моделей для національного права;
- інкорпорацію принципів «м'якого права» у договори регіонального або глобального рівня.

Таким чином, адаптація міжнародного права до викликів, що генерує стрімкий розвиток ШІ та автономних озброєнь, потребує системної трансформації, яка має поєднувати жорсткі юридичні заборони, превентивний технічний контроль, інституційну відповідальність та міждержавне співробітництво. Відмова від регулювання або його відкладання створює реальну загрозу руйнування базових засад міжнародного гуманітарного та безпекового порядку.

Висновки. Існуюча нормативна основа є дуже фрагментарною. Цивільний ШІ дедалі більше охоплюється жорстко-правовими рамками (наприклад, EU AI Act; Конвенція Ради Європи), тоді як військовий сегмент все ще регулюється переважно політичними зобов'язаннями й загальними принципами МГП.

Міжнародна спільнота демонструє політичну волю, але поки що без реальних результатів. Ухвалення резолюції A/78/L.49 і запуск GGE LAWS 2025 свідчать про намір напрацювати універсальний підхід, проте консенсус щодо обов'язкового договору ще не досягнуто.

Серйозними прогалинами є: 1) відсутність єдиного визначення «значущого людського контролю»; 2) трудомісткий механізм атрибуції відповідальності; 3) разюча різниця між рівнем технічної експертизи різних держав.

Подальша адаптація міжнародного права має спиратися на багаторівневу модель, поєднуючи гнучкість «м'якого права» та обов'язковість міжнародних договорів, із чітко визначеним механізмом верифікації й санкцій. Тільки так можна забезпечити баланс між інноваціями й безпекою, захистом прав людини та стратегічною стабільністю у добу активного розвитку штучного інтелекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Меликов Р.Г. Міжнародно-правове регулювання використання автономних систем озброєння під час ведення воєнних дій: дис...доктора філос.; Національний університет «Одеська юридична академія». Одеса, 2023. 205 с.

2. Малишева Н.Р. Кібербезпека космічної діяльності та можливості її забезпечення засобами міжнародного права. *Правова держава*. Випуск 32, 2021. С. 245–257.
3. Федчук Т.Ю. Контроль дотримання норм міжнародного гуманітарного права при використанні зброї керованої штучним інтелектом. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. № 4, 2024. С. 785–791. URL: <https://app-journal.in.ua/wp-content/uploads/2024/04/131.pdf> (дата звернення: 04.07.2025)
4. Меликов Р.Г. Автономні системи озброєння та принцип розрізнення в міжнародному гуманітарному праві. *Право і суспільство*. 2021. № 6. С. 315–320.
5. Додатковий протокол, який стосується захисту жертв міжнародних збройних конфліктів від 8 червня 1977 року: Протокол I до Женевських конвенцій від 12 серпня 1949 року. URL: https://zakon.rada.gov.ua/laws/show/995_199 (дата звернення: 04.07.2025)
6. Статут Організації Об'єднаних Націй від 26 червня 1945 року. URL: https://unic.un.org/aroundworld/unics/common/documents/publications/uncharter/UN%20Charter_Ukrainian.pdf (дата звернення: 04.07.2025)
7. Завадський А.А. Адміністративно-правове регулювання штучного інтелекту у сфері оборони: міжнародний вимір та національні пріоритети. *Збірник наукових праць Харківського національного педагогічного університету імені Г.С. Сковороди «ПРАВО»*. Випуск 40, 2024 р. С. 87–98.
8. Artificial Intelligence Act, Regulation № 2024/1689, European Union. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (дата звернення: 04.07.2025)
9. Прокопович-Ткаченко Д.І., Саричев В.І., Остальцев О.А., Смишляєв С.М., Шаволін А.О. Військові системи AI (MILAI): суспільно-політичні виклики. *Юридичний науковий електронний журнал*. № 4/2024. С. 448–452.