

**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

Кваліфікаційна наукова
праця на правах рукопису

ДЕРКАЧ ОЛЕНА ОЛЕКСАНДРІВНА

УДК 341.9:347.78:347.191.4:339.166.5(043.3)

ДИСЕРТАЦІЯ

**«СТАНОВЛЕННЯ МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ВІЙСЬКОВИХ ЦІЛЯХ»**

Спеціальність 293 «Міжнародне право»

Галузь знань 29 «Міжнародні відносини»

Подається на здобуття наукового ступеня доктора філософії.

Дисертація містить результати власних досліджень. Використання ідей,
результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ О.О. Деркач

(підпис, ініціали та прізвище здобувача)

Науковий керівник: Забара Ігор Миколайович,

Кандидат юридичних наук, доцент.

Київ – 2026

АНОТАЦІЯ

Становлення міжнародно-правового регулювання використання штучного інтелекту у військових цілях - кваліфікаційна наукова праця на правах рукопису.

Дисертаційне дослідження присвячено комплексному аналізу Становлення міжнародно-правового регулювання використання штучного інтелекту у військових цілях. У роботі досліджено штучний інтелект як новий комплексний об'єкт міжнародно-правового осмислення, що формується на перетині міжнародного гуманітарного права, міжнародного права прав людини, права міжнародної безпеки, режимів контролю над озброєннями, кібербезпеки, технічної стандартизації та практики міжнародних організацій.

Актуальність дослідження зумовлена тим, що штучний інтелект поступово переходить із площини загального технологічного розвитку до сфери військового планування, оборонної модернізації, розвідки, кібербезпеки, автономних систем, підтримки прийняття рішень і стратегічної стабільності. Його використання у військовій сфері створює нові виклики для міжнародного права, оскільки алгоритмічні системи можуть впливати на правомірність застосування сили, дотримання міжнародного гуманітарного права, захист цивільного населення, відповідальність держав і контроль над озброєннями.

У роботі обґрунтовано, що чинне міжнародне право не втрачає застосовності до військового використання штучного інтелекту. Водночас його практична реалізація ускладнюється автономністю систем, непрозорістю алгоритмічних рішень, залежністю від даних, швидкістю обробки інформації, участю приватного сектору та складністю визначення належного рівня людського контролю. У зв'язку з цим особливого значення набуває не лише аналіз змісту міжнародно-правових норм, а й дослідження інституційних, технічних і процедурних механізмів, через які ці норми можуть бути реалізовані у військовому домені.

У першому розділі досліджено становлення і розвиток інституту штучного інтелекту в міжнародному праві. Розкрито основні теоретичні підходи до розуміння

штучного інтелекту як міжнародно-правового явища, визначено його міжгалузеву природу та проаналізовано співвідношення актів м'якого права, міжнародних стандартів, регіональних актів і чинних норм міжнародного права. Значну увагу приділено питанню штучного інтелекту як технології подвійного використання, оскільки його цивільне, безпекове і військове застосування формує особливі вимоги до відповідальності, людського контролю, прозорості, управління даними та життєвого циклу системи.

У другому розділі систематизовано основні національні, регіональні та союзницькі підходи до регулювання військового використання штучного інтелекту. Досліджено американську, європейську, далекосхідну та натівську моделі правового й інституційного оформлення військового ШІ. У межах порівняльного аналізу встановлено, що попри відмінності політичних, правових і безпекових підходів, у цих моделях поступово формується спільне нормативне ядро. До нього належать вимоги законності, підзвітності, людського контролю, верифікації, валідації, аудиту, простежуваності, управління ризиками та правової експертизи протягом життєвого циклу військової системи ШІ.

У третьому розділі розглянуто розвиток військової сфери інституту штучного інтелекту в межах міжнародних конференцій та інституцій. Визначено значення конференції REAIM як політико-експертного середовища, у межах якого відповідальне використання ШІ у військовій сфері розглядається не лише крізь призму летальних автономних систем озброєнь, а як ширший військовий домен, що охоплює системи підтримки прийняття рішень, алгоритмічну розвідку, кібероперації, автономні платформи, генеративний ШІ та управління даними. Окремо розкрито роль Організації Об'єднаних Націй у формуванні універсальних доктринальних основ міжнародно-правового регулювання військового ШІ.

У дослідженні доведено, що міжнародно-правове регулювання військового штучного інтелекту формується не шляхом одномоментного прийняття універсального договору, а як багаторівневий процес. Він поєднує чинні норми міжнародного права,

акти м'якого права, регіональні моделі, союзницькі стандарти, гуманітарно-правові обмеження, технічні процедури, політичні декларації та універсальні доктринальні акти. Такий процес відображає поступову юридизацію відповідального використання штучного інтелекту у військовій сфері та водночас зберігає значення вже чинних норм міжнародного права.

Наукова новизна роботи полягає у комплексному розгляді військового штучного інтелекту не лише як технологічного або етичного явища, а як окремого напрямку становлення міжнародно-правового регулювання. У роботі систематизовано національні, регіональні та союзницькі моделі регулювання військового ШІ, визначено їхнє спільне нормативне ядро, обґрунтовано значення REAIM як проміжного нормативного середовища та розкрито роль ООН у формуванні перших універсальних доктринальних засад військового ШІ.

Практичне значення одержаних результатів полягає у можливості їх використання для подальших наукових досліджень у сфері міжнародного права новітніх військових технологій, підготовки навчальних матеріалів, аналізу національних стратегій у сфері військового ШІ, розроблення підходів до правової експертизи систем штучного інтелекту, а також формування позицій держав у межах ООН, REAIM, НАТО, Конвенції про конкретні види звичайної зброї та інших міжнародних форматів співробітництва.

Ключові слова: Штучний інтелект, використання штучного інтелекту міжнародно-правове регулювання, міжнародне гуманітарне право, технології подвійного використання, міжнародна безпека, збройний конфлікт, міжнародна відповідальність, REAIM, НАТО, системи управління, кібератака, спецслужби.

ABSTRACT

The Formation of International Legal Regulation of the Use of Artificial Intelligence in the Military Sphere is a qualification scholarly work submitted as a manuscript.

The dissertation research is devoted to a comprehensive analysis of the formation of international legal regulation of the use of artificial intelligence in the military sphere. The study examines artificial intelligence as a new complex object of international legal understanding, formed at the intersection of international humanitarian law, international human rights law, the law of international security, arms control regimes, cybersecurity, technical standardization, and the practice of international organizations.

The relevance of the research is determined by the fact that artificial intelligence is gradually moving from the sphere of general technological development into the field of military planning, defence modernization, intelligence, cybersecurity, autonomous systems, decision-making support, and strategic stability. Its use in the military sphere creates new challenges for international law, since algorithmic systems may affect the legality of the use of force, compliance with international humanitarian law, the protection of civilians, state responsibility, and arms control.

The study substantiates that existing international law does not lose its applicability to the military use of artificial intelligence. At the same time, its practical implementation is complicated by the autonomy of systems, the opacity of algorithmic decisions, dependence on data, the speed of information processing, the involvement of the private sector, and the difficulty of determining the appropriate level of human control. In this regard, particular importance is attached not only to the analysis of the content of international legal norms, but also to the study of the institutional, technical, and procedural mechanisms through which these norms can be implemented in the military domain.

The first chapter examines the formation and development of the institution of artificial intelligence in international law. It reveals the main theoretical approaches to understanding artificial intelligence as an international legal phenomenon, defines its cross-sectoral nature, and analyzes the correlation between soft law instruments, international standards, regional

acts, and existing norms of international law. Considerable attention is paid to the issue of artificial intelligence as a dual-use technology, since its civilian, security, and military applications create specific requirements regarding responsibility, human control, transparency, data governance, and the life cycle of the system.

The second chapter systematizes the main national, regional, and allied approaches to the regulation of the military use of artificial intelligence. It examines the American, European, Far Eastern, and NATO models of the legal and institutional structuring of military AI. Within the framework of the comparative analysis, it is established that, despite differences in political, legal, and security approaches, these models are gradually forming a common normative core. This core includes the requirements of legality, accountability, human control, verification, validation, audit, traceability, risk management, and legal review throughout the life cycle of a military AI system.

The third chapter considers the development of the military dimension of the institution of artificial intelligence within international conferences and institutions. It determines the significance of the REAIM conference as a political and expert environment in which the responsible use of AI in the military sphere is considered not only through the prism of lethal autonomous weapons systems, but also as a broader military domain encompassing decision-support systems, algorithmic intelligence, cyber operations, autonomous platforms, generative AI, and data governance. The role of the United Nations in shaping the universal doctrinal foundations of international legal regulation of military AI is examined separately.

The research proves that international legal regulation of military artificial intelligence is not being formed through the immediate adoption of a universal treaty, but rather as a multi-level process. It combines existing norms of international law, soft law instruments, regional models, allied standards, humanitarian legal restrictions, technical procedures, political declarations, and universal doctrinal acts. This process reflects the gradual legalization of the responsible use of artificial intelligence in the military sphere while preserving the significance of already existing norms of international law.

The scientific novelty of the work lies in the comprehensive consideration of military artificial intelligence not merely as a technological or ethical phenomenon, but as a distinct area in the formation of international legal regulation. The study systematizes national, regional, and allied models of military AI regulation, identifies their common normative core, substantiates the significance of REAIM as an intermediate normative environment, and reveals the role of the UN in shaping the first universal doctrinal foundations of military AI.

The practical significance of the results obtained lies in the possibility of their use for further scholarly research in the field of international law of emerging military technologies, the preparation of educational materials, the analysis of national strategies in the field of military AI, the development of approaches to the legal review of artificial intelligence systems, as well as the formation of states' positions within the UN, REAIM, NATO, the Convention on Certain Conventional Weapons, and other international cooperation formats.

Key words: Artificial intelligence, the use of artificial intelligence, international legal regulation, international humanitarian law, dual-use technologies, international security, armed conflict, international responsibility, REAIM, NATO, management systems, cyberattack, special services.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	9
РОЗДІЛ 1. СТАНОВЛЕННЯ І РОЗВИТОК ІНСТИТУТУ ШТУЧНОГО ІНТЕЛЕКТУ В МІЖНАРОДНОМУ ПРАВІ.....	22
1.1. Поняття інституту «штучний інтелект» в міжнародному праві: теоретичні підходи	22
1.2. Штучний інтелект як технологія подвійного використання: міжнародно-правові аспекти	44
1.3. Роль глобалізації у формуванні міжнародно-правових засад інституту штучного інтелекту ..	60
Висновки до 1-го розділу	70
РОЗДІЛ 2. СТАНОВЛЕННЯ ЗАСАД МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВІЙСЬКОВОГО ВИКОРИСТАННЯ ІНСТИТУТУ ШТУЧНОГО ІНТЕЛЕКТУ	71
2.1. Американський підхід до міжнародно-правового регулювання використання [технологій] штучного інтелекту у військовій та безпековій сферах	71
2.2. Європейські підходи до міжнародно-правового регулювання використання [технологій] штучного інтелекту у військовій та безпековій сферах	91
2.3. Далекосхідні підходи до міжнародно-правового регулювання використання [технологій] штучного інтелекту у військовій та безпековій сферах	112
2.4. Концептуальні підходи НАТО до міжнародно-правового регулювання використання штучного інтелекту у військовій сфері	136
Висновки до 2-го розділу	147
РОЗДІЛ 3. РОЗВИТОК ВІЙСЬКОВОЇ СФЕРИ ІНСТИТУТУ ШТУЧНОГО ІНТЕЛЕКТУ В РАМКАХ МІЖНАРОДНИХ КОНФЕРЕНЦІЙ І ІНСТИТУЦІЙ.....	148
3.1. REAİM: визначення засад використання штучного інтелекту у військовій сфері.....	148
3.2. ООН: формування універсальних доктринальних основ використання штучного інтелекту у військовій сфері	170
Висновки до 3-го розділу	190
ВИСНОВКИ	192
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	198
ДОДАТКИ.....	218

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AI — Artificial Intelligence, штучний інтелект.

AI Act — Artificial Intelligence Act, Акт Європейського Союзу про штучний інтелект.

AISI — Artificial Intelligence Safety Institute, Інститут безпеки штучного інтелекту.

AJIL — American Journal of International Law, Американський журнал міжнародного права.

CCW — Convention on Certain Conventional Weapons, Конвенція про конкретні види звичайної зброї.

CCW GGE — Group of Governmental Experts within the Convention on Certain Conventional Weapons, Група урядових експертів у межах Конвенції про конкретні види звичайної зброї.

CETS — Council of Europe Treaty Series, серія договорів Ради Європи.

C-UAS — Counter-Unmanned Aircraft Systems, системи протидії безпілотним авіаційним системам.

DAIC — Defence Artificial Intelligence Centre, Оборонний центр штучного інтелекту.

DAPA — Defense Acquisition Program Administration, Адміністрація оборонних закупівель Республіки Корея.

DARB — Data and Artificial Intelligence Review Board, Рада з питань даних і штучного інтелекту НАТО.

DGA — Direction générale de l'armement, Генеральна дирекція з озброєнь Франції.

DIANA — Defence Innovation Accelerator for the North Atlantic, Оборонний інноваційний акселератор для Північної Атлантики.

DPIA — Data Protection Impact Assessment, оцінка впливу на захист даних.

DSA — Digital Services Act, Акт Європейського Союзу про цифрові послуги.

EU — European Union, Європейський Союз.

G7 — Group of Seven, Група семи.

GA UN — General Assembly of the United Nations, Генеральна Асамблея Організації Об'єднаних Націй.

GPAI — Global Partnership on Artificial Intelligence, Глобальне партнерство зі штучного інтелекту.

HRIA — Human Rights Impact Assessment, оцінка впливу на права людини.

ICRC — International Committee of the Red Cross, Міжнародний Комітет Червоного Хреста.

ICT — Information and Communication Technologies, інформаційно-комунікаційні технології.

IEEE — Institute of Electrical and Electronics Engineers, Інститут інженерів з електротехніки та електроніки.

IHL — International Humanitarian Law, міжнародне гуманітарне право.

IHRL — International Human Rights Law, міжнародне право прав людини.

IMO — International Maritime Organization, Міжнародна морська організація.

LAWS — Lethal Autonomous Weapon Systems, летальні автономні системи озброєнь.

LLMOps — Large Language Model Operations, операційне управління великими мовними моделями.

MASS — Maritime Autonomous Surface Ships, морські автономні надводні судна.

MHC — Meaningful Human Control, значущий людський контроль.

MLOps — Machine Learning Operations, операційне управління системами машинного навчання.

NATO — North Atlantic Treaty Organization, Організація Північноатлантичного договору.

OECD — Organisation for Economic Co-operation and Development, Організація економічного співробітництва та розвитку.

REAIM — Responsible Artificial Intelligence in the Military Domain, відповідальне використання штучного інтелекту у військовій сфері.

TRIPS — Agreement on Trade-Related Aspects of Intellectual Property Rights, Угода про торговельні аспекти прав інтелектуальної власності.

UN — United Nations, Організація Об'єднаних Націй.

UNESCO — United Nations Educational, Scientific and Cultural Organization, Організація Об'єднаних Націй з питань освіти, науки і культури.

WHO — World Health Organization, Всесвітня організація охорони здоров'я.

WIPO — World Intellectual Property Organization, Всесвітня організація інтелектуальної власності.

WoS — Web of Science, міжнародна наукометрична база даних Web of Science.

AI — Artificial Intelligence, штучний інтелект; використовується у випадках передачі англomовної абрeвіатури в українському тексті.

БПЛА — безпілотний літальний апарат.

ВООЗ — Всесвітня організація охорони здоров'я.

ВІПО — Всесвітня організація інтелектуальної власності.

ГА ООН — Генеральна Асамблея Організації Об'єднаних Націй.

ГП — глобальне інформаційне суспільство.

ЄС — Європейський Союз.

ЄСПЛ — Європейський суд з прав людини.

ІКТ — інформаційно-комунікаційні технології.

КНР — Китайська Народна Республіка.

LAWS / ЛАСО — летальні автономні системи озброєнь; у роботі переважно використовується англomовне скорочення LAWS.

МПП — міжнародне гуманітарне право.

МКЧХ — Міжнародний Комітет Червоного Хреста.

МП — міжнародне право.

МППЛ — міжнародне право прав людини.

НАТО — Організація Північноатлантичного договору.

НДР — науково-дослідна робота.

ОЕСР — Організація економічного співробітництва та розвитку.

ООН — Організація Об'єднаних Націй.

ОНП — освітньо-наукова програма.

РЄ — Рада Європи.

РК — Республіка Корея.

США — Сполучені Штати Америки.

ШІ — штучний інтелект.

ЮНЕСКО — Організація Об'єднаних Націй з питань освіти, науки і культури.

ВСТУП

Актуальність теми дослідження зумовлена тим, що штучний інтелект поступово переходить із площини загального технологічного розвитку до сфери військового планування, оборонної модернізації, розвідки, кібербезпеки, автономних систем, підтримки прийняття рішень і стратегічної стабільності. Його використання у військовій сфері створює якісно нову ситуацію для міжнародного права, оскільки алгоритмічні системи можуть впливати не лише на технічну ефективність військових операцій, а й на правомірність застосування сили, дотримання міжнародного гуманітарного права, захист цивільного населення, відповідальність держав і контроль над озброєннями.

Особливість проблематики полягає в тому, що чинне міжнародне право не втрачає застосовності до військового використання штучного інтелекту, однак потребує нових процедурних форм реалізації. Норми Статуту ООН, міжнародного гуманітарного права, міжнародного права людини, міжнародної відповідальності та режимів міжнародної безпеки залишаються чинними, проте їх практичне застосування ускладнюється автономністю, непрозорістю алгоритмів, залежністю систем від даних, швидкістю прийняття рішень, участю приватного сектору та складністю визначення належного рівня людського контролю. У зв'язку з цим особливого значення набуває аналіз не лише змісту правових норм, а й тих інституційних, технічних і доктринальних механізмів, через які ці норми можуть бути реалізовані у військовому домені.

Становлення міжнародно-правового регулювання військового штучного інтелекту відбувається не одномоментно і не через один універсальний договір. Воно формується через поєднання національних стратегій, регіональних підходів, союзницьких стандартів, актів м'якого права, політичних декларацій, технічних стандартів, позицій міжнародних організацій і доктринальних напрацювань. Саме тому дослідження цієї теми потребує системного підходу, який дозволяє простежити перехід від загального становлення інституту штучного інтелекту в міжнародному праві до формування спеціальних моделей його військового регулювання, а далі до перших

універсальних доктринальних закріплень на рівні REAIM та Організації Об'єднаних Націй.

У науковій літературі питання штучного інтелекту розглядається у контексті прав людини, цифрового врядування, етики, міжнародної безпеки, автономної зброї та відповідальності держав. Водночас комплексне дослідження військового штучного інтелекту як окремого напрямку становлення міжнародно-правового регулювання потребує подальшого розвитку. Особливої уваги потребують регіональні та національно-союзницькі моделі правового оформлення військового ШІ, а також перехід від таких моделей до універсальних міжнародних підходів, закріплених у процесі REAIM і резолюціях Генеральної Асамблеї ООН.

Метою роботи є комплексне дослідження Становлення міжнародно-правового регулювання використання штучного інтелекту у військових цілях, визначення його інституційних, доктринальних і нормативних особливостей, а також з'ясування ролі національних, регіональних, союзницьких та універсальних міжнародних підходів у формуванні майбутнього правового режиму військового ШІ.

Для досягнення поставленої мети необхідно вирішити такі **завдання**:

1. дослідити становлення інституту штучного інтелекту в міжнародному праві, визначити його правову природу, міжгалузевий характер, основні доктринальні підходи до його розуміння та місце в системі сучасних міжнародно-правових інститутів;
2. проаналізувати особливості формування міжнародно-правового регулювання штучного інтелекту на етапі 2017-2026 рр., з урахуванням відсутності єдиного універсального конвенційного визначення штучного інтелекту та військового штучного інтелекту, а також ролі міжнародних і регіональних організацій у виробленні базових правових, етичних, технічних і безпекових підходів;
3. визначити взаємозв'язок цивільного, безпекового та військового застосування штучного інтелекту як технології подвійного використання, а також визначити його значення для міжнародного гуманітарного права, міжнародного права

прав людини, права міжнародної безпеки, кібербезпеки, контролю над озброєннями та режимів відповідальності;

4. розкрити вплив глобалізації, діджиталізації та цифрової конвергенції на розвиток інституту штучного інтелекту, зокрема на формування нових умов транскордонного обігу даних, масштабування алгоритмічних систем, взаємопроникнення цивільних і військових технологій та потребу в особливому міжнародно-правовому режимі їх використання;

5. охарактеризувати американський, європейський і далекосхідний підходи до міжнародно-правового регулювання використання штучного інтелекту у військовій та безпековій сферах, визначити їхні спільні й відмінні риси, правові, інституційні та доктринальні особливості, а також значення для формування майбутніх міжнародних стандартів відповідального військового ШІ;

6. визначити основні проблеми міжнародно-правового регулювання військового штучного інтелекту, зокрема питання летальних автономних систем озброєнь, значущого людського контролю, категоризації систем за рівнем автономності та ризику, відповідальності за шкоду, алгоритмічної непрозорості, міжнародного нагляду та застосування ШІ у збройних конфліктах;

7. дослідити концептуальні підходи НАТО та процесу REAIM до відповідального використання штучного інтелекту у військовій сфері, визначити їхню правову і політичну природу, інституційно-стандартизаційне значення, межі впливу та роль у формуванні спільної мови відповідального, підконтрольного і правомірного військового ШІ;

8. обґрунтувати роль Організації Об'єднаних Націй у формуванні універсальних доктринальних основ використання штучного інтелекту у військовій сфері та сформулювати авторське бачення перспективного розвитку міжнародного права у цій сфері, що передбачає закріплення базових принципів, створення спеціалізованих механізмів контролю, розроблення підходів для цивільної і військової сфер та узгодження міжнародного права з національними правовими системами.

Об'єктом дослідження є міжнародно-правові відносини, що виникають у процесі розробки, регулювання, впровадження і використання технологій штучного інтелекту у військовій сфері.

Предметом дослідження є Становлення міжнародно-правового регулювання використання штучного інтелекту у військових цілях, його доктринальні засади, регіональні й союзницькі моделі, універсальні підходи ООН та REAIM, а також правові проблеми відповідальності, людського контролю, управління ризиками і життєвого циклу військових систем ШІ.

Методологічну основу дослідження становить поєднання загальнонаукових і спеціально-юридичних методів. Діалектичний метод використано для аналізу розвитку міжнародно-правового регулювання ШІ як динамічного процесу. Системний метод дав змогу розглянути військовий ШІ як комплексний об'єкт, пов'язаний із міжнародним гуманітарним правом, міжнародною безпекою, правами людини, контролем над озброєннями та кібербезпекою. Порівняльно-правовий метод застосовано для зіставлення американської, європейської, далекосхідної та натівської моделей. Формально-юридичний метод використано для аналізу резолюцій ООН, документів REAIM, актів НАТО, позицій МКЧХ та інших міжнародно-правових і політико-правових документів. Метод правового моделювання дав змогу визначити можливі напрями подальшої юридикації військового ШІ.

Наукова новизна роботи полягає у комплексному розгляді військового штучного інтелекту не лише як технологічного або етичного явища, а як окремого напрямку становлення міжнародно-правового регулювання. У роботі систематизовано національні, регіональні та союзницькі моделі регулювання військового ШІ, визначено їхнє спільне нормативне ядро, обґрунтовано значення REAIM як проміжного нормативного середовища та розкрито роль ООН у формуванні перших універсальних доктринальних засад військового ШІ.

Практичне значення одержаних результатів полягає у можливості використання висновків роботи для подальших наукових досліджень у сфері міжнародного права

новітніх військових технологій, підготовки навчальних матеріалів, аналізу національних стратегій у сфері військового ШІ, розроблення підходів до правової експертизи систем ШІ, а також формування позицій держав у межах ООН, REAIM, НАТО, CCW та інших міжнародних форматів.

Особистий внесок здобувача. Дисертаційне дослідження є самостійною науковою працею здобувачки, у якій сформульовано авторський підхід до розуміння Становлення міжнародно-правового регулювання використання штучного інтелекту у військових цілях. Особистий внесок здобувачки полягає у визначенні військового штучного інтелекту як комплексного об'єкта міжнародно-правового регулювання, систематизації національних, регіональних, союзницьких та універсальних підходів до його правового оформлення, виокремленні спільного нормативного ядра відповідального військового ШІ, а також обґрунтуванні значення REAIM та Організації Об'єднаних Націй у формуванні доктринальних засад майбутнього міжнародно-правового режиму військового штучного інтелекту. У наукових працях, підготовлених у співавторстві, особистий внесок здобувачки полягає в аналізі міжнародно-правових аспектів використання штучного інтелекту у військовій сфері, дослідженні проблем відповідального ШІ, летальних автономних систем озброєнь, міжнародного правопорядку, а також сучасних напрямів наукових досліджень технологій військового штучного інтелекту.

Апробація матеріалів дисертації. Основні положення, висновки та окремі результати дисертаційного дослідження апробовано шляхом підготовки й опублікування наукових праць за темою дисертації. Результати дослідження відображено у публікаціях, присвячених використанню штучного інтелекту для аналізу впливу військово-технічного співробітництва на формування політичних альянсів, міжнародному захисту прав людини в умовах діджиталізації та розвитку штучного інтелекту, військовим викликам штучного інтелекту для міжнародного порядку, а також сучасним міжнародно-правовим напрямам наукових досліджень технологій військового штучного інтелекту. Зазначені публікації засвідчують апробацію ключових

теоретичних і прикладних положень роботи, зокрема щодо міжнародно-правового регулювання штучного інтелекту, відповідального військового ШІ, міжнародного гуманітарного права, міжнародної безпеки, REAIM, летальних автономних систем озброєнь та глобального інформаційного суспільства.

Публікації за темою дисертації. Основні наукові результати дисертаційного дослідження висвітлено у чотирьох наукових публікаціях здобувачки. Серед них одна публікація в іноземному періодичному виданні, індексованому в міжнародних наукометричних базах, а саме: Aliksieienko I., Huta S., Bohuslavets A., Derkach O., Derkach O. The use of artificial intelligence for analysing the impact of Military Technical Cooperation on political alliance establishment in XX-XXI centuries 2025 року, DOI: 10.5281/ZENODO.15659390. Також результати дослідження відображено у фахових наукових виданнях України: у статті Деркач О. О. Міжнародний захист прав людини в умовах діджиталізації та розвитку штучного інтелекту: міжнародно-правові стандарти 2024 року, DOI: 10.32782/2663-5666.2024.4.15; у статті Derkach O., Zabara I. Artificial intelligence: military challenges to international order and contours of international legal regulation 2025 року, DOI: 10.17721/apmv.2024.161.1.109-114; а також у статті Забара І. М., Деркач О. О. Технології військового штучного інтелекту: сучасні міжнародно-правові напрямки наукових досліджень 2024 року, DOI: 10.24144/2307-3322.2024.86.5.36.

Структура та обсяг дисертації. Структура дисертації зумовлена метою, завданнями, об'єктом і предметом дослідження. Дисертація складається зі вступу, трьох розділів, які об'єднують дев'ять підрозділів, висновків до розділів, загальних висновків, списку використаних джерел та додатків. У першому розділі досліджено становлення і розвиток інституту штучного інтелекту в міжнародному праві, його теоретичні засади, міжгалузеву природу, подвійне використання та вплив глобалізації на формування міжнародно-правових підходів. У другому розділі розкрито національні, регіональні та союзницькі моделі регулювання військового штучного інтелекту, зокрема американський, європейський, далеосхідний та натівський підходи.

У третьому розділі проаналізовано розвиток військової сфери інституту штучного інтелекту в межах міжнародних конференцій та інституцій, передусім REAIM та Організації Об'єднаних Націй. Загальний обсяг дисертації становить 221 сторінку, з яких основний текст охоплює вступ, три розділи та загальні висновки; список використаних джерел і додатки подано після основної частини роботи.

Наукова новизна одержаних результатів. Наукова новизна одержаних результатів полягає у комплексному дослідженні Становлення міжнародно-правового регулювання використання штучного інтелекту у військових цілях як нового міжгалузевого напрямку розвитку міжнародного права, що формується на перетині міжнародного гуманітарного права, міжнародного права прав людини, права міжнародної безпеки, режимів контролю над озброєннями, кібербезпеки, технічної стандартизації та практики міжнародних організацій.

Вперше у межах дослідження обґрунтовано, що військовий штучний інтелект доцільно розглядати не лише як нову технологію або окрему категорію озброєння, а як цілісний об'єкт міжнародно-правового регулювання, який впливає на весь цикл прийняття рішень у сфері застосування сили: від збору даних, розвідки, аналізу оперативної обстановки і підтримки командування до автономізації окремих функцій, вибору цілей, кібероперацій, інформаційного впливу та стратегічної стабільності.

Вперше запропоновано розглядати становлення міжнародно-правового регулювання військового штучного інтелекту як багаторівневий процес, у якому національні та регіональні моделі формують початкові підходи до поєднання інновацій і контролю, НАТО конкретизує принципи відповідального військового ШІ в союзницькому оборонному середовищі, REAIM створює політико-експертний простір для вироблення спільної мови відповідального військового ШІ, а ООН надає цим процесам універсального доктринального значення.

Вперше систематизовано американський, європейський і далеосхідний підходи до міжнародно-правового регулювання військового використання штучного інтелекту не лише як окремі політико-правові моделі, а як елементи ширшого процесу

формування майбутнього міжнародного режиму відповідального, підконтрольного і правомірного використання військового ШІ.

Вперше обґрунтовано, що основна проблема міжнародно-правового регулювання військового ШІ полягає не у відсутності права як такого, а у недостатній пристосованості чинних норм до алгоритмічної, автономної, технічно складної та багаторівневої природи нових військових систем. У цьому контексті доведено, що чинні норми міжнародного гуманітарного права, міжнародного права прав людини, міжнародної відповідальності та міжнародної безпеки не втрачають юридичного значення, але потребують нових процедурних форм реалізації.

Удосконалено науковий підхід до розуміння штучного інтелекту як технології подвійного використання, що створює перетин правових режимів, оскільки цивільні інновації у сфері медицини, транспорту, освіти, цифрових послуг, аналізу даних і автоматизованого прийняття рішень одночасно формують потенціал для безпекового і військового застосування.

Удосконалено характеристику ролі НАТО у формуванні стандартів відповідального військового ШІ. Доведено, що підхід Альянсу має не договірний, а інституційно-стандартизаційний характер, оскільки він поєднує правові принципи, політичні зобов'язання, внутрішні процедури оцінки, технологічну інфраструктуру, інтероперабельність і партнерську інноваційну екосистему.

Набуло подальшого розвитку положення про значення процесу REAIM як проміжного політико-правового середовища, у межах якого військовий ШІ розглядається не лише через проблематику летальних автономних систем озброєнь, а як ширший військовий домен, що охоплює системи підтримки прийняття рішень, алгоритмічну розвідку, кібероперації, автономні платформи, генеративний ШІ, управління даними і стратегічну стабільність.

Набуло подальшого розвитку положення про роль ООН у формуванні універсальних доктринальних основ регулювання військового ШІ. Обґрунтовано, що

специфіка підходу ООН полягає не у створенні завершеного договірному режиму, а у визначенні мінімально узгоджених правових, гуманітарних, технічних, етичних і безпекових орієнтирів, які можуть бути використані державами для розвитку національних стратегій, міждержавної співпраці та майбутніх міжнародно-правових інструментів.

РОЗДІЛ 1. СТАНОВЛЕННЯ І РОЗВИТОК ІНСТИТУТУ ШТУЧНОГО ІНТЕЛЕКТУ В МІЖНАРОДНОМУ ПРАВІ

1.1. Поняття інституту «штучний інтелект» в міжнародному праві: теоретичні підходи

У теорії міжнародного права інститут - це комплекс міжнародно-правових норм, що регулюють певну однорідну сферу відносин або специфічне поняття в межах ширшої галузі [1, с. 29]. Виникнення нових явищ у відносинах нерідко веде до формування відповідних нових інститутів або навіть галузей міжнародного права. Зокрема, у XX столітті розвиток технологій та нових сфер діяльності породив такі нові галузі, як міжнародне космічне право, міжнародне екологічне право, міжнародне атомне право тощо. В контексті дослідження постає необхідність уточнення категоріального апарату, а саме формування інституту штучного інтелекту у міжнародному праві, та його розуміння.

Штучний інтелект, як феномен, не розглядається як складова у жодній традиційній галузі права, натомість перетинається з багатьма з них - від прав людини до міжнародної безпеки. Теоретики виділяють декілька підходів до правового осмислення використання штучного інтелекту у міжнародних відносинах.

У цьому контексті важливо враховувати, що штучний інтелект не є лише технічною категорією. У міжнародному праві він поступово набуває значення комплексного регуляторного об'єкта, оскільки одночасно пов'язаний із правами людини, цифровою безпекою, міжнародним гуманітарним правом, міжнародною відповідальністю, економічними режимами, трансфером технологій, інтелектуальною власністю та діяльністю міжнародних організацій. Саме ця багатовимірність ускладнює його включення до традиційної системи міжнародно-правових інститутів. Якщо класичні інститути міжнародного права формувалися навколо відносно визначених сфер, наприклад правонаступництва держав, дипломатичного захисту або відповідальності держав, то інститут штучного інтелекту формується на перетині кількох режимів, що вже мають власну логіку, джерела і механізми реалізації [1; 5; 6].

Окремого значення набуває питання про те, чи може штучний інтелект бути самостійним предметом міжнародно-правового регулювання, або він має розглядатися лише як технологічний чинник, що впливає на вже існуючі інститути. Перший підхід передбачає формування нового комплексного інституту, який матиме власні принципи, власні критерії ризику, власні механізми контролю та, можливо, спеціальний міжнародний орган координації. Другий підхід виходить із того, що міжнародне право вже має достатній набір інструментів для реагування на технологічні зміни, а тому потребує не створення нової галузі, а адаптації чинних норм до нових умов. У такому розумінні штучний інтелект не руйнує систему міжнародного права, а виявляє її слабкі місця, передусім у питаннях імпутації дій, відповідальності, людського контролю, доказування та транскордонної шкоди [5; 6; 7; 8].

У фаховій літературі виокремлено дві провідні позиції правового осмислення ШІ на міжнародній арені.

Перша наполягає на формуванні окремого міжнародно-правового інституту й навіть спеціалізованого органу на кшталт Міжнародного агентства з атомної енергії для штучного інтелекту; цю лінію системно обґрунтовує Simon Chesterman [2, с. 186-188], політичну підтримку ідеї висловлював Генеральний секретар Організації Об'єднаних Націй António Guterres [3], а у військовому вимірі Міжнародний Комітет Червоного Хреста послідовно закликає до юридично зобов'язуючих норм щодо автономних систем озброєння із збереженням значущого людського контролю [4].

Цей підхід фактично виходить із того, що фрагментарного застосування існуючих норм недостатньо. Штучний інтелект створює новий тип регуляторної проблеми, оскільки рішення може прийматися або підтримуватися системою, яка діє із певним рівнем автономності, навчається на великих масивах даних, має непрозорий алгоритмічний механізм та здатна масштабувати наслідки помилки. У правовому вимірі це означає, що традиційний зв'язок між дією, суб'єктом, виною, контролем і відповідальністю стає складнішим. Саме тому прихильники окремого інституту виходять із потреби в єдиних міжнародних принципах, процедурних гарантіях,

режимах аудиту, правилах оцінки ризику та міжнародному моніторингу найбільш небезпечних систем [2; 3; 4].

Друга, тобто інтеграційна, виходить із достатності та еластичності чинної архітектури міжнародного права: застосування норм прав людини, міжнародного гуманітарного права, режимів відповідальності та експортного контролю з поступовою деталізацією під нові технології; цю лінію послідовно артикулюють, зокрема, Ashley Deeks, вступ до симпозіуму AJIL Unbound і стаття High-Tech International Law [5, с. 138-140; 6, с. 580-585], та Rebecca Crootoof, праці про автономні озброєння й межі аналогії в міжнародному гуманітарному праві [7, с. 1355-1360; 8, с. 60-66].

Інтеграційний підхід має значну доктринальну вагу, оскільки він не потребує радикального перегляду системи міжнародного права. Його логіка полягає у тому, що міжнародне право вже неодноразово адаптувалося до нових технологій. Так було у випадку з космічною діяльністю, ядерною енергетикою, кіберпростором, біомедичними технологіями та новими видами озброєнь. Відповідно, штучний інтелект може бути включений до вже наявної нормативної архітектури через роз'яснення чинних принципів, ухвалення керівних документів, формування технічних стандартів, розвиток практики міжнародних організацій та уточнення державних зобов'язань. У такій моделі штучний інтелект не отримує статусу самостійного правового центру, але стає чинником, який модифікує зміст уже відомих інститутів [5; 6; 8].

Окремо триває дискусія про міжнародну правосуб'єктність ШІ: чи може надрозвинутий ШІ отримати статус самостійного суб'єкта нарівні з державами або міжнародними організаціями. Класична доктрина вважає головними суб'єктами міжнародного права держави, а міжнародним організаціям визнає похідну правосуб'єктність; часткову правосуб'єктність мають нації/народи та фізичні особи, передусім у сфері прав людини [9, с. 115-120]. Наразі ШІ не є суб'єктом міжнародного права, оскільки не володіє ні територією, ні суверенітетом, ні власною волею у правовому сенсі; проте в науковому дискурсі з'являлися припущення про обмежену електронну правосуб'єктність. Зокрема, у Резолюції Європарламенту 2017 р. було

запропоновано розглянути створення спеціальної правової категорії для електронних осіб, довгостроково, для найскладніших автономних роботів [10]. У теорії це питання осмислювали як можливість наділення ШІ правами/обов'язками за аналогією з корпораціями чи міжнародними організаціями, див. L. B. Solum [11, с. 1231-1235], однак значна частина представників доктрини, зокрема J. J. Bryson, M. E. Diamantis, T. D. Grant, переконливо застерігає від такої моделі як такої, що радше ускладнює притягнення до відповідальності й розмиває людський контроль [12, с. 273-275, 285-289]. Тому практичний фокус регулювання сьогодні зосереджено на питаннях відповідальності людських і державних агентів, розробників, провайдерів, операторів, користувачів і держав, а не зміна кола суб'єктів міжнародного права [9, с. 115-120; 12, с. 285-289].

З огляду на це, питання правосуб'єктності штучного інтелекту доцільно розглядати не як безпосередній напрям сучасного міжнародно-правового регулювання, а як доктринальний індикатор ширшої проблеми відповідальності. Сама по собі автономність технологічної системи не створює міжнародної правосуб'єктності, оскільки міжнародне право пов'язує правосуб'єктність із здатністю бути носієм прав і обов'язків у межах міжнародного правопорядку. Штучний інтелект не може самостійно брати на себе міжнародні зобов'язання, реалізовувати міжнародну відповідальність, вступати у договірні відносини, здійснювати дипломатичні функції або бути стороною міжнародного спору. Тому його автономність має значення для встановлення фактичного ланцюга прийняття рішення, але не для визнання його суб'єктом міжнародного права [9; 11; 12].

Водночас дискусія про правосуб'єктність не є зайвою для теми інституту штучного інтелекту. Вона демонструє, що міжнародне право стикається з явищем, у якому розподіл контролю, знання і відповідальності може бути непрямим. Наприклад, у випадку автономної системи озброєння рішення про вибір цілі може бути технічно пов'язане з алгоритмічною класифікацією, але юридично відповідальність має залишатися за людьми та державами, які розробили, перевірили, дозволили,

застосували або не запобігли неправомірному використанню такої системи. Саме тому концепція електронної особи сьогодні не стала основою міжнародно-правового регулювання, а домінуючим є підхід, за яким нові технології мають вписуватися в систему людської, організаційної та державної відповідальності [7; 8; 12].

1.1.1. Термін інститут у контексті міжнародного права та його застосування до штучного інтелекту

Чисельність міжнародних ініціатив і прийнятих норм останніх років демонструє еволюційне формування міжгалузевого інституту регулювання ШІ на перетині кількох правопорядків [17; 18, с. 1-2; 13; 14; 15; 16]. У доктрині інститут розуміють як відносно самостійну підсистему норм і принципів, що впорядковує однорідну сферу відносин у межах системи міжнародного права; інститути можуть бути загальносистемними, галузевими та міжгалузевими [17; 18, с. 1-2]. У наданих матеріалах це окреслено як поступову інституціоналізацію ШІ через нарощування принципів, процедур і наглядових механізмів [17; 18, с. 2-3].

Початковий імпульс надали норми м'якого права, *soft law*, людиноцентричність, недискримінація, прозорість, підзвітність, людський нагляд, який став орієнтиром для державної політики й ліг в основу подальших рішень [13; 18, с. 3-4].

Наступний етап - юридизація: перехід від декларативних засад до обов'язкових міжнародно-правових стандартів у регіональних рамках із поширенням вимог на весь життєвий цикл систем ШІ [14; 18, с. 6]. Паралельно міжурядові формати виробляють узгоджені підходи та добровільні кодекси для розробників, що зближує політику і практики впровадження в державах [15; 16; 18, с. 6-7]. У безпековому вимірі послідовно артикулюється запит на юридично зобов'язуючі обмеження щодо автономних систем озброєння і збереження значущого людського контролю, що доповнює чинні норми міжнародного гуманітарного права [4; 7; 8; 18, с. 6-7].

Сформований масив актів має гібридну природу: поєднує обов'язкові договори, *soft law*, технічні стандарти та наглядові практики [13; 14; 15; 16; 18, с. 1-4].

Ця гібридність є однією з ключових ознак становлення інституту штучного інтелекту у міжнародному праві. На відміну від класичних інститутів, де домінуючим джерелом часто виступає міжнародний договір або звичаєва норма, регулювання штучного інтелекту формується через одночасне накопичення різних за юридичною силою актів. До нього входять рекомендації міжнародних організацій, рамкові конвенції, політичні декларації, технічні стандарти, етичні принципи, національні стратегії, документи професійних організацій та практики приватних технологічних компаній. Така структура не є випадковою, оскільки сам об'єкт регулювання швидко змінюється і не завжди може бути охоплений одним універсальним договором [13; 14; 15; 16].

У сфері цивільно-правових відносин домінує інтеграційний підхід: застосування гарантій приватності, недискримінації та процесуальних прав до алгоритмічних рішень із фокусом на відповідальності людських і державних суб'єктів; концепт електронної особи розглядають як теоретичний маркер дискусії [10; 12; 18, с. 1-4].

У сфері безпеки триває оформлення інституту автономних систем озброєння на стику чинних норм і нових юридичних обмежень [4; 7; 8; 18, с. 6-7].

Міжурядова координація через платформи співпраці забезпечує зближення стандартів і практик [15; 16; 18, с. 6-7].

З позиції міжнародного права важливо, що така координація не обмежується суто політичним обміном. Вона поступово створює спільну мову регулювання: ризик, життєвий цикл системи ШІ, прозорість, пояснюваність, підзвітність, оцінка впливу, аудит, людський нагляд, безпека моделі, захист даних, недискримінація та належне управління. Саме повторюваність цих категорій у документах Організації Об'єднаних Націй, Організації економічного співробітництва та розвитку, Ради Європи, Європейського Союзу, Групи семи та ЮНЕСКО свідчить про формування спільного нормативного ядра. Поки що воно не завжди має характер юридично обов'язкових норм, однак вже виконує функцію стандарту належної поведінки для держав, міжнародних організацій і приватних суб'єктів [13; 14; 15; 16; 31].

Одним із важливих у сучасних дослідженнях виступає питання можливого змісту інституту. Так, пропонується зміст інституту ШІ в міжнародному праві узагальнено може містити наступні складові елементи:

Загальносистемні принципи:

- “Парасолькові” зобов’язання щодо прав людини, демократії та верховенства права протягом життєвого циклу ШІ [14; 17; 18, с. 6].
- Етичні засади [13; 18, с. 3-4].
- Узгоджені підходи та добровільні кодекси для розробників у міжурядових форматах [15; 16; 18, с. 6-7].
- Галузеві інститути:
- Права людини і ШІ: приватність, недискримінація, право на ефективний засіб юридичного захисту; сумісність із демократичними засадами [13; 14; 18, с. 1-4; 22].
- МГП та автономні системи озброєнь, тобто міжнародне гуманітарне право та lethal autonomous weapon systems, летальні автономні системи озброєння: запобігання неконтрольованому застосуванню сили; значущий людський контроль; рух до нових юридичних обмежень [4; 7; 8; 18, с. 6-7; 20].
- Економічні режими та кіберкомпонент: експортний контроль чутливих технологій, кібербезпека, стандарти відповідності [15; 18, с. 3-4, 6-7; 21].
- Правосуб’єктність/електронна особа: дискусійна зона; фокус на відповідальності людей/організацій [10; 11; 12; 17].
- Міжурядові механізми координації.
- Керівні принципи та кодекси поведінки для розробників [16; 18, с. 6-7].
- Інструменти узгодження політики і реалізації стандартів у державах [15].
- Відкриті до приєднання рамки з потенціалом глобального поширення [14].

Доцільно також зазначити, що зміст інституту штучного інтелекту не може бути зведений лише до питань етики або технічної безпеки. У міжнародно-правовому вимірі він охоплює щонайменше три рівні регулювання. Перший рівень становлять загальні

принципи, які визначають допустимі межі використання ШІ з погляду прав людини, демократії, верховенства права та безпеки. Другий рівень становлять спеціальні галузеві режими, у межах яких ШІ застосовується у конкретних сферах, наприклад у медицині, освіті, фінансових послугах, військовій справі, кібербезпеці, морському транспорті або інтелектуальній власності. Третій рівень становлять інституційні та процедурні механізми, тобто оцінка ризиків, аудит, сертифікація, моніторинг, звітність, наглядові органи, міжнародна координація та процедури правового захисту [14; 15; 25; 26; 31].

У міжнародному праві вже склався міжгалузевий комплекс інститутів, що регулюють ШІ, який поєднує тверді договори, м'які стандарти та галузеві режими. Формальне ядро задає Рамкова конвенція Ради Європи про ШІ, права людини, демократію і верховенство права - перший у світі юридично зобов'язуючий договір у цій сфері [14].

Глобальний етичний каркас забезпечує Рекомендація ЮНЕСКО з етики ШІ (2021) [13], доповнена Принципами Організації економічного співробітництва та розвитку щодо ШІ (2019) [15] і результатами процесу Хіросіма з ШІ Групи семи (керівні принципи й добровільний кодекс для розробників) [16].

У військовій сфері формується специфічний інститут автономної зброї, lethal autonomous weapon systems, у межах міжнародного гуманітарного права: Міжнародний Комітет Червоного Хреста наполягає на юридично зобов'язуючому регулюванні та значущому людському контролі [4].

У цивільно-правовій сфері продовжує зберігатися інтеграційний підхід: питання правосуб'єктності електронної особи обговорюються як концепт, Резолюція Європейського парламенту 2017 р. - пропозиція до розгляду [10], тоді як відповідальність і підзвітність вже покладаються на людських та державних агентів, доктрина [12].

Базуючись на проведеному дослідженні автором наводиться узагальнена класифікація інститутів ШІ в МП (Таблиця 1) (Додаток 1).

Водночас наведена класифікація не є завершеною, оскільки інститут штучного інтелекту перебуває у стані формування. Його структура може змінюватися залежно від подальшого розвитку міжнародних договорів, практики держав, рішень міжнародних організацій та технологічних змін. Наприклад, у разі прийняття окремого договору щодо автономних систем озброєння відповідний блок може набути більш чітких ознак спеціального міжнародно-правового режиму. У разі розвитку глобального механізму оцінки передових моделей ШІ може сформуватися окремий процедурний інститут міжнародного нагляду за високоризиковими системами. У разі закріплення обов'язкових правил щодо транскордонної шкоди може бути конкретизовано питання міжнародної відповідальності держав за використання або неналежний контроль систем ШІ [4; 14; 24; 31].

Таким чином, можна зробити висновок про те, що як категорія, так і термін інститут штучного інтелекту (ШІ) використовується у наступному розумінні:

- по-перше, для позначення спеціальних міжнародно-правових режимів та норм, розроблених саме для регулювання ШІ, етичні принципи, договори, стандарти тощо;
- по-друге, для опису процедури адаптації існуючих інститутів міжнародного права, як-то суверенітет, права людини, відповідальність, до нових сучасних підходів та викликів, пов'язаних із ШІ. Обидва теоретичні підходи співіснують і розвиваються паралельно.

У той же час, варто підкреслити, що на практиці вже виникають прогалини, коли відсутність усталених норм змушує шукати аналогії, наприклад, чи може держава притягти до міжнародної відповідальності іншу державу за кібератаку з використанням ШІ-вірусу, питання застосування інституту міжнародної відповідальності в кіберпросторі. Наразі багато питань чітко не врегульовані, що вказує на необхідність подальшого розвитку міжнародно-правових інститутів.

1.1.2. Критичне осмислення включення штучного інтелекту (ШІ) до системи міжнародно-правових інститутів

Теоретичні підходи в науці міжнародного права різняться. Скептичний підхід у науці наголошує: міжнародне право звично запізнюється за технологічними змінами; у сфері ШІ це проявляється фрагментацією підходів і браком консенсусу щодо обов'язкових норм. У науковій фаховій літературі прямо вказується на повільність нормотворчих процедур та сіру зону застосування традиційних доктрин до нових ризиків, зокрема у *due diligence* держав у кіберпросторі [23, с. 321-323; 24, с. 790-793]. Звідси - аргумент про кризу адекватності права перед рухливою ціллю регулювання: держави обмежуються мінімальним спільним знаменником загальних принципів, обережно ставлячись до жорстких зобов'язань. У цьому ж ключі розвивається думка, що деталізований універсальний договір про ШІ наразі малоімовірний через геополітичні розбіжності [24, с. 793-796].

Скептичний підхід має під собою об'єктивні підстави. По-перше, технології штучного інтелекту розвиваються швидше, ніж міжнародні переговорні процеси. По-друге, держави мають різні політичні, безпекові та економічні інтереси у сфері ШІ. Для одних держав пріоритетом є інноваційна конкурентоспроможність, для інших - цифровий суверенітет, для третіх - військова перевага або контроль за інформаційним середовищем. По-третє, приватні технологічні компанії володіють значною частиною інфраструктури, даних, моделей і обчислювальних потужностей, що ускладнює класичну міждержавну модель регулювання. Унаслідок цього міжнародне право змушене реагувати не лише на поведінку держав, а й на транснаціональну технологічну екосистему, в якій приватні суб'єкти мають фактичну регуляторну вагу [23; 24; 29; 30].

Паралельно існує помірковано-оптимістичний науковий напрям: накопичення спільних ризиків здатне підштовхувати до поступової юридизації м'яких стандартів. Як приклад демонструють успішні рамкові компроміси в інших доменах - Паризька угода з клімату та Будапештська конвенція з кіберзлочинності, що з'явилися попри тривалі суперечки [28; 27]. На цьому тлі показовим стало ухвалення Рамкової конвенції Ради Європи про ШІ (2024) - першого обов'язкового договору в цій тематиці, що фіксує

базові гарантії прав людини та демократичного порядку у життєвому циклі штучного інтелекту (ШІ) [14]. Публічні заклики лідерів індустрії до регуляції, слухання в Сенаті США, пропозиції щодо ліцензування високопотужних моделей, також вже створюють політичне вікно можливостей для нормотворчості [29; 30].

Помірковано-оптимістичний підхід спирається на те, що міжнародне право не завжди розвивається шляхом негайного прийняття універсального договору. Часто спочатку формується спільна термінологія, далі з'являються рекомендації, декларації, принципи і модельні правила, після цього виникають регіональні або секторальні юридично обов'язкові акти, а згодом окремі положення можуть набувати ширшого міжнародного значення. Саме такий процес простежується у сфері штучного інтелекту: від етичних документів і принципів відповідального ШІ до Рамкової конвенції Ради Європи, Регламенту Європейського Союзу про штучний інтелект та резолюцій Організації Об'єднаних Націй щодо військового виміру ШІ [13; 14; 15; 50; 114].

Практично орієнтований підхід фокусується на галузевих напрямках замість великої теорії: повітряне й морське право, автономні БПЛА та судна, право інтелектуальної власності, авторство творів ШІ тощо. Як приклад - у морському секторі Міжнародна морська організація завершила регуляторний огляд для автономних надводних суден і готує не обов'язковий, а згодом - обов'язковий MASS-кодекс, що поступово впроваджує нові технічні та відповідальнісні вимоги в існуючі інструменти, зокрема SOLAS, COLREGs, MARPOL [26; 32; 33]. Всесвітня організація інтелектуальної власності (ВІПО) з 2019 р. веде WIPO Conversation про авторство/винахідництво та дані, пропонуючи інструментарій політики інтелектуальної власності на випадок зростання автономності творчих і технічних результатів ШІ [25; 34; 35]. Такий підхід мінімізує зіткнення з основами системи, адаптуючи наявні інститути через цільові оновлення.

Значення практично орієнтованого підходу полягає у тому, що він дозволяє уникнути надмірної абстрактності. У різних секторах штучний інтелект створює різні ризики. У сфері інтелектуальної власності головним є питання авторства,

винахідництва, використання даних для навчання моделей і охорони результатів, створених за допомогою ШІ. У морському праві та транспорті важливими є безпека руху, сертифікація автономних систем, розподіл відповідальності між власником, оператором, виробником і державою прапора. У військовій сфері визначальними залишаються принципи розрізнення, пропорційності, запобіжних заходів і людського контролю. Отже, один універсальний підхід не може повністю замінити секторальні режими, але може забезпечити для них спільну правову основу [25; 26; 32; 33].

Найбільш дискусійним питанням у міжнародному праві щодо інституту штучного інтелекту виступає питання щодо міжнародної відповідальності за шкоду від використання систем ШІ. Класична доктрина вимагає наявності протиправного діяння, яке можна висунути державі, але у кіберсередовищі складність встановлення зв'язку держава - дія провокує пошук моделей розширеного належного піклування (*due diligence*) та аналогій зі спеціальними режимами відповідальності. В академічних дебатах пропонують розвивати кібер-*due diligence* як стандарт превенції, спираючись на доктрину нейтралітету та практику міжгалузевих режимів; водночас підкреслюється брак зобов'язуючого консенсусу й ризики ескалації при різночитанні обов'язків третіми державами [24, с. 792-797; 36; 37; 38].

У сфері штучного інтелекту проблема *due diligence* має особливе значення. Держава може не бути безпосереднім розробником системи, але вона може дозволяти її використання, закуповувати її для публічного сектору, інтегрувати у військову інфраструктуру, експортувати відповідні технології або не запобігати використанню її території для шкідливих операцій. У таких випадках виникає питання про мінімальний стандарт належної поведінки держави. Йдеться не лише про обов'язок не порушувати міжнародне право власними діями, а й про обов'язок запобігати передбачуваній шкоді, здійснювати нагляд, перевіряти високоризикові системи, забезпечувати прозорість процедур та реагувати на відомі ризики. Саме в цьому аспекті інститут штучного інтелекту зближується з кіберправом і режимами транскордонної шкоди [24; 36; 37].

Для високоризикових технологій у науці наводиться і космічна аналогія - режим абсолютної відповідальності держави за шкоду, завдану космічними об'єктами, Конвенція 1972 р., як орієнтир для майбутніх конструкцій у III-секторах з транскордонною шкодою [39; 40; 41].

Однак механічне перенесення космічної моделі на штучний інтелект є проблемним. Космічний об'єкт має відносно визначений статус, державу запуску, реєстрацію та фізичну траєкторію. Натомість система III може створюватися у кількох юрисдикціях, навчатися на даних із різних держав, розгортатися через хмарну інфраструктуру, використовуватися приватним суб'єктом і спричиняти шкоду одночасно в багатьох правопорядках. Тому аналогія з космічним правом корисна не як готова модель, а як методологічний орієнтир для формування спеціальних режимів відповідальності за високоризикові технології [39; 40; 41].

Паралельно лунають застереження щодо *ethics washing* - підміни реальної підзвітності декларативними етичними кодексами компаній або міжурядових ініціатив, що знижує стимул до обов'язкових норм і ефективного правозастосування [42; 43; 44]. Щоб уникнути фрагментації та дефектів саморегулювання, міжнародні організації нарощують інституційну спроможність: від процесів Групи семи, Організації економічного співробітництва та розвитку, ЮНЕСКО до створення в системі Організації Об'єднаних Націй дорадчого механізму з III та підготовки глобальних політичних орієнтирів, зокрема *Global Digital Compact* [16; 15; 13; 31]. У підсумку зазначимо, що формується поступова траєкторія визнання проблематики (рис. 1) (Додаток 2) від накопичення норм *soft law* до секторальної юридизації й появи міжгалузевого інституту, що працює через поєднання рамкових принципів і галузевих кодексів [14; 26; 25].

Критичне осмислення включення штучного інтелекту до системи міжнародно-правових інститутів, таким чином, не зводиться до питання про те, потрібен чи не потрібен окремий універсальний договір. Воно охоплює ширше коло питань: чи достатньо чинних принципів міжнародного права для регулювання автономних рішень;

чи здатні м'які стандарти перетворитися на юридично значущу практику; яким має бути співвідношення державного і приватного контролю; яким чином встановлювати відповідальність за шкоду, спричинену складними алгоритмічними системами; чи можливий єдиний підхід для цивільного і військового використання ШІ. Саме ці питання визначають подальший розвиток інституту штучного інтелекту в міжнародному праві.

1.1.3. Становлення розвитку інституту штучного інтелекту (ШІ) в міжнародному праві

Початок міжнародно-правової інституалізації ШІ пов'язують не з єдиним актом, а з послідовністю подій, які і розпочали дискусію - від академічних декларацій до політичних рішень.

Перший імпульс задав експертний консенсус першого міжнародного акту з тематики штучного інтелекту - Принципів Азіломар (2017): їх напрацювали учасники конференції Beneficial AI 2017 під егідою Future of Life Institute. Цей початковий документ містить 23 принципи, згруповані у трьох кластерах:

- Research Issues, ціль досліджень, зв'язок наука - політика, культура співпраці, уникнення гонки безпеки,
- Ethics & Values, безпека, прозорість і можливість аудиту, відповідальність розробників, вирівнювання цінностей, повага до гідності та прав, приватність, спільна вигода і спільний добробут, людський контроль, недопущення підриву демократичних процесів, уникнення гонки озброєнь у ЛАСО, тобто летальних автономних системах озброєння,
- Longer-term Issues, обережність щодо верхніх меж здібностей, планування під екзистенційні ризики, контроль над самовдосконаленням, спрямованість суперінтелекту на спільне благо [45].

Саме ця етична матриця стала містком між академічною спільнотою та урядами: значна частина дослідників і лідерів індустрії публічно приєдналась до принципів, що легітимувало перехід до міжурядових стандартів [45].

На цій хвилі Організація економічного співробітництва та розвитку у травні 2019 р. на рівні Ради міністрів ухвалила Рекомендацію щодо ШІ (OECD AI Principles) - перший міжурядовий стандарт довірчого, людиноцентричного ШІ [15, с. 2-3].

Документ має дві опори:

(1) п'ять ціннісних принципів для всіх акторів ШІ - інклюзивне зростання та добробут; людські цінності й справедливість; прозорість і пояснюваність; надійність/безпека; підзвітність [15, с. 3];

(2) п'ять рекомендацій урядам - інвестиції в R&D; цифрова екосистема для ШІ; сприятливе регуляторне середовище; розвиток людського капіталу і справедливий перехід на ринку праці; міжнародна кооперація [15, с. 2-3].

Розроблення Рекомендацій забезпечила AI Group of Experts at the OECD (AIGO) - понад 50 мультидисциплінарних експертів, уряди, індустрія, академія, громадські організації, профспілки, які у 2018-2019 рр. провели серію засідань, Париж, МІТ, Дубай, і підготували проєкт принципів для CDEP, Комітету з цифрової економічної політики [15, с. 3-4]. Рекомендація відкрита для приєднання не-членів Організації економічного співробітництва та розвитку, передбачає подальші метрики, огляд імплементації та розвиток інструментів через OECD.AI [15, с. 4-5].

У травні 2024 р. принципи оновлено, аби врахувати нові технологічні й політичні реалії, зберігаючи їх гнучкість та міжюрисдикційну сумісність [15]. Станом на сьогодні 47 юрисдикцій офіційно дотримуються Принципів Організації економічного співробітництва та розвитку: усі держави-члени ОЕСР, від Австралії, Канади, Японії та Кореї до країн ЄС, Великої Британії, Туреччини, Ізраїлю, Чилі, Колумбії, Коста-Рики, Мексики, Нової Зеландії, та не-члени - Аргентина, Бразилія, Єгипет, Мальта, Перу, Румунія, Сінгапур, Україна [15, с. 10-11; 15];

у G20 ці засади закріплені як G20 AI Principles, прямо виведені з документа Організації економічного співробітництва та розвитку, їх підтримали всі члени G20, включно з Китаєм, Індією, Індонезією, росією, Саудівською Аравією та ПАР [15].

Значення Принципів Організації економічного співробітництва та розвитку полягає в тому, що вони створили перший міжурядовий нормативний каркас, який був прийнятний для різних правових систем. Їхня сила полягає не в обов'язковості, а в тому, що вони стали базою для подальших національних стратегій, політик і міжнародних документів. Саме через такі принципи формується попередня стадія міжнародно-правового інституту: спочатку держави погоджуються щодо мови, критеріїв і базових цінностей, після цього ці положення переходять до регіонального права, технічних стандартів, національного законодавства та практики міжнародних організацій [15; 16; 18].

Другим прискорювачем виступила інституціоналізація співпраці через GPAI, Global Partnership on Artificial Intelligence, тобто Глобальне партнерство зі штучного інтелекту. Ідея Партнерства виникла на ґрунті франко-канадської ініціативи після саміту Групи семи (2018), а офіційний запуск відбувся 15 червня 2020 р. за участі 15 держав-засновниць, Австралія, Канада, Франція, Німеччина, Індія, Італія, Японія, Мексика, Нова Зеландія, Республіка Корея, Сінгапур, Словенія, Іспанія, Сполучене Королівство, США, та ЄС; адміністративну опору від старту забезпечив секретаріат в екосистемі Організації економічного співробітництва та розвитку [46; 53; 52]. Організаційна модель одразу будувалась як міжурядова та мультистейкхолдерна: Рада/Керівний комітет від країн-учасниць та експертні робочі групи, Responsible AI; Data Governance; Future of Work; Innovation & Commercialization; згодом - тематичні місії AI & Pandemic Response, AI & Climate [46; 55; 56]. Для операційної підтримки створено центри експертної спроможності у Парижі (Франція) та Монреалі (Канада), пізніше - в Токіо (Японія), що координують дослідження, пілоти і методики для урядів [52].

У 2023 р. Індія, як Голова, задала курс на зближення з інструментами Організації економічного співробітництва та розвитку; у липні 2024 р. оголошено інтегроване партнерство GPAI-OECD, покликане уникати дублювань і консолідувати імплементацію спільних принципів [47; 51; 54]. Це дало стабільніший бюджет, ясніший

мандат і прозорішу координацію політик, брак яких раніше гальмував перехід від декларацій до режимного врядування [46; 47].

Від стартових 15 учасників Партнерство зросло до 44 юрисдикцій, стан на 2024/25, серед яких Аргентина, Австралія, Бразилія, Канада, країни ЄС, Індія, Ізраїль, Японія, Мексика, Нова Зеландія, Польща, Республіка Корея, Сенегал, Сербія, Сінгапур, Словенія, Іспанія, Швеція, Туреччина, Сполучене Королівство, США, а також Європейський Союз; офіційно фіксується, що це collaborative global initiative of 44 member countries [52]. Розміщення центрів у Парижі та Монреалі було політично підтримане Францією і Канадою на старті, що забезпечило баланс між європейськими та північноамериканськими школами; пізніше доєднався азійський вузол у Токіо [53; 52].

GPAI приземляє і спрямовує етичні принципи у державну політику через практичні керівництва й пілотні проекти. Наприклад, Data Governance WG Report 2023 деталізує моделі доступу та обміну даними, інституційні ролі, публічні трасти даних, правові підстави, запобігання дискримінації, що виступає основою для дорожніх карт урядів [55]. Responsible AI WG напрацьовує кейси алгоритмічної прозорості в публічному секторі та інструменти оцінювання, audit/assessment, підзвітності й пояснюваності [56]. Через інтеграцію з OECD.AI, Політична обсерваторія, ці матеріали поєднуються з Принципами Організації економічного співробітництва та розвитку щодо ШІ та картою національних політик, спрощуючи імплементацію та взаємне навчання [52; 15]. На міжурядовому рівні робота GPAI доповнює Hiroshima AI Process, Керівні принципи й Кодекс для розробників, і Рамкову конвенцію Ради Європи про ШІ, формуючи цілісну екосистему - від етики до права [16; 14; 52].

На нашу думку варто підкреслити один аспект - чому інтеграція з Організацією економічного співробітництва та розвитку стала такою важливою критичною. Це пояснюється наступним: ранні аналітики відзначали дефіцит інституційної визначеності: паралельні платформи, невизначений бюджет, ризик дублювання мереж [46]. Рішення 2024 року - GPAI and OECD unite - зафіксувало спільну архітектуру:

єдиний бренд GPAI, опору на аналітичні ресурси Організації економічного співробітництва та розвитку, збереження мультистейкхолдерних робочих груп і продовження роботи центрів у Парижі, Монреалі та Токіо [51; 52]. Це зняло структурні бар'єри, пришвидшує вироблення застосовних стандартів, керування даними, оцінка ризиків, прозорість, аудит, і відкриває ширший доступ країнам, що не є членами Організації економічного співробітництва та розвитку, але дотримуються Принципів Організації економічного співробітництва та розвитку щодо ШІ [52; 15].

Третім прискорювачем стала поява жорсткіших рамок у відповідь на суспільні ризики, що вибухово постали після прориву генеративних моделей ШІ у 2022-2023 роках. На тлі суспільного резонансу провідні керівники індустрії публічно закликали до наднаціонального регулятора та моделі Міжнародного агентства з атомної енергії для ШІ; цю ідею підтримав Генеральний секретар Організації Об'єднаних Націй, прямо схваливши створення міжнародного наглядового органу для ШІ [29; 48].

У політичній площині Група семи запустила Hiroshima AI Process (2023) із двома ключовими складовими: міжнародними керівними принципами та Міжнародним кодексом поведінки для організацій, що розробляють передові системи ШІ, ризик-орієнтований підхід, безпека/надійність, прозорість, підзвітність, управління ланцюгом поставок, протидія зловживанням [16; 20].

Від цієї попередньої рамкової домовленості перейшли до урядово-приватної співпраці на форумі безпеки: 1-2 листопада 2023 р. Велика Британія провела AI Safety Summit в Блетчлі-Парк, де 28 держав і ЄС, серед них США, Велика Британія, ЄС, Китай, Канада, Японія, Республіка Корея, Італія, Франція, Індія, Бразилія, Сінгапур тощо, підписали Блетчлійську декларацію, інша назва - Декларація Блетчлі. Декларація зафіксувала спільне розуміння ризиків frontier AI, зобов'язання оцінювати модельні ризики до і після розгортання, посилювати інформаційний обмін між урядами та розробниками, а також домовленість продовжити процес у 2024-2025 рр. в Республіці Корея та Франції. Паралельно країни заснували/посилили інститути безпеки ШІ, напр., UK AI Safety Institute; синхронно США оголосили створення NIST AI Safety Institute,

відкривши канал взаємодії між національними інспекційними/тестовими структурами [50].

Наступним кроком у розвитку став AI Seoul Summit 2024, Республіка Корея, травень 2024, де уряди, компанії та науковці ухвалили три пакети документів: Seoul Declaration, Frontier AI Safety Commitments, добровільні зобов'язання компаній щодо ідентифікації, оцінювання й управління ризиками; тестування моделей; розкриття відомостей для нагляду; механізми запобігання зловмисним/небажаним використанням, та Seoul Ministerial Statement, узгодження державних підходів до оцінювання ризиків і обміну сигналами небезпеки. Це оформило архітектуру процесу (Рис. 2) (Додаток 3).

У межах цієї архітектури важливою стає не лише сама наявність декларацій, а й формування постійної процедури. Якщо попередні документи мали переважно принциповий характер, то процес Блетчлі - Сеул - подальші саміти формує регулярний формат взаємодії держав, компаній, науковців і технічних інститутів безпеки. У міжнародно-правовому сенсі це є ознакою інституціоналізації: з'являються повторювані зустрічі, спільні документи, робочі поняття, механізми оцінки ризику та обмін інформацією між державами і приватним сектором. Поки що цей процес не має характеру міжнародного договору, але він створює матеріальну основу для майбутніх обов'язкових стандартів [49; 50; 57].

Паралельно, в системи Організації Об'єднаних Націй було сформовано Групу високого рівня з питань ШІ (HLAB-AI), що у 2023-2024 рр. видала проміжну та фінальну доповіді з рекомендаціями: створити міжнародну наукову панель для синтезу доказів, аналог ІРСС, забезпечити глобальний доступ до обчислювальних ресурсів і даних для країн Глобального Півдня, виробити координаційні механізми між агенціями Організації Об'єднаних Націй і державами, а також інтегрувати ці напрацювання до Global Digital Compact. Ці пропозиції покликані зшити воєдино урядові ініціативи, Група семи/Блетчлі/Сеул, із загальносвітньою інституційною опорою Організації Об'єднаних Націй [31].

Участь Організації Об'єднаних Націй має принципове значення, оскільки саме універсальний рівень дозволяє уникнути повної регіоналізації регулювання ІІІ. Європейський Союз, Рада Європи, Організація економічного співробітництва та розвитку і Група семи формують сильні нормативні стандарти, однак вони не охоплюють усю міжнародну спільноту. Для держав Глобального Півдня питання ІІІ пов'язане не лише з безпекою, а й з доступом до даних, обчислювальних ресурсів, цифрової інфраструктури та справедливого розподілу переваг технологічного розвитку. Тому рекомендації Групи високого рівня з питань ІІІ мають значення не тільки для безпеки, а й для подолання цифрової нерівності та формування більш інклюзивної архітектури глобального врядування [31; 102; 103].

Четвертим прискорювачем процесів став перехід до юридично зобов'язуючих режимів. Європейський Союз у 2024 р. ухвалив AI Act - перший комплексний регламент ризик-орієнтованого регулювання ІІІ з екстериторіальним ефектом, який поширюється на постачальників і користувачів систем, що виходять на ринок ЄС. Регламент вводить багаторівневу модель: заборонені практики; високоризикові системи з обов'язковими вимогами; обмежений ризик із вимогами прозорості; та мінімальний ризик без спеціальних зобов'язань [51]. Заборони охоплюють, зокрема, маніпулятивні/підсвідомі техніки, експлуатацію уразливостей, соціальне скорингування, прогностичні кримінальні ризики на основі профілювання, нетаргетований скрейпінг зображень для баз облич, емоційне розпізнавання у праці та освіті, а також декілька видів біометричної категоризації [51].

Для високоризикових систем обов'язковими стають управління ризиками, якість даних, документація, технічні досьє, кібербезпека, людський нагляд, логування, оцінка відповідності, реєстрація у відповідній базі та виконання вимог прозорості. Окремо регламент встановлює вимоги до моделей загального призначення та моделей із системним ризиком, що має значення для генеративного ІІІ та великих моделей, здатних впливати на значну кількість користувачів і секторів [51].

AI Act не є актом міжнародного права у вузькому сенсі, однак його значення для міжнародно-правового регулювання є суттєвим. Через екстериторіальний ефект він впливає на постачальників систем ШІ поза межами Європейського Союзу, якщо їхні продукти або послуги використовуються на ринку ЄС. У цьому проявляється нормативна сила європейського ринку, яка може сприяти поступовій гармонізації стандартів у ширшому міжнародному масштабі. Подібно до того, як Загальний регламент про захист даних вплинув на глобальні стандарти приватності, AI Act потенційно може стати орієнтиром для національних і регіональних моделей регулювання ШІ [50; 51].

На рівні міжнародного права статус першого договору дістав Рамковий конвент Ради Європи про ШІ, права людини, демократію і верховенство права. Текст відкрито до підписання 5 вересня 2024 р.; він обов'язковий і відкритий для приєднання держав поза Радою Європи [14]. Конвент фіксує мету і предмет: забезпечити, щоб діяльність протягом усього життєвого циклу систем ШІ була сумісна з правами людини, демократією і верховенством права; встановлює градуїзовані й диференційовані заходи відповідно до тяжкості/ймовірності впливів; охоплює публічних суб'єктів та приватних, що діють від їхнього імені, а для решти приватних - вимагає визначити національну модель імплементації [14].

Передбачено принципи прозорості й нагляду, підзвітності, рівності й недискримінації, приватності і захисту даних, надійності, а також рамку управління ризиками та впливами, ідентифікація, оцінка, запобігання/пом'якшення, моніторинг, документація, тестування до першого використання та при значних змінах. На державах-учасниках лежить обов'язок забезпечити засоби правового захисту і процесуальні гарантії, включно з доступом до релевантної інформації про системи, що істотно впливають на права людини. Для імплементації й тлумачення засновано Конференцію Сторін і механізм подання звітів; передбачено можливість ухвалення додаткових інструментів та оцінку мораторіїв чи заборон на несумісні застосування

[14]. У наданих матеріалах ця траєкторія чітко подана як поступ від soft law до обов'язкових норм та інституціоналізації контролю [18, с. 1-2; 18, с. 3-4; 18, с. 6-7].

Рамкова конвенція Ради Європи є особливо важливою для розуміння саме міжнародно-правового інституту штучного інтелекту. Вона не встановлює вичерпного технічного регулювання всіх систем ШІ, але формує правову рамку, яка пов'язує ШІ з правами людини, демократією та верховенством права. Такий підхід підтверджує, що інститут штучного інтелекту у міжнародному праві не може бути суто технологічним або безпековим. Його нормативне ядро становлять права людини, процедурні гарантії, підзвітність держави та вимога сумісності технологічного розвитку з базовими принципами міжнародного публічного права [14; 18].

Історія становлення має й внутрішню динаміку підтримки (Таблиця 2) (Додаток 4). На ранніх етапах важливу роль зіграли академічні авторитети й міждисциплінарні мережі, учасники азіломарського процесу, IEEE та університетські центри етики ШІ, які переводили етичні імперативи у політичні меседжі [45]. Далі ініціативу підхопили міжурядові платформи, Організація економічного співробітництва та розвитку, Група семи, де консенсус будувався навколо цінностей безпечності, підзвітності та прав людини [15; 16]. Рубіконом стали європейські рішення, AI Act, Конвенція Ради Європи, що юридично кристалізували принципи і створили де-факто глобальні стандарти через ефект ринкової тяглості [51; 14]. На рівні Організації Об'єднаних Націй триває збірка парасолькової глобальної архітектури: діалог щодо можливих інституцій, від координаційного органу до автономної агенції, подібної до Міжнародного агентства з атомної енергії, і механізмів наукової експертизи та солідарності, фонди доступу до потужностей, наукова панель [31; 48]. Узгоджено, що без інклюзивної участі країн, які не контролюють обчислювальні ресурси й моделі, рівності правил не буде [31].

У підсумку вимальовується поступова інституціоналізація: від етичних принципів і добровільних кодексів - до правозобов'язуючих рамок і постійних майданчиків співпраці. У базовій роботі це зафіксовано як міжгалузеве становлення інститутів ШІ із ядром прав людини, процедурних гарантій, вимог прозорості та

контролю, що вже працює у правозастосуванні й переходить до стадії конвенційних та регламентаційних механізмів [17; 18, с. 1-2; 18, с. 6-7].

1.2. Штучний інтелект як технологія подвійного використання: міжнародно-правові аспекти

Початкові роботи, які заклали цивільно-правовий напрямок розвитку ШІ, зокрема проект підтримки рішень MYCIN, Стенфорд, старт - 1972 р., продемонстрували, що алгоритмічні системи здатні обробляти дані й видавати рекомендації, сумірні з експертним рівнем. Саме з цього кола expert systems розпочалось поширення технологій ШІ на перші практики у медицині та фінансових послугах, де автоматизація аналізу поєдналася з вимогою пояснюваності результатів [58].

Вказаний етап має принципове значення для розуміння подальшого міжнародно-правового розвитку ШІ. Спочатку штучний інтелект розглядався переважно як інструмент підтримки професійного рішення, тобто як допоміжна технологія, що не замінює людину повністю, але посилює її здатність до аналізу. Водночас саме на цьому рівні виникло перше ключове правове питання: чи може особа, на яку впливає алгоритмічна рекомендація, зрозуміти логіку такого рішення, перевірити його обґрунтованість і оскаржити наслідки його застосування. Тому вже ранні цивільні системи ШІ поставили питання не лише ефективності, а й прозорості, пояснюваності та відповідальності.

Військовий вектор технічно спирався на старіші "запрограмовані" засоби, але якісно нову планку автономності задала ізраїльська IAI Harpy: у 1980-х її створювали як засіб виявлення і ураження РЛС-цілей за сигнатурами, а в 1990-х вивели на ринок як "барражуючий боєприпас" типу fire-and-forget. Від цього моменту автономний пошук/ураження цілі перестав бути лише лабораторним експериментом і став "стабільною лінійкою продукції" [59; 60]. Протягом наступних десятиліть рішення цієї ніші масштабували США, Республіка Корея, Індія, Туреччина, Китай та інші

виробники, що прискорило гонку автономних функцій ураження і поставило на порядок денний питання про межі допустимості такої автономності [59; 63].

У військовому вимірі автономність має іншу правову якість, ніж у цивільній сфері. Якщо у медицині, фінансах або транспорті алгоритмічна помилка зазвичай розглядається через категорії шкоди, відповідальності, недискримінації та процесуального захисту, то у сфері збройного конфлікту вона безпосередньо пов'язана із застосуванням сили, ураженням цілі, ризиком загибелі цивільних осіб і дотриманням принципів міжнародного гуманітарного права. Саме тому одна й та сама технологічна основа може мати різний правовий режим залежно від сфери застосування. Комп'ютерний зір, автономна навігація, розпізнавання об'єктів, алгоритмічна класифікація і прогнозування у цивільному середовищі можуть використовуватися для діагностики, логістики або безпечного транспорту, а у військовому середовищі - для розвідки, наведення, вибору цілі та прискорення циклу ураження.

Паралельно формувалася правова позиція на національному рівні: у США оновлено DoD Directive 3000.09 (25.01.2023), яка окреслює політику щодо автономних/напіваавтономних функцій у зброї, встановлює вимоги безпеки, процедури прийняття рішень і перевірок, щоб мінімізувати ризик ненавмисного ураження та зберігати контроль людини над критичними функціями [61]. Такі національні рамки фактично виконують роль "еталона" для союзників і партнерів, перетікаючи у багатосторонні переговорні процеси.

У цьому контексті національні підходи набувають міжнародно-правового значення не тому, що самі по собі створюють універсальні зобов'язання, а тому, що вони формують практику держав щодо допустимих меж автономності. У сфері нових військових технологій практика держав має особливу вагу, оскільки саме вона демонструє, як держави тлумачать свої обов'язки за міжнародним гуманітарним правом, як вони проводять правові огляди нової зброї, які параметри людського контролю визнають достатніми, які технічні запобіжники закладають у системи і яку

роль відводять командиру, оператору, розробнику та державному органу, що ухвалює рішення про прийняття системи на озброєння.

Технологічна "спільна основа" ІІІ - комп'ютерний зір, навігація, планування, робота з великими даними, великі мовні моделі - робить системи ІІІ системами подвійного призначення: модулі, що підвищують точність діагностики чи керують автономним транспортом, у військовій сфері оптимізують наведення, розвідку та ураження. Це породжує регуляторну асиметрію: у цивільній площині домінують стандарти прав людини, приватність, недискримінація, процесуальні гарантії, і вимоги прозорості/підзвітності [13; 14; 51; 18, с. 3-4], тоді як у військовій - імперативи міжнародного гуманітарного права щодо розрізнення, пропорційності і заборони зайвих страждань, із посиленням контролем автономних функцій у критичних фазах ураження [18, с. 6-7].

Саме подвійне використання є центральною проблемою правового режиму ІІІ. На відміну від класичних видів озброєнь, які часто мають чітко визначене військове призначення, значна частина ІІІ-інструментів створюється у цивільному секторі, фінансується приватними компаніями, навчається на відкритих або комерційних даних і лише згодом інтегрується у військові процеси. Це стосується систем розпізнавання зображень, автоматичної обробки мови, прогностичної аналітики, навігаційних модулів, систем кіберзахисту, обробки супутникових знімків, управління логістикою та моделювання сценаріїв. Тому міжнародне право стикається з об'єктом, який не можна повністю врегулювати ні як цивільну технологію, ні як військовий засіб.

У цивільному векторі міжнародно-правове реагування спирається на три взаємопов'язані методи.

По-перше, інтеграцію прав людини: до алгоритмічних практик застосовуються вимоги законності/необхідності/пропорційності щодо обробки даних, заборона дискримінації, гарантії ефективного засобу правового захисту, що вже віддзеркалено в європейській регуляції ризик-орієнтованого типу [51; 14; 18, с. 3-4].

По-друге, м'які стандарти рівня ЮНЕСКО, тобто Організації Об'єднаних Націй з питань освіти, науки і культури, та ОЕСР, тобто Організації економічного співробітництва та розвитку, формують людиноцентричні орієнтири - прозорість, підзвітність, керованість ризиками, які держави імплементують у національні політики та практику [13; 15].

По-третє, інструменти оцінювання впливу та технічні норми, AI/algorithmic impact assessments, аудит, логування, вимоги до якості даних і надійності, з'єднують soft law з обов'язковими режимами та міждержавною стандартизацією [15; 51; 18, с. 6-7].

У межах цивільного регулювання важливо, що міжнародні стандарти поступово переходять від загального проголошення принципів до процедурної конкретизації. Недостатньо лише задекларувати прозорість або недискримінацію. Необхідно встановити, хто саме проводить оцінку ризику, які дані використовуються для навчання моделі, чи можна перевірити логіку результату, чи ведеться журналювання дій системи, чи має особа доступ до людського перегляду рішення, чи передбачено ефективний засіб юридичного захисту. Саме на цьому рівні цивільний ІІІ стає предметом не тільки етичної дискусії, а й юридично перевірюваного регулювання.

У військовому векторі розвитку ІІІ базою слугує чинне міжнародне гуманітарне право: принципи розрізнення, пропорційності та заборони зайвих страждань застосовні до будь-яких засобів ведення війни, а ст. 36 ДП І, тобто Додаткового протоколу І до Женевських конвенцій, вимагає від держав проводити правову експертизу кожного нового виду зброї - включно з автономними функціями, сценаріями застосування і параметрами "людського контролю" [62]. Дискусії у форматі K333/CCW, тобто Конвенції про заборону або обмеження застосування конкретних видів звичайної зброї / Convention on Certain Conventional Weapons, Групи урядових експертів з ЛАСО, тобто летальних автономних систем озброєння, зосереджені на виробленні спільних визначень автономності, параметрів "значущого людського контролю", а також на виборі моделі правотворення - від політичних декларацій до спеціального протоколу

чи окремого договору [59; 4]. До появи "жорстких" норм діють рамки безпеки "передових ШІ": Hiroshima AI Process, принципи й кодекс для розробників, Блетчлійська декларація, 28 держав; оцінювання ризиків і доступ урядів до тестування моделей, AI Seoul Summit, зобов'язання компаній щодо ідентифікації, оцінки та управління ризиками - механізм швидкої конвергенції практик, що зшиває урядові й промислові підходи [16; 50; 57].

Правова експертиза нової зброї має особливе значення саме для автономних і напіваавтономних систем. У класичних видах зброї перевірка часто зосереджується на фізичних характеристиках засобу, способі ураження, передбачуваних наслідках і сумісності із заборонами міжнародного гуманітарного права. У випадку ШІ-систем оцінка має включати також якість даних, надійність алгоритму, передбачуваність поведінки в різних середовищах, стійкість до перешкод, можливість людського втручання, умови втрати зв'язку, обмеження цільових профілів і здатність системи функціонувати без порушення принципів розрізнення та пропорційності. Тому ст. 36 ДП І у цьому контексті перетворюється на ключовий правовий міст між класичним міжнародним гуманітарним правом і сучасною технологічною практикою.

Суміжність цивільного і військового векторів дедалі частіше врегульовується комбінацією рамкових конвенцій і політичних процесів: у цивільному полі працює відкритий до приєднання "договірний каркас" із вимогами по всьому життєвому циклу систем, у військовому - нарощуються параметри допустимої автономності, експертиз і прозорості, що зрештою сприяє уніфікації мінімальних стандартів безпеки та підзвітності [14; 16; 50; 57; 18, с. 1-2; 18, с. 6-7].

Сучасні цивільні застосування ШІ охоплюють охорону здоров'я, транспорт, енергетику, освіту, фінансові послуги, державне управління та креативні індустрії; у кожній із цих сфер алгоритми виконують класифікацію, прогнозування, персоналізацію та автоматизовану підтримку рішень, що безпосередньо впливають на становище людини в економічних і соціальних відносинах [18, с. 3-4]. Разом із вигодами виникають системні ризики: вторгнення в приватність через масиви даних,

непрозорість логіки моделей, відтворення або посилення упереджень, обмеження доступу до базових послуг за рахунок автоматизованого скорингу. У відповідь склалася доктрина захисту прав у цифровому середовищі: вона переносить дію чинних міжнародних стандартів прав людини на алгоритмічні процеси і кодифікує "цифрові права людини" як операційний блок гарантій - приватність онлайн, заборона дискримінації, свобода вираження у мережі, право не підлягати виключно автоматизованому рішенню без належного людського перегляду, право на пояснення та ефективний засіб юридичного захисту [18, с. 3-4].

Матеріальне ядро доктрини зобов'язує суб'єктів уникати дискримінаційних ефектів даних і моделей, мінімізувати ідентифікаційні та репутаційні ризики, гарантувати безпеку й надійність систем у всьому життєвому циклі [13; 15].

Процесуальна складова вимагає прозорості та підзвітності: користувач і особа, на яку впливає система, мають отримувати релевантну інформацію про використання ШІ, зрозумілі пояснення значущих рішень, можливість швидкого оскарження з доступом до документації, журналів подій і результатів оцінок впливу [13; 14].

До цього додається горизонтальна дія прав у відносинах "людина - платформа - постачальник ШІ" та позитивні обов'язки держави: не лише утримуватися від порушень, а й створювати регуляторні та інституційні запобіжники з належним наглядом і дієвими засобами правового захисту [14; 18, с. 3-4].

Правова конструкція регулювання ШІ вибудовується пошарово. На рівні ціннісних орієнтирів Рекомендація ЮНЕСКО з етики ШІ закріплює людиноцентричність, запобігання масовому стеженню та соціальному скорингу, вимоги прозорості, підзвітності, рівності та інклюзії; документ адресований усім акторам і задає мінімальний етичний знаменник для державних політик [13].

Принципи ОЕСР щодо ШІ поєднують п'ять ціннісних засад, інклюзивне зростання, права людини та справедливість, прозорість/пояснюваність, надійність/безпека, підзвітність, із п'ятьма урядовими напрямками, інвестиції в R&D,

цифрова екосистема, "розумне" регулювання, людський капітал, міжнародна кооперація, створюючи місток від етики до політик і процедур [15].

Далі діє рівень обов'язкових вимог. AI Act ЄС вводить ризик-орієнтовану модель: заборонені практики, зокрема маніпулятивні техніки, експлуатація вразливостей, соціальний скоринг, жорсткі вимоги до високоризикових систем, управління ризиками, якість наборів даних, технічна документація, журналювання, кібербезпека, людський нагляд, оцінка відповідності та реєстрація, окремі обов'язки для моделей загального призначення та моделей із системним ризиком [51].

У площині міжнародного публічного права Рамкова конвенція Ради Європи про ШІ фіксує мінімальні гарантії прав людини, демократії та верховенства права для всієї діяльності із ШІ у публічному секторі й для приватних суб'єктів, що діють від імені влади, вимагає процедур управління ризиками та ефективних засобів правового захисту, і створює інституційні механізми тлумачення та моніторингу виконання [14].

Фактично, можна сказати, що "практика імплементації трансформує доктрину в операційні обов'язки". Провайдери й користувачі систем впроваджують AI/algorithmic impact assessments на етапах проєктування і впровадження, проводять незалежні аудити надійності та недискримінації, документують джерела даних і версії моделей, забезпечують журналювання та можливість реконструкції ланцюга причинно-наслідкових подій, встановлюють механізми скарг і оперативного виправлення помилок, повідомляють наглядові органи про серйозні інциденти [51; 14; 18, с. 6-7]. У публічних сервісах пріоритетним стає "людський контроль" над критичними рішеннями: забороняються або обмежуються практики суто автоматизованих відмов у доступі до базових послуг, кредитування, працевлаштування, соціальної підтримки без можливості швидкого людського перегляду [51; 14]. Для зниження системної упередженості поширюються вимоги до якості даних, репрезентативність, точність, відсутність дискримінаційних маркерів, тестування на справедливість і запровадження коригувальних механізмів "за дизайном" [15; 51].

Окремим принциповим питанням постає суміжність цифрових прав із іншими режимами: захист персональних даних і конфіденційності обробки, споживчі стандарти безпеки, трудові гарантії при використанні ІІІ у відборі та оцінюванні праці, права дитини в онлайн-середовищі, доступність сервісів для людей з інвалідністю. Ці складові елементи посилюють позитивні обов'язки держави й формують мультисекторальні нагляди, що координуються з принципами ЮНЕСКО та ОЕСР і юридичними рамками Ради Європи та ЄС [13; 15; 14; 51]. У актах цих організацій підкреслено, що цей перехід від декларацій до процедурної "архітектури відповідальності" вже відбувся: застосування прав людини до алгоритмічних рішень, впровадження оцінок впливу, аудитів і людського перегляду фіксується як новий стандарт правозастосування у цивільному обороті ІІІ [18, с. 3-4; 18, с. 6-7].

У цьому аспекті цивільне регулювання ІІІ не можна розглядати лише як внутрішньодержавну політику. Воно має міжнародно-правовий вимір, оскільки цифрові сервіси, хмарні обчислення, платформи, дані та моделі функціонують транскордонно. Алгоритмічне рішення, прийняте або підготовлене в одній юрисдикції, може впливати на особу в іншій юрисдикції, а постачальник системи, її користувач і суб'єкт даних можуть перебувати у різних державах. Тому питання юрисдикції, застосовного права, міжнародної співпраці наглядових органів і взаємного визнання стандартів набувають особливого значення. У цьому проявляється ще одна ознака подвійного використання: одна й та сама технологія не лише поєднує цивільну і військову функції, а й перетинає внутрішнє, регіональне та міжнародне право.

Загальна логіка цивільного регулювання полягає в поєднанні трьох шарів: етичні принципи як базовий консенсус [13; 15], обов'язкові рамки, що задають "червоні лінії" і вимоги до високого ризику [51; 14], та процесуальні інструменти, які роблять права перевірюваними - від оцінок впливу і аудитів до механізмів оскарження й інституційного нагляду [51; 14; 18, с. 6-7]. Така багаторівнева конструкція вирівнює інновації з правами і створює передумови для взаємного визнання підходів між юрисдикціями без втрати захисту людини як кінцевої мети цифрової трансформації.

Поки універсального договору про цивільні аспекти ІІІ не існує, головну роль відіграють "м'які" інструменти, які задають орієнтири для національних законів і практик. Рада Європи першою на міжурядовому рівні звернула увагу на небезпеку маніпулятивних алгоритмів: Декларація КМ РЄ від 13.02.2019 попередила про ризики впливу на політичну та соціальну поведінку та окреслила рамку протидії таким практикам [64]. У 2020 р. КМ РЄ ухвалив Рекомендацію СМ/Rec(2020)1 щодо впливу алгоритмічних систем на права людини - із вимогою до держав переглянути національне регулювання, вбудувати оцінювання ризиків, прозорість і підзвітність по всьому життєвому циклу систем [65].

"Глобальний етичний консенсус" зафіксовано в Рекомендації ЮНЕСКО з етики ІІІ (2021), яка закріплює людиноцентричність, заборону масового стеження та соціального рейтингування, принципи прозорості й підзвітності для всіх акторів [13], а Принципи ОЕСР щодо ІІІ (2019) конкретизують цінності інклюзивності, безпеки, пояснюваності та відповідальності й дають урядам "дорожню карту" імплементації [15].

На рівні обов'язкових вимог ризик-орієнтований підхід materialізовано в AI Act ЄС: заборонені практики, жорсткі вимоги до високоризикових систем, управління ризиками, якість даних, технічна документація, логування, людський нагляд, оцінка відповідності, реєстрація, окремі обов'язки для моделей загального призначення та моделей із системним ризиком [51].

У площині міжнародного публічного права Рамкова конвенція РЄ про ІІІ закріплює мінімальні гарантії прав людини, демократії та верховенства права для всієї діяльності із ІІІ у публічному секторі та для приватних суб'єктів, що діють "від імені" влади, вимагаючи процедур управління ризиками та ефективних засобів правового захисту [14]. Змістовним наповненням цих рамок стає доктрина захисту прав у цифровому середовищі: перенесення чинних міжнародних зобов'язань на алгоритмічні процеси; операційний блок "цифрових прав людини", приватність онлайн, заборона дискримінації, право не підлягати суто автоматизованому рішення без належного

людського контролю, право на пояснення та ефективний засіб захисту; позитивні обов'язки держави щодо запобігання порушенням із боку приватних акторів; процесуалізація захисту через AI/algorithmic impact assessments, незалежні аудити, людський перегляд і механізми оскарження [18, с. 3-4; 18, с. 6-7; 13; 15; 51; 14]. Для транскордонної узгодженості дедалі активніше задіюються технічні стандарти, ISO/IEC JTC 1/SC 42 - дані, надійність, оцінювання; профільні напрацювання в межах ITU, тобто Міжнародного союзу електрозв'язку, як місток між "м'якими" принципами та регуляторними вимогами [70; 71].

Технічна стандартизація у цій сфері має не допоміжне, а системне значення. Вона дозволяє перетворити загальні юридичні вимоги на перевірювані технічні процедури. Наприклад, вимога надійності потребує критеріїв тестування; вимога прозорості - документації та пояснюваності; вимога недискримінації - оцінки наборів даних і результатів моделі; вимога підзвітності - журналювання, відстежуваності та визначення відповідальних суб'єктів. Саме тому стандарти ISO/IEC та ITU можуть у майбутньому виконувати роль технічного додатку до міжнародно-правових режимів, особливо у сферах високого ризику та подвійного використання [70; 71].

У військовому регулюванні штучного інтелекту ключове завдання - зберегти дієвість норм міжнародного гуманітарного права (МГП) в умовах, коли алгоритми беруть на себе дедалі критичніші функції розвідки, цілевказання та ураження. Базові принципи розрізнення, пропорційності та заборони зайвих страждань застосовні незалежно від рівня автономності системи; відтак держава повинна доводити, що її алгоритмічні рішення здатні забезпечити ці вимоги на практиці [18, с. 6-7]. Саме тут фокусується правова дискусія: наскільки "значущим" має бути людський контроль, щоби запобігти дегуманізації війни та помилковим ураженням [4].

У цьому контексті поняття "значущий людський контроль" не може зводитися до формальної присутності людини в ланцюгу прийняття рішення. Для міжнародного гуманітарного права важливо, щоб людина мала реальну можливість розуміти параметри дії системи, оцінювати контекст, перевіряти ціль, враховувати обставини

конкретної атаки, зупинити або змінити рішення системи і нести відповідальність за застосування сили. Якщо людський контроль є лише номінальним, а швидкість, складність або непрозорість системи фактично позбавляє оператора здатності впливати на результат, такий контроль не відповідає гуманітарній логіці регулювання автономної зброї.

Історично "технологічний зсув" розпочався з інтеграції безпілотників у цикл ураження. У 1982 р. Ізраїль застосував розвідувальні БПЛА Mastiff/Scout у долині Бекаа для вимотування сирійської ППО та високоточного подавлення ракетних комплексів - талонна операція, що продемонструвала, як безпілотна розвідка змінює тактику та знижує ризики для пілотованої авіації [72; 73]. На початку 2000-х США перетворили MQ-1 Predator із "очей у небі" на ударну платформу, інтегрувавши AGM-114 Hellfire; уже перші епізоди 2001 р. засвідчили уразливість до хибних розвідданих і складність процедур віддаленого ухвалення рішень [74; 75]. 3 листопада 2002 р. удар Predator у Ємені започаткував практику екстериторіальних "цілевих уражень" поза класичними театрами війни - із новими питаннями про юрисдикцію, кваліфікацію конфлікту та співвідношення МГП і міжнародного права прав людини [76].

Негативні ефекти та лакуни регулювання були прямо окреслені в мандатних доповідях ООН. У 2010 р. доповідач Філіп Алстон застеріг від "ерозії гарантій" через непрозорість "цілевих убивств" і відсутність належної підзвітності; він наполіг на чітких критеріях статусу цілі, правових підставах та механізмах ex post контролю [77].

У 2013 р. Кристоф Гейнс виніс у центр порядку денного проблему летальної автономії: алгоритми без достатнього людського втручання не гарантують належного розрізнення й пропорційності; запропоновано мораторій до вироблення надійних правових запобіжників [78; 79].

На національному рівні судові інстанції почали формувати "контури відповідальності": Пешаварський Високий суд у 2013 р. визнав удари дронів у Пакистані такими, що порушують суверенітет і норми МГП; у Німеччині суди розглядали обов'язки уряду щодо використання бази Ramstein у зв'язку з

екстериторіальними ударами; у Великій Британії судовий контроль стосувався передачі розвідданих і потенційної причетності до міжнародних злочинів - ці справи загалом заклали рамку опосередкованої відповідальності транзитних держав і партнерів по обміну даними [80; 81; 82; 83; 84].

Ці приклади демонструють, що технологічне посередництво не усуває питання відповідальності, а навпаки ускладнює його. У випадку дистанційного або автономізованого застосування сили відповідальними можуть бути не лише безпосередні оператори, а й держави, що надають інфраструктуру, розвіддані, програмне забезпечення, логістичну підтримку або територію для операцій. Таким чином, ІІІ виводить на перший план питання співучасті, належного контролю, обов'язку запобігання та меж допустимої передачі даних у військових цілях.

Міжнародно-правове регулювання почало розвиватися двома напрямками.

Перший напрямок розвивається шляхом тлумачення й імплементації чинного МГП: зокрема, через обов'язкову правову експертизу нових засобів і методів ведення війни за ст. 36 ДП І, оцінювання сценаріїв, меж автономності, параметрів людського контролю, технічних запобіжників, та вимогу зберігати "значущий людський контроль" над критичними функціями, виявлення, відбір і ураження цілі [62; 4].

Другий напрямок розвивається шляхом "правотворення в межах Конвенції про окремі види звичайної зброї": з 2014 р. Група урядових експертів із ЛАСО виробила керівні принципи й термінологію, але через розбіжності позицій великих військових держав дискусія триває щодо форми майбутнього режиму - від протоколу до окремого договору [67]. До появи "жорстких" зобов'язань функцію тимчасових обмежувачів виконують політичні документи: Політична декларація про відповідальне використання ІІІ та автономії в межах процесу REAIM, широке коло держав-підписантів, і окрема Політична декларація США щодо відповідального військового застосування ІІІ та автономії, стандарти планування, випробувань, оцінювання ризиків, прозорості й підзвітності [69; 68].

Варто зазначити, що сучасні військові розробки вийшли далеко за межі тематики використання дронів, що відповідно ставить питання і перед міжнародним правом. Стрімко поширюються барражуючі боєприпаси та "роєві" тактики; наземні й морські автономні платформи набувають стійкості до втрати зв'язку; у командуванні та управлінні застосовують системи підтримки рішень на базі аналізу великих масивів сенсорних даних; у кіберпросторі ІІІ використовується для автоматизації виявлення вразливостей, фішингових кампаній і оборонної кіберстійкості; електронна боротьба та радіотехнічна розвідка покладаються на алгоритми класифікації сигналів; системи ПРО/ППО інтегрують комп'ютерний зір для розпізнавання цілей у реальному часі; масово розвиваються контр-дронові комплекси з елементами ІІІ. Ці напрями посилюють традиційні ризики, автоматизаційна упередженість оператора, брак пояснюваності, підвищена швидкість ескалаційних циклів, уразливість до підміни даних та імітацій, і підштовхують до стандартизації "технічних запобіжників" - вимог до надійності, кіберстійкості, відстежуваності рішень (traceability) і "безпечного зупину", що вже напрацьовуються в ISO/IEC та ITU й можуть бути інкорпоровані в майбутні правові режими як додатки або технічні протоколи [70; 71].

Паралельно зберігається обов'язок держав здійснювати правові огляди за ст. 36 до прийняття нових систем; міжнародний діалог у форматі CCW, а також політичні декларації виконують роль "рейок", які не дають практиці випередити право настільки, щоб зруйнувати гуманітарні гарантії [62; 67; 68; 69].

У підсумку можемо погодитись із тим, що військове регулювання ІІІ еволюціонує до "двоколіїної моделі": негайна імплементація МГП і правових експертиз - поруч із поступовою кодифікацією параметрів допустимої автономності, людського контролю та технічної надійності у багатосторонніх форматах, що має утримати технологічний прогрес у межах гуманності війни [4; 62; 67; 70; 71; 18, с. 6-7].

Водночас "двоколіїна модель" не знімає всіх проблем. Її слабким місцем залишається відсутність універсального визначення автономної системи озброєння,

єдиного критерію значущого людського контролю та узгодженого механізму перевірки державних практик. Держави можуть по-різному тлумачити допустимий рівень автономності, межі делегування рішення машині, обсяг попереднього тестування та умови застосування в реальному бою. Тому перехід від політичних декларацій до більш конкретних норм залишається необхідним, особливо у частині систем, здатних самостійно виявляти, класифікувати і уражати цілі без достатнього людського втручання.

У військовому регулюванні ІІІ саме російсько-українська війна стала "лабораторією" для перевірки спроможності норм МГП витримувати натиск автономізації: алгоритми вже працюють у розвідці, цілевказанні, ураженні та протидії засобам супротивника, а отже - щоденно тестують межі принципів розрізнення, пропорційності та запобігання зайвим стражданням [18, с. 6-7]. Відповіддю України стало інституційне оформлення безпілотного компоненту: створено Сили безпілотних систем як окремий рід військ, анонс - лютий 2024 р.; правове оформлення та розгортання - 2024-2025 рр., що централізує розробку, закупівлі й застосування наземних, повітряних і морських платформ [85; 88; 92].

Паралельно нарощується цифрова "нервова система" ведення бою: платформу ситуаційної обізнаності Delta інтегровано у багатодоменні операції, вона акумулює сенсорні дані, підтримує планування, обмін у реальному часі й дедалі ширше використовує алгоритмічний аналіз для виявлення цілей та скорочення циклу "спостереження-рішення-дія" [89; 90; 93].

На рівні тактики широке застосування отримали FPV-дрони з елементами машинного зору, барражуючі боєприпаси та випробування ройових сценаріїв; українські підрозділи неодноразово застосовували малі автономні групи дронів, а вітчизняні розробники тестують масштабування до великих роїв [87; 94].

Супротивник відповідає прискореною автономізацією ударних засобів, зокрема Lancet та інші барражуючі системи, і системною радіоелектронною протидією. РФ розгортає масоване глушіння супутникової навігації, GPS/GNSS, у прикордонних і

прифронтових зонах, що впливає як на цивільну авіацію, так і на військові спроможності, змушуючи сторони переходити до інерціальної, візуальної та радіолокаційної навігації, а також розвивати алгоритми, стійкі до завад [96; 95]. Аналітики фіксують еволюцію російського "kill chain" від поодиноких Lancet-3 на початку вторгнення до комплекснішої системи виявлення-ураження з використанням безпілотників і коригованих боєприпасів; у відповідь українські сили масштабували контрдронові рішення, мобільну ППО та маневр у "смузі EW" [91; 97; 98].

Зауважимо, що практичні наслідки для права двоякі. З одного боку, інструменталізація штучного інтелекту виявила вузькі місця МГП у частині верифікації цілі за умов "зашумленого" середовища та високої швидкості ескалації; з іншого - прискорила впровадження процедур експертиз (*ex ante*) і технічних запобіжників, *traceability*, надійність, "безпечний зупин", як мінімум де-факто стандартів, які вже напрацьовують ISO/IEC та ITU і які можуть бути інкорпоровані у майбутні правові режими [70; 71].

Поза тематикою використання дронів бойова практика виходить на новий рівень застосування ШІ: алгоритмічна підтримка командування та управління, *fusion* сенсорних потоків у реальному часі, пріоритизація цілей, електронна боротьба, класифікація сигналів, адаптивні перешкоди, кібероперації, автоматизація пошуку вразливостей і оборонних *playbooks*, контр-дронові комплекси, детекція, ідентифікація, перехоплення, а також ППО/ПРО з комп'ютерним зором для розпізнавання об'єктів на високих швидкостях [89; 93; 99].

Україна, спираючись на масиви бойових даних, розвиває алгоритми для прискореного аналізу знімків з БпЛА й супутників та для пілотування дальніх ударних систем; офіційні особи прямо зазначають, що ШІ скорочує час пошуку цілей з "десятків годин" до хвилин і відкриває шлях до вищого рівня автономності, включно з роями [86].

У відповідь міжнародні дискусії щодо "значущого людського контролю", прозорості й верифікованості державних практик отримали нову емпіричну базу саме зі Сходу Європи; уроки України вже імпортуються у НАТО-процеси взаємосумісності

та у формування загальних технічних профілів безпеки для автономних функцій ураження й протидії [90; 99; 71].

Узагальнюючи, штучний інтелект як технологія подвійного використання формує для міжнародного права не одну, а кілька взаємопов'язаних проблем. Перша полягає у складності розмежування цивільного і військового призначення, оскільки базові модулі ШІ можуть переходити між секторами без зміни своєї технічної природи. Друга полягає у фрагментації правового регулювання: цивільна сфера орієнтується на права людини, прозорість, недискримінацію і захист даних, тоді як військова сфера спирається на міжнародне гуманітарне право, правові огляди зброї та контроль над застосуванням сили. Третя полягає у зростанні ролі технічних стандартів, які поступово стають фактичними інструментами юридичної операціоналізації принципів. Четверта полягає у тому, що реальна бойова практика, зокрема досвід російсько-української війни, випереджає універсальну нормотворчість і змушує держави швидше визначати межі допустимої автономності.

Тому міжнародно-правове регулювання ШІ у сфері подвійного використання доцільно розглядати як багаторівневу систему. На першому рівні діють загальні принципи прав людини, демократії, верховенства права та міжнародного гуманітарного права. На другому рівні формуються спеціальні режими для цивільних високоризикових систем і військових автономних функцій. На третьому рівні розвиваються технічні стандарти, оцінки впливу, аудити, правові огляди, логування, *traceability* та механізми людського контролю. На четвертому рівні поступово формується міжнародна координація, яка поєднує ООН, Раду Європи, ЄС, ОЕСР, ЮНЕСКО, НАТО, процеси REAIM, Hiroshima AI Process, AI Safety Summit та дискусії в межах CCW. Саме така поетапна і багат шарова модель дозволяє зберегти баланс між технологічним розвитком, безпекою, правами людини та гуманітарними обмеженнями застосування сили.

1.3. Роль глобалізації у формуванні міжнародно-правових засад інституту штучного інтелекту

Глобалізація в сучасній теорії описується як інтенсифікація транснаціональних взаємозв'язків, коли локальні процеси дедалі частіше визначаються віддаленими економічними, політичними та інформаційними потоками; цю парадигму закладено в працях Ентоні Гідденса, Девіда Гелда та Мануеля Кастельса, які показали, як мережеві структури перетворюють взаємозалежність на нову "нормальність" світового порядку [117; 118; 120-121]. Після пандемії COVID-19 мова йде вже не про кінець глобалізації, а про її перекалібрування: МВФ (Міжнародний валютний фонд) фіксує геоекономічну фрагментацію поряд зі збереженням взаємозалежності, а СОТ (Світова організація торгівлі) демонструє відновлення торгівлі й сталий ріст "цифрово доставлюваних послуг", які підтримують інтеграцію навіть за умов політичних бар'єрів [112; 113]. Саме на цьому тлі діджиталізація, тобто системне використання даних, мереж і обчислень у публічних і приватних процесах, стає інфраструктурою глобалізації: вона здешевлює доступ до інформації та обчислювальних ресурсів, прискорює транскордонні потоки даних і створює умови для масштабованих систем ШІ (штучного інтелекту) як технології загального призначення [106; 107].

У міжнародно-правовому вимірі це означає, що штучний інтелект не може розглядатися лише як внутрішня технологічна політика окремої держави. Його функціонування залежить від глобальних ланцюгів даних, хмарної інфраструктури, міжнародного ринку напівпровідників, транскордонних сервісів, цифрової торгівлі, кібербезпеки та діяльності приватних платформних корпорацій. Тому глобалізація створює не лише технологічну, а й нормативну взаємозалежність: рішення однієї держави щодо стандартів ШІ може впливати на суб'єктів в інших юрисдикціях, а відсутність узгоджених підходів створює ризики фрагментації правового простору. У цьому сенсі формування міжнародно-правових засад інституту ШІ є прямим наслідком глобального характеру цифрової інфраструктури.

Цей взаємозв'язок безпосередньо релевантний для міжнародного права. Коли ІІІ вбудовується у транскордонні інформаційні, торговельні та безпекові процеси, виникає потреба одночасно в кількох типах міжнародно-правових інститутів:

- правозахисних, для захисту приватності, недискримінації, процесуальних гарантій і належної обачності в алгоритмічних рішеннях;
- безпекових, для операціоналізації вимог міжнародного гуманітарного права та запобігання зловживанням, зокрема маніпуляції інформацією, автономним функціям ураження;
- торговельно-економічних, для режимів транскордонних потоків даних і недискримінаційного доступу до ринків;
- технічних, для спільних стандартів життєвого циклу моделей і управління ризиками [100; 101; 106].

Така багаторівнева структура підтверджує, що міжнародно-правовий інститут ІІІ формується не ізольовано, а на стику кількох процесів. Правозахисний блок пов'язаний із цифровими правами людини і захистом від дискримінаційних алгоритмічних рішень. Безпековий блок охоплює питання військового ІІІ, летальних автономних систем озброєння, кібероперацій та інформаційного впливу. Торговельно-економічний блок стосується переміщення даних, доступу до цифрових ринків, експортного контролю і технологічної конкуренції. Технічний блок забезпечує практичне перетворення принципів на процедури, оскільки саме через стандарти, аудити, сертифікацію та оцінку ризиків загальні норми набувають операційного змісту.

Політичні "опори" цієї архітектури вже закріплені в Пакті заради майбутнього та Глобальному цифровому договорі, що визначають довіру до даних, міждіагностичність і безпеку алгоритмів як спільні орієнтири для держав і міжнародних організацій [102-105]. На рівні регуляторної імплементації діджиталізація спричинила перехід від етики до процедур: стандарти ISO/IEC (Міжнародна організація зі стандартизації / Міжнародна електротехнічна комісія), зокрема ISO/IEC 42001 для систем управління ІІІ та пакет SC 42 щодо якості даних, надійності й оцінювання ризиків, виконують роль

"технічних скоб", через які принципи перетворюються на верифіковані практики, придатні для взаємного визнання у правопорядках різних країн [108].

Окремо важливо, що діджиталізація змінює не лише предмет, а й форму міжнародно-правового інституцієтворення. По-перше, вона приводить у правове поле нових потужних акторів - глобальних хмарних і платформних провайдерів, без участі яких забезпечити транспарентність і підзвітність алгоритмічних систем неможливо; звідси акцент ООН (Організації Об'єднаних Націй) і регіональних утворень на багатостейкхолдерному врядуванні [102-105]. По-друге, діджиталізація підсилює ефект "екстериторіальної дії" норм: регіональні режими на кшталт AI Act ЄС (Європейського Союзу) задають вимоги, що де-факто поширюються на глобальних постачальників, і це стимулює зближення підходів, аби уникнути фрагментації стандартів [109]. По-третє, у сфері миру та безпеки вже окреслено "вхідну рамку" універсального рівня: резолюція ГА ООН (Генеральної Асамблеї Організації Об'єднаних Націй) A/RES/79/239 підтвердила застосовність міжнародного права, включно з МГП (міжнародним гуманітарним правом) і МППЛ (міжнародним правом прав людини), до військового ІІІ та закликала до відповідального використання; на рівні безпекових союзів НАТО (Організація Північноатлантичного договору) закріпив принципи відповідального застосування, сумісні з міжнародним правом і суміжними політичними процесами, зокрема REAIM (Responsible AI in the Military Domain, відповідальний штучний інтелект у військовій сфері) і Блетчлі [114; 100-101].

Це важливо тому, що по-перше, без аналітичної прив'язки до глобалізації та діджиталізації інститути ІІІ виглядають як ізольовані ініціативи, тоді як насправді вони є відповіддю на структурні зміни світового господарства та комунікацій [117-118; 112-113]. По-друге, щоб пояснити багаторівневість правотворення, автором було розроблено відповідну модель (Рис. 3) (Додаток 5). Така модель демонструє послідовність переходу від універсальних політичних орієнтирів до регіональних правових режимів, технічних стандартів і процедур імплементації. Її зміст полягає в тому, що міжнародне правотворення у сфері ІІІ не рухається лінійно від одного

договору до одного національного закону, а формується через взаємодію кількох рівнів: глобального, регіонального, секторального, технічного та національного [102-105; 108; 109].

Така послідовність демонструє механізм переходу від soft law до юридично зобов'язуючих норм [102-105; 108; 109]. По-третє, вона дозволяє запобігати фрагментації: показати, де саме потрібні інтерфейси взаємного визнання, оцінка відповідності, аудити, міжоперабельність даних і моделей, аби національні режими не створювали бар'єри для прав людини, безпеки та торгівлі в цифрову епоху [106; 113]. І по-четверте, вона дозволяє визначити ролі акторів: універсальні органи, насамперед ГА ООН, задають принципи й процес, секторальні та регіональні майданчики, зокрема РЄ (Рада Європи), ЄС, НАТО, ОЕСР (Організація економічного співробітництва та розвитку), ITU (Міжнародний союз електрозв'язку), ISO (Міжнародна організація зі стандартизації), заповнюють техніко-правові прогалини; така координація і є суттю інституцієтворення в епоху діджиталізації [100-101; 102-105; 108-109].

Системна відповідь міжнародної спільноти на цей зсув закріплена у Пакті заради майбутнього (A/RES/79/1) та додатку до нього - Глобальному цифровому договорі. Обидва документи задають "спільні правила гри" для цифрової екосистеми: довіру до даних, міжоперабельність, безпеку алгоритмів, інклюзивність та багатостейкхолдерну взаємодію. Вони прямо адресують штучний інтелект як сегмент цифрового порядку, що потребує узгоджених принципів і механізмів реалізації [102-105]. У практичній площині ці політичні орієнтири вже підживлюють перехід від "етики" до операційного врядування: від етичних декларацій - до вимог управління ризиками ШІ на рівні організацій, зокрема ISO/IEC 42001, і пакетів стандартів довіри/якості даних, SC 42, які де-факто стають проксі-нормами для майбутніх договорів [108].

У цьому контексті особливого значення набуває питання про співвідношення політичних і технічних інструментів. Політичні документи, такі як Пакт заради майбутнього або Глобальний цифровий договір, визначають цілі, принципи та загальні напрями співпраці. Однак вони не дають вичерпних процедур перевірки алгоритмічних

систем. Таку функцію виконують технічні стандарти, що деталізують, як саме має здійснюватися управління ризиками, документування моделі, контроль якості даних, валідація, аудит і постійний моніторинг. Саме тому в умовах глобалізації технічна стандартизація стає частиною ширшої міжнародно-правової архітектури, хоча формально вона не завжди має договірну природу.

Ключовим рушієм, що поєднує глобалізаційні процеси з діджиталізацією, є цифрова конвергенція - узгоджена робота трьох шарів інфраструктури: даних, обчислювальних ресурсів і мережевого середовища. Саме вона забезпечує безперервний життєвий цикл систем III: збір і підготовку даних, тренування моделей, їх розгортання та подальший моніторинг у реальних умовах. На кожній стадії виникають вимоги до належного врядування даними, походження, якості, правові підстави обробки, до технічної надійності, робастності, кіберстійкості, і до процедурної підзвітності, аудити, протоколи тестування, протидія дискримінації, без яких неможливе правове закріплення практик у транскордонному вимірі [106; 108].

У результаті ця конвергенція "приземляє" формування міжнародно-правових інститутів III одразу в кількох площинах. У правозахисній - це вимоги прозорості, недискримінації, можливості оскарження рішень і належної обачності, зокрема у відповідь на маніпулятивні можливості алгоритмічних процесів, зафіксовані в документах Ради Європи [109]. У сфері міжнародної безпеки - підтвердження застосовності норм міжнародного права та міжнародного гуманітарного права до алгоритмічних систем і закріплення "значущого людського контролю" в оборонних політиках і принципах, що вибудовуються в ООН і НАТО [100; 101]. В економіко-правовому вимірі - режими транскордонних потоків даних і взаємне визнання оцінок відповідності, потрібні для збереження сумісності ринків і недискримінаційного доступу до них. Технічна площина забезпечується стандартами і системами сертифікації, зокрема ISO/IEC 42001 та пакетами SC 42 щодо управління ризиками, якості даних і довіри до III, що перетворюють принципи на операційні вимоги для розробників і замовників [108]. Доповнюють це міжурядові процеси WSIS/ITU (World

Summit on the Information Society / International Telecommunication Union, Всесвітній саміт з питань інформаційного суспільства / Міжнародний союз електрозв'язку), спрямовані на міжоперабельність і узгодження цифрових політик, які слугують інституційним "мостом" між політичними рамками та технічними нормами [110-111].

Цифрова конвергенція як злиття трьох шарів, тобто "дані - обчислення - мережі", забезпечує безперервний життєвий цикл систем ІІІ: збір і підготовку даних, тренування, вивантаження, розгортання та моніторинг. Для відображення цього процесу в роботі доцільно використати модель цифрової конвергенції, що забезпечує життєвий цикл систем ІІІ (Рис. 4) (Додаток 6). Зміст цієї моделі полягає в тому, що кожен інфраструктурний шар одночасно має технічний і правовий вимір: дані потребують законності обробки, якості та захисту; обчислення потребують безпеки, доступності та контролю; мережі потребують стійкості, кіберзахисту та міжоперабельності [100; 101; 109; 108; 110-111].

На цьому циклі "вішаються" відповідні інститути: правозахисні, прозорість, недискримінація, оскаржуваність; безпекові, застосовність норм МП (міжнародного права) і МГП, вимога людського контролю; економічні, режими трансграничних потоків даних, взаємне визнання сертифікації; а також стандарти та сертифікаційні механізми, що надають технічні "скоби" для права [100; 101; 109; 108; 110-111].

Таким чином, цифрова конвергенція виконує подвійну функцію: по-перше, створює матеріальну основу для масштабованих систем ІІІ у глобальному обігу; по-друге, задає правотворчу архітектуру, у межах якої правозахисні, безпекові, економічні та технічні інститути взаємно підсилюють одне одного. Саме завдяки стандартизованим метрикам, аудиторам, сертифікації та міжоперабельним мережевим рішенням стає можливим перехід від політичних декларацій до практик, що підлягають верифікації й контролю, а відтак - до юридично зобов'язуючих режимів, узгоджених між державами і релевантними міжнародними організаціями [100; 101; 109; 108; 110-111].

Після пандемії COVID-19 дискусія про "кінець глобалізації" справді загострилася, однак емпіричні ряди свідчать радше про її структурне переформатування: МВФ фіксує геоекономічну фрагментацію, переналаштування ланцюгів постачання, нові бар'єри, але водночас підкреслює збереження взаємозалежностей через торгівлю, інвестиції та поширення технологій [112]. СОТ у звіті за 2024 рік відзначає відновлення товарної торгівлі після спаду 2023-го і стійкість каналів цифрової торгівлі та "цифрово доставлюваних послуг", які стали ключовим носієм діджиталізації на глобальному ринку [113]. Для правотворення це задає подвійне завдання: зменшувати регуляторну фрагментацію за рахунок сумісних стандартів і взаємного визнання процедур, оцінка відповідності, нагляд, інтероперабельність даних і моделей, водночас захищаючи легітимні публічні інтереси - безпеку, права людини і довіру до алгоритмів - у рамці політичних орієнтирів Пакту заради майбутнього та Глобального цифрового договору [102-105; 116].

Це означає, що сучасна глобалізація у сфері ІІІ не є однорідним процесом відкритості. Вона поєднує взаємозалежність і фрагментацію. З одного боку, держави, компанії та користувачі залишаються залежними від транскордонних цифрових сервісів, обчислювальних потужностей, даних і міжнародної торгівлі. З іншого боку, зростає тенденція до технологічного суверенітету, контролю за критичними технологіями, обмеження експорту, локалізації даних і формування регіональних нормативних блоків. Для міжнародного права це створює складне завдання: забезпечити достатню сумісність стандартів без повного усунення права держав встановлювати власні моделі захисту безпеки, прав людини і публічного порядку.

У воєнному вимірі ця логіка проявляється найяскравіше у війні росії проти України, де діджиталізація бойового простору і використання ІІІ створили випробувальний полігон для норм міжнародного гуманітарного права та процедур відповідального застосування. Резолюція ГА ООН A/RES/79/239 підтвердила застосовність міжнародного права, включно з МГП і МППЛ, до військових систем ІІІ, закріпила вимогу відповідального використання та інклюзивного діалогу як основу

подальшого нормотворення [114]. На боці України сформовано інституційні передумови для керованого впровадження технологій: створені Сили безпілотних систем як окремий рід військ, розгортається платформа ситуаційної обізнаності Delta для багатодоменної інтеграції сенсорних потоків і прискореного циклу "виявлення-рішення-дія", у підрозділах масштабовано застосування FPV-дронів, барражуючих боеприпасів і сценаріїв роїв із елементами машинного зору [85; 88-90; 93-94]. Противник відповідає насиченою радіоелектронною боротьбою та глушінням GNSS (Global Navigation Satellite System, глобальна навігаційна супутникова система), що примушує до розвитку алгоритмів стійкої навігації й адаптивних контр-дронових рішень; еволюцію "kill chain" РФ і відповідні українські контрзаходи фіксують незалежні аналітики [91; 95-98]. Усе це безпосередньо пов'язує діджиталізацію з правом: зростання швидкості та автоматизації рішень висуває вимогу формалізованого людського контролю над критичними функціями ураження, відстежуваності (traceability) і надійності алгоритмів, а також регулярних правових експертиз за ст. 36 ДП І (Додаткового протоколу І) до Женевських конвенцій як мінімум де-факто стандартів на поточному етапі [100-101; 108].

Практика війни в Україні водночас підштовхує до зближення політичних і технічних шарів регулювання: політичні рамки ООН, відповідальне використання, і оборонні принципи НАТО, законність, підзвітність, надійність, керованість/можливість відключення, зменшення упередженості, відстежуваність, знаходять технічну опору в стандартах управління ІІІ та каталогах вимог до якості даних і кіберстійкості, ISO/IEC 42001; пакети SC 42, що полегшує взаємне визнання перевірок і аудиту в транснаціональних операціях постачання та спільних програмах випробувань [101; 108]. У підсумку цифровізація війни зумовлює не лише появу нових технологічних практик, ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance, розвідка, спостереження, виявлення цілей і рекогносцировка) на базі ІІІ, C2-системи (Command and Control, системи командування і управління) з алгоритмічною підтримкою, інтегровані контр-дронові комплекси, а й прискорює інституційний перехід від декларацій до процедур: від політичного підтвердження застосовності

права - до впровадження спільних тестів безпеки, методів валідації, механізмів підзвітності та, зрештою, до кодифікації мінімальних юридично зобов'язуючих параметрів допустимої автономності в озброєннях [100-101; 114; 85-99].

Після уточнення положень про глобалізацію та діджиталізацію доцільно візуалізувати, як інфраструктурні шари, дані, обчислення, мережі, "несуть" життєвий цикл ІІІ і де саме "підчіплюються" міжнародно-правові інститути. Це допомагає зв'язати політичні рамки, Пакт, Глобальний цифровий договір, із технічними стандартами ISO/IEC та подальшою юридизацією норм у праві прав людини, безпеки, торгівлі й стандартизації [102-105; 108-111]. Для цього в роботі доцільно використати схему (Рис. 5) (Додаток 7), логіка полягає у тому, що дані, обчислення і мережі утворюють матеріальну основу систем ІІІ, а правозахисні, безпекові, економічні та технічні інститути формують нормативну надбудову над цією основою.

Діджиталізація створила матеріальну основу для масштабованого застосування ІІІ й одночасно породила попит на узгоджені правила прозорості, підзвітності та безпеки. Політичну відповідь на це сформульовано у Пакті заради майбутнього та Глобальному цифровому договору: вони задають спільні орієнтири щодо довіри до даних, міждоперабельності та безпеки алгоритмів, які далі конкретизуються у секторах [102-105]. Щоб перейти від декларацій до практик, міжнародна спільнота спирається на технічні стандарти: ISO/IEC 42001 фіксує вимоги до систем управління ІІІ на рівні організацій, а пакет SC 42 деталізує життєвий цикл, якість даних, робастність, валідація, оцінка ризику, забезпечуючи інструменти аудиту та взаємного визнання між юрисдикціями [108]. Після COVID-19 глобалізація не зникла, а перекалібрувалася: на тлі фрагментації зберігається висока взаємозалежність через цифрову торгівлю й "цифрово доставлявані послуги", що робить критичною сумісність інститутів у сфері ІІІ, аби уникати розривів стандартів і правової невизначеності [112-113; 116].

У площині миру й безпеки закладено універсальну "вхідну рамку" - резолюцію A/RES/79/239 про застосовність міжнародного права, включно з МГП і МППЛ, до військових систем ІІІ і вимогу відповідального використання; у безпекових союзах,

насамперед НАТО, діють операційні принципи відповідального застосування, законність, підзвітність, надійність, керованість, зменшення упередженості, відстежуваність, що поєднують політичні орієнтири з технічними процедурами тестування та сертифікації [100-101; 114]. Сукупно це вибудовує багаторівневу архітектуру врядування: універсальні майданчики формують принципи та процеси, регіональні й галузеві платформи - стандарти й механізми оцінки відповідності, держави - імплементують і здійснюють нагляд. Така послідовність забезпечує поступовий перехід від "м'яких" документів до юридично зобов'язуючих режимів без розриву між нормами й практикою, зберігаючи баланс між інноваціями, захистом прав людини, безпекою та справедливими умовами торгівлі [100-101; 102-105; 108; 112-114; 116].

Узагальнено можна зазначити, що глобалізація впливає на формування міжнародно-правових засад інституту ІІІ у трьох основних площинах. Перша площина є матеріальною: глобальні мережі, дані, обчислювальна інфраструктура і цифрові сервіси створюють об'єктивні умови для транскордонного застосування ІІІ. Друга площина є нормативною: держави і міжнародні організації змушені виробляти спільні принципи, оскільки ізольоване регулювання не здатне охопити реальні ланцюги створення, навчання, розгортання і використання систем ІІІ. Третя площина є інституційною: у регулювання включаються не лише держави, а й міжнародні організації, технічні органи стандартизації, регіональні союзи, приватні технологічні компанії, наукові центри і професійні спільноти.

Саме тому роль глобалізації не можна зводити лише до фону розвитку ІІІ. Вона виступає чинником, який пояснює, чому інститут ІІІ в міжнародному праві має міжгалузевий і багаторівневий характер. Якщо цивільне застосування ІІІ ставить питання прав людини, приватності, недискримінації та цифрової торгівлі, то військове застосування активізує міжнародне гуманітарне право, контроль автономності, відповідальне використання та правові експертизи нових засобів ведення війни. Якщо економічний вимір вимагає сумісності стандартів і взаємного визнання процедур, то

технічний вимір забезпечує операційні інструменти для аудиту, сертифікації, тестування і контролю. У сукупності це підтверджує, що міжнародно-правове регулювання ІІІ формується не як єдиний ізольований режим, а як комплекс взаємопов'язаних норм, процедур і стандартів, що виникають у відповідь на глобалізовану природу цифрових технологій.

Висновки до 1-го розділу

У першому розділі проаналізовано становлення інституту штучного інтелекту в міжнародному праві як міжгалузевого правового явища, що формується на перетині прав людини, міжнародного гуманітарного права, міжнародної відповідальності, кібербезпеки, інтелектуальної власності, цифрової торгівлі та міжнародної безпеки. Досліджено два основні підходи до його правового осмислення: перший передбачає формування окремого міжнародно-правового інституту ІІІ, другий виходить із адаптації чинних норм міжнародного права до нових технологічних умов. Обґрунтовано, що на сучасному етапі ці підходи не виключають один одного, а співіснують у межах поступової інституціоналізації ІІІ.

Узагальнено, що інститут ІІІ формується через поєднання актів м'якого права, юридично зобов'язуючих договорів, технічних стандартів, етичних принципів, регіональних регламентів і практик міжнародних організацій. Окремо досліджено ІІІ як технологію подвійного використання, що пояснює його одночасну належність до цивільного, економічного, безпекового і військового регулювання. Встановлено, що головним правовим питанням залишається не міжнародна правосуб'єктність ІІІ, а збереження відповідальності держав, розробників, операторів і користувачів за результати використання таких систем.

РОЗДІЛ 2. СТАНОВЛЕННЯ ЗАСАД МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВІЙСЬКОВОГО ВИКОРИСТАННЯ ІНСТИТУТУ ШТУЧНОГО ІНТЕЛЕКТУ

2.1. Американський підхід до міжнародно-правового регулювання використання [технологій] штучного інтелекту у військовій та безпековій сферах

Початок розвитку американської школи ШІ задав Дартмутський літній проєкт 1956 року: Джон Маккарті, автор терміна *artificial intelligence*, Марвін Мінський, Герберт Саймон і Аллен Ньюелл запропонували дослідницьку програму "симуляції інтелекту технічними системами", визначивши теми навчання, використання мови, абстрагування та розв'язання задач як ядро нової дисципліни [128]. На інституційному рівні в США склався стійкий трикутник "університети - оборонні агентства - ринок": фінансування DARPA (Defense Advanced Research Projects Agency, Агентство перспективних оборонних дослідницьких проєктів) й Пентагону забезпечувало тривалий період досліджень; лабораторії MIT (Massachusetts Institute of Technology, Массачусетський технологічний інститут), Стенфорда, CMU (Carnegie Mellon University, Університет Карнегі-Меллона) та інших університетів формували кадрову базу і методологію; підприємницькі кластери Кремнієвої долини конвертували прототипи в продукти [129; 131].

Визначальними віхами стали програма Strategic Computing (1983-1993), яка інституційно "перевчила" спільноту від демонстрацій до вимірюваних прикладних результатів, і призова модель DARPA Grand Challenge (2004-2007), що створила ринок автономної мобільності та прискорила перехід від дослідницьких платформ до індустріальних систем керування [130; 131]. Хвиля "глибинного навчання" 2010-х була швидко інтегрована у корпораціях США, зокрема Google, Meta, Microsoft, і пов'язана з академічними центрами NYU (New York University, Нью-Йоркський університет), Stanford, CMU, що закріпило структурне лідерство Сполучених Штатів у глобальній екосистемі ШІ [128; 129; 130; 131].

Американська модель розвитку ШІ сформувалася як послідовний ланцюг взаємодії трьох підсистем - державного оборонного фінансування, університетсько-

лабораторної мережі та ринкових платформ масштабування, що разом створили стале середовище перенесення наукового результату у практику. Тривалі оборонні програми, подібні до Strategic Computing (1983-1993), забезпечили горизонти досліджень, сформулювали вимірювані технологічні орієнтири, зокрема автономні функції керування, експертні системи, VLSI (very-large-scale integration, надвелика інтеграція мікросхем), і виробили інституційні процедури оцінювання результативності та трансферу розробок у прикладні домени [131]. Відтак у змагальних форматах DARPA, зокрема Grand Challenge 2004-2007 років, було закріплено інженерні критерії спроможності для автономних систем, що пришвидшило вихід із лабораторних прототипів до промислових платформ і створило цілі сегменти ринку автономної мобільності [130]. На цьому фундаменті університетські центри, зокрема MIT, Stanford, CMU та інші, виконали роль механізму методологізації: вони забезпечили відкритість публікацій, відтворюваність результатів, підготовку кадрів і безперервну циркуляцію знань між академією та індустріальними лабораторіями. Коли у 2010-х роках "глибинне навчання" стало домінантним підходом, саме така мережа сприяла швидкій інституціоналізації нових методів у корпораціях США та закріпила їхній пріоритет у глобальній екосистемі ШІ [129].

Причинно-наслідковий ланцюг американської моделі доцільно подати через авторську схему, у якій послідовно відображено зв'язок між оборонним фінансуванням, університетськими лабораторіями, ринковими платформами, секторальним правозастосуванням та подальшим формуванням регуляторних вимог (Рис. 6) (Додаток 8). Така модель дозволяє показати, що американський підхід не виник як єдиний законодавчий акт, а сформувався як інституційна траєкторія, у межах якої технологічні прориви, ринкове масштабування і відомче регулювання поступово створювали нормативне поле для ШІ [129-131; 132-136].

До того ж приєднався прискорювальний механізм ринкових платформ. Масштабні сервіси на кшталт YouTube і Netflix конвертували академічні напрацювання у стійкі операційні рішення: двоступеневі архітектури добору і ранжування рекомендацій, експериментальні дизайни А/В, керування даними та інфраструктурою

моделювання стали нормою інженерної практики на мільярдах вибірок і безперервних потоках подій [132; 133]. Саме це масштабування створило вимірювані зовнішні ефекти - від клінічних застосувань до безпеки транспорту і справедливості алгоритмів, на які регуляторні та судові інституції почали реагувати у секторальний спосіб.

У медичній сфері FDA (Food and Drug Administration, Управління з контролю за продуктами і лікарськими засобами США) сформуло референтний кейс, надавши допуск автономній системі діагностики IDx-DR із визначеними умовами застосування та відповідальності; у транспорті NHTSA (National Highway Traffic Safety Administration, Національна адміністрація безпеки дорожнього руху США) застосувало інструменти відкликання і технічного нагляду щодо функцій часткової автоматизації керування; у публічній політиці реконструкція алгоритму ризику рецидиву COMPAS стала підставою для вимог прозорості, аудитів і процедур оскарження автоматизованих оцінок [134; 136; 135].

Так виникає характерна для США траєкторія "експост-врядування": спочатку - широке впровадження і накопичення емпіричних даних про ризики та ефекти, а вже потім - інституціоналізація вимог через стандарти, регуляторні приписи, прецедентні рішення й організаційні процедури управління ризиками. Зворотний зв'язок із цього регуляторного контуру повертається у процес проектування систем: підвищуються вимоги до якості й походження даних, тестування, валідації й простежуваності, у цикли розробки вбудовуються практики оцінювання впливу, а на рівні виробників та операторів формуються політики відповідності. Сукупно це пояснює стійкість моделі без наявності єдиного рамкового федерального акту про ШІ: функції нормотворення розподілені між довгими оборонними програмами як генераторами технологічних пріоритетів, університетсько-індустріальною мережею як носієм методів і кадрів та секторальними регуляторами і судами як механізмами кодифікації практик після масштабування [129-131; 132-136].

У сегменті цифрових платформ рекомендаційні системи стали базовою інфраструктурою персоналізації контенту й монетизації аудиторії. На матеріалі Netflix

детально описано перехід від евристичних схем до ансамблів моделей та безперервних експериментальних циклів, де A/B-тестування виступає механізмом емпіричної валідації гіпотез щодо добору та ранжування, а організаційна практика "онлайн-експериментів за замовчуванням" забезпечує керованість впливу моделі на ключові бізнес-метрики утримання та конверсії [132]. Ця архітектура включає розподіл функцій між офлайнним тренуванням і онлайнною інференцією, керування холодним стартом, багаторівневі фільтри якості й контроль зсувів даних.

У кейсі YouTube задокументовано глибинну двоступеневу конструкцію: на першому етапі компактна нейромережа відбирає мільйони кандидатів до невеликого списку з урахуванням користувацької історії та контексту сеансу, на другому - більша модель ранжує ці кандидати з оптимізацією кількох цільових функцій, зокрема переглядів, довжини сесії, взаємодій [133]. Зміна парадигми від "ознакових" до "представницьких" підходів, тобто векторизації користувача і контенту, пояснює приріст стійкості й масштабованості систем на порядках взаємодій; саме цей клас рішень згодом стандартизується у вигляді внутрішніх політик контролю релевантності, захисту від маніпуляцій і механізмів пояснюваності для модерації [132; 133].

У сфері охорони здоров'я реперним є прецедент схвалення FDA автономної діагностичної системи IDx-DR для виявлення діабетичної ретинопатії в первинній ланці без обов'язкового паралельного тлумачення офтальмологом [134]. Клінічний пакет і регуляторне рішення фіксують вимоги до даних, зокрема якості знімків і протоколів збору, метрик, чутливості/специфічності на заздалегідь визначених порогах, процедур калібрування та валідації, а також умови використання в закладах із визначеною компетенцією персоналу [134]. Цей допуск зміщує акцент із "decision support" до "decision autonomy" у чітко визначеному завданні, формуючи матрицю розподілу відповідальності між виробником, який відповідає за алгоритмічну працездатність у межах заявлених умов, закладом, який відповідає за процес і інфраструктуру, та клініцистом, який інтегрує висновок у лікувальне рішення. Наслідком стає поява відомих керівництв щодо керованості ризиків AI-виробів медичного призначення, управління змінами моделей, документування даних,

постмаркетинговий моніторинг, які у США виконують роль де-факто стандартів для суміжних клінічних застосувань [134].

У правоохоронній системі проблематика алгоритмічної справедливості та підзвітності увійшла в правозастосовний дискурс через публічно резонансні кейси у кримінальній юстиції. Реконструкція роботи скорингу COMPAS виявила асиметрії помилок між групами, чутливість до непрямих ознак і обмеженість процедур оскарження автоматизованих оцінок у судовому процесі [135]. Висвітлені методологічні конфлікти між різними формалізаціями "справедливості", зокрема рівність помилок, рівність позитивних прогнозів, калібрування, продемонстрували неможливість їх одночасного досягнення на нерівноважних розподілах і, як наслідок, необхідність експліцитного нормативного вибору критеріїв для публічних задач. Далі ця дискусія трансформувалася у вимоги до прозорості, опису моделі, даних і метрик, незалежних аудитів, ведення журналів рішень і права на ефективне оскарження, що в США імплементується переважно через керівництва та політики відомств на рівні штатів і муніципалітетів, а також через судові прецеденти у справах щодо доступу до алгоритмічних інструментів, розкриття ознак і вагових коефіцієнтів [135].

У транспорті та безпеці руху сфокусованим індикатором переходу від експериментальних функцій водіння до регуляторної практики став нагляд NHTSA за системами допомоги водієві з елементами автоматизації. Масштабне відкликання Tesla за повідомленням 23V-838 із вимогою оновлень, спрямованих на зниження неправильного використання Autosteer, закріпило підхід "програмного" відкликання як інструмента виправлення поведінки складних кіберфізичних систем у полі експлуатації; паралельно технічне розслідування EA22002 концентрується на верифікації заявлених функцій у різних сценаріях дорожньої обстановки [136]. Судовий вердикт 2025 року у справі про летальний інцидент з використанням Autopilot підсилив регуляторно-правову вісь: у фокусі опинилися питання доказовості, доступу до телеметрії та журналів подій, комунікаційних практик виробника, меж допустимості маркетингових тверджень щодо "самокерування" і розподілу відповідальності між водієм та системою в режимах часткової автоматизації [136]. У сукупності ці елементи

визначають траєкторію, за якої секторальний нагляд і судові процедури інкрементально формують вимоги до життєвого циклу моделей у критичних застосуваннях: дані та сценарії валідації, інтервенційні механізми безпечного відмовляння, журнали прийняття рішень, політики оновлень і післяринкового моніторингу [132; 133; 134; 135; 136].

Наведені кейси демонструють характерну для США послідовність нормотворення: спочатку відбувається широке технічне та комерційне впровадження алгоритмічних рішень у масштабі великих платформ і критичних секторів, після чого на основі накопичених емпіричних даних про ризики і зовнішні ефекти ініціюється кодифікація практик у формі секторальних регуляторних приписів і судових прецедентів. У медичній сфері це реалізується через допуски та умови застосування, що деталізують вимоги до даних, валідації, калібрування, простежуваності і постмаркетингового моніторингу, зокрема на прикладі IDx-DR [134]. У транспорті - через наглядові процедури, програмні відкликання і технічні розслідування, які інкорпоруєть "поведінкові" вимоги до систем часткової автоматизації у реальних сценаріях експлуатації, на прикладі Autosteer/Autopilot [136]. У публічному секторі - через прецедентні дискусії щодо критеріїв алгоритмічної справедливості, процедур оскаржуваності та прозорості інструментів ризик-скорингу COMPAS, що трансформуються в організаційні вимоги до аудитів і розкриття параметрів застосування [135]. Для масових цифрових платформ ядром стають внутрішні політики управління даними і експериментуванням, А/В-тестування, керування зсувами, контроль за релевантністю та маніпулятивними практиками, які поступово узгоджуються з очікуваннями регулятора і судів стосовно прозорості та підзвітності [132; 133].

У підсумку за відсутності єдиного федерального акта про III регуляторна щільність забезпечується поєднанням секторального "післядіючого" регулювання, зокрема допуски, відкликання, інспекції, керівництва, судових рішень у справах про приватність, відповідальність за продукцію та недобросовісні комунікації, а також організаційних механізмів управління ризиками в межах життєвого циклу моделей,

зокрема контроль якості даних, валідаційні протоколи, журнали рішень, післяринковий нагляд. Така конфігурація зближує етичні принципи з операційними вимогами до проектування, розгортання і супроводу систем, не вимагаючи на початкових етапах кодифікації у вигляді всеохопного федерального закону [132-136].

Для систематизації виявлених закономірностей доцільно використати таблицю, у якій узагальнено, як у США відбувається трансформація технічних та організаційних практик у нормативні вимоги в різних секторах (Таблиця 3) (Додаток 9). Добір доменів здійснено за критеріями наявності масштабного впровадження ШІ, оформлених регуляторних інструментів або судових рішень і відстежуваних наслідків для життєвого циклу моделей. Для кожного домену в таблиці подано характерний інструмент або механізм, відповідний юридичний ефект та опорні джерела. Матеріал має аналітичний характер і слугує "картою відповідності" між практикою застосування ШІ та еволюцією регуляторних підходів у США, окреслюючи вектори подальшої гармонізації стандартів і нагляду [132-136].

Правове регулювання ШІ у США має стратифіковану природу: ініціація відбувається одночасно на рівні Білого дому, Конгресу та відомств, але закріплення норм переважно здійснюється секторально і "післядійово", на підставі емпіричних ризиків та прецедентів. Конгрес започаткував інституційну основу досліджень і координації через National AI Initiative Act (2020), яким створено Національний офіс з питань ШІ при OSTP (Office of Science and Technology Policy, Офіс науки і технологічної політики) і визначено механізми міжвідомчої взаємодії [137].

На рівні виконавчої влади у 2022 р. Офіс науки і технологічної політики оприлюднив "Blueprint for an AI Bill of Rights" - п'ять принципів проектування і застосування автоматизованих систем, зокрема безпечність та ефективність, протидія дискримінації, приватність, пояснюваність, людиноцентричний контроль, що виконують роль політичного орієнтира для відомств і штатів [138; 139]. У жовтні 2023 р. було видано Виконавчий указ 14110 про "безпечну, надійну і доброчесну" розробку та використання ШІ, який зобов'язував розробників найпотужніших моделей проводити оцінювання безпеки та ділитися результатами з урядом, доручав NIST

(National Institute of Standards and Technology, Національний інститут стандартів і технологій США) розробити методики тестування, а відомствам - інтегрувати захист прав споживачів і працівників у політики III [140; 141].

Паралельно NIST завершив добровільний "AI Risk Management Framework 1.0" у січні 2023 р. як технічний каркас управління ризиками для організацій, що охоплює ідентифікацію, оцінювання, пом'якшення та моніторинг ризиків із профілюванням під різні домени застосування [142]. Для федеральних агенцій OMB (Office of Management and Budget, Адміністративно-бюджетне управління США) закріпив обов'язкові мінімальні практики управління ризиками у меморандумі M-24-10 від 28 березня 2024 р.: створення органів управління III, інвентаризація випадків використання, оцінки впливу на права і безпеку, політики прозорості щодо систем, що взаємодіють із громадянами [143]. Попри наявність цих правових рамок, 23 січня 2025 р. нова адміністрація видала указ "Removing Barriers to American Leadership in Artificial Intelligence", яким було скасовано низку політик попереднього періоду в частині вимог і процедур, що вважалися "перешкодами" для інновацій; це створило регуляторну нестабільність і підвищило роль відомчих керівництв і стандартів, що залишилися чинними, зокрема NIST AI RMF та OMB M-24-10 [144]. Інформаційні повідомлення про скасування ключових положень EO-14110 підтвердили тренд на дерегуляційний перегляд, зберігаючи водночас окремі лінії діяльності агентств і координацію з галуззю [145].

Секторальна площина продовжує виконувати функцію "де-факто регулювання". У медицині FDA через систему настанов і допусків переходить від статичних до "еволюційних" AI-виробів, фіналізуювши підхід "предвстановлених планів змін" (PCCP, Predetermined Change Control Plan) для безпечних оновлень моделей без окремої ринкової заявки на кожну модифікацію; це кодифікує вимоги до даних, валідації, простежуваності, постринкового нагляду та звітності [134; 146; 147]. У сфері праці ЕЕОС (Equal Employment Opportunity Commission, Комісія з рівних можливостей у сфері зайнятості США) роз'яснила застосування Title VII до алгоритмічних інструментів добору і оцінювання персоналу, наголосивши на обов'язку роботодавців

запобігати непропорційній шкоді захищеним групам і забезпечувати аудит та оскаржуваність [148-151].

У захисті споживачів чотири федеральні органи, FTC (Federal Trade Commission, Федеральна торгова комісія), DOJ (Department of Justice, Міністерство юстиції США), CFPB (Consumer Financial Protection Bureau, Бюро фінансового захисту споживачів), ЕЕОС, зробили спільну заяву: "винятку для III" не існує - чинні закони про недобросовісні практики, дискримінацію та конкурентну політику поширюються на автоматизовані системи; отже, неправдиві маркетингові твердження про функціональність "на III", алгоритмічна дискримінація і непрозорі профілювання підлягають примусовому правозастосуванню [152-154]. У цифрових платформах і транспорті триває посилення нагляду NHTSA й судових процедур, зокрема програмні відкликання, технічні розслідування, питання доказовості та розподілу відповідальності у режимах часткової автоматизації, що формує техніко-юридичні вимоги до життєвого циклу моделей у критичних застосуваннях [136].

Водночас ключова риса США - "клаптевість" на рівні штатів і муніципалітетів: поруч із загальними правами на приватність, CCPA/CPRA (California Consumer Privacy Act / California Privacy Rights Act, Каліфорнійський закон про захист приватності споживачів / Каліфорнійський закон про права на приватність) з окремим регулятором CPPA (California Privacy Protection Agency, Каліфорнійське агентство із захисту приватності), виникають доменно-специфічні норми щодо алгоритмічних інструментів, зокрема Нью-Йорк, Local Law 144 про аудити упередженості AEDT (Automated Employment Decision Tools, автоматизовані інструменти прийняття рішень у сфері зайнятості), та перший у країні комплексний "ризик-орієнтований" закон штату щодо III - Colorado AI Act, який з 2026 р. встановлює обов'язки розробників і користувачів "високоризикових" систем, презумпції належної обачності за умови дотримання процедур і повідомлень споживачам [155-161]. Така фрагментація, посилена множенням нових приватних законів різних штатів, створює неоднорідні зобов'язання, ускладнюючи міжштатну діяльність та підвищуючи транзакційні витрати відповідності.

Наслідки цієї архітектури для правового поля можна звести до кількох векторів. По-перше, діє горизонтальна політика без "великого" федерального закону: загальнонаціональні орієнтири, зокрема Blueprint, EO-14110, його подальші скасування, NIST AI RMF, OMB M-24-10, задають методологію і мінімальні очікування, але не створюють уніфікованої кодексуальної рамки; тому "тверді" норми формуються переважно у секторах і штатах [139-144; 155-161]. По-друге, посилюється роль відомчого правозастосування: FTC/DOJ/CFPB/EEOC та галузеві регулятори, зокрема FDA і NHTSA, конвертують етичні принципи в операційні вимоги через керівництва, допуски, відкликання і прецеденти; це швидко реагує на ризики, але породжує різноманітність і локальні стандарти [134; 136; 147; 152-154]. По-третє, динамічним залишається співвідношення "регуляція - інновації": дерегуляційні кроки 2025 р. зменшили федеральні бар'єри для R&D (research and development, дослідження і розробки), однак підвищили значення добровільних стандартів і відповідальності компаній за власні системи управління ризиками; у відсутності єдиного закону функцію "узгоджувача" фактично виконують NIST AI RMF і галузеві керівництва [142-144; 146-147].

У підсумку американська модель залишається гібридною: політичні ініціативи задають ціннісно-процедурні орієнтири, технічні стандарти - операційні механізми, а секторальні регулятори й суди - фактичні "кодіфікатори" вимог до життєвого циклу ІІІ. Стійкість системи забезпечується інституційною інерцією NIST/OMB/агентств/спецслужб і активним правозастосуванням, зокрема антимонопольним, споживчим, трудовим, тоді як головна прогалина - відсутність єдиного федерального акта - компенсується щільністю м'якого права, "пошаровим" наглядом і зростаючою роллю прав штатів [132-136; 139-161].

Значний масив практик залишається поза прямою кодифікацією на федеральному рівні: немає спеціального закону, що системно регулює автоматизовані рішення у сфері праці, добір/оцінювання, кредитуванні, страхуванні, рекламі, а також у правоохоронній діяльності; застосовуються загальні норми про недискримінацію, захист споживачів і приватність, а деталізація переважно здійснюється на рівні штатів і відомств. За

підсумками 118-го скликання Конгресу в 2023-2024 рр. зареєстровано понад 150 законопроектів щодо ШІ, однак жоден не став законом, що інституційно зафіксувало "дефіцит всеохопної рамки" та перенесло навантаження на "м'яке" право, секторальне правозастосування і політику штатів [162]. Паралельно Національна конференція законодавчих зборів штатів (NCSL, National Conference of State Legislatures) відзначає різке зростання активності на субнаціональному рівні, однак їхній характер залишається фрагментарним і неоднорідним, із різними тестами впливу, визначеннями "високого ризику" й процедурами аудитів, що підвищує транзакційні витрати відповідності для бізнесу між юрисдикціями [163].

Юридична аналітика підтверджує: домінує модель "саморегулювання під наглядом" - внутрішні кодекси й аудити алгоритмів, орієнтація на міждержавні принципи ОЕСР (Організація економічного співробітництва та розвитку) 2019 р. та технічні рамки NIST замість єдиного федерального "AI-акта"; водночас на рівні штатів формується "кляптева ковдра" норм, від локальних аудитів інструментів зайнятості до ризик-орієнтованих актів, зокрема Colorado AI Act, що ускладнює уніфікацію практик [15; 142; 163; 164]. Додатковим чинником регуляторної нестабільності став політичний зсув у січні 2025 р.: новий президентський указ про "усунення бар'єрів" для американського лідерства в ШІ скасував низку вимог попереднього періоду, переорієнтувавши федеральну політику з безпеково-підзвітної на проінноваційну; фактично це підвищило вагу добровільних стандартів, NIST AI RMF, інституцій дослідження безпеки, U.S. AI Safety Institute, AISIC (Artificial Intelligence Safety Institute Consortium, Консорціум Інституту безпеки ШІ), та прав штатів як носіїв "твердих" зобов'язань [142; 144; 165; 166].

Звідси впливає причинний комплекс, чому у США регулювання не переходить до єдиного федерального закону: політична поляризація щодо масштабу регулювання; економічні побоювання "задушити" інновації в конкуренції з Китайською Народною Республікою; лобістська перевага великої індустрії на користь гнучких правил; висока швидкість технологічної еволюції, що ускладнює вироблення усталених дефініцій, критеріїв ризику і меж відповідальності. Поки Конгрес не схвалив загальну рамку,

системоутворювальними залишаються секторальний нагляд, зокрема FDA, NHTSA, міжвідомчі керівництва, судові прецеденти та "політика штатів", які разом поступово конвертують етичні принципи в операційні вимоги до життєвого циклу моделей [134; 136; 142; 144; 162-166].

Міжнародна арена: ініціативи та позиція США

Публічні заклики до посиленого регулювання ШІ у 2023-2025 рр. створили короткочасне "вікно можливостей", однак не трансформувалися у всеосяжний федеральний акт, а законодавча інерція зберігається попри зростання ризиків і політичної уваги. Кульмінацією став розгляд у підкомітеті Сенату 16 травня 2023 р., де керівники індустрії, зокрема керівник OpenAI Сем Альтман, відкрито підтримали ідею запровадження державного ліцензування для найбільш потужних моделей і загалом рамок безпеки для "frontier AI" [175; 176]. У березні 2023 р. група науковців і підприємців, серед яких Ілон Маск, підписала відкритого листа з пропозицією на пів року призупинити тренування систем потужніших за GPT-4; однак жодна з провідних лабораторій цього не зробила, а вже у липні 2023 р. Маск запустив власну компанію xAI, що продемонструвало обмеженість мораторіальних підходів без правового підкріплення [177; 178].

Паралельно виконавча влада намагалася сконцентрувати зусилля: 4 травня 2023 р. віцепрезидентка Камала Гарріс провела зустріч із CEO (chief executive officer, виконавчий директор) провідних компаній, зокрема Google, Microsoft, OpenAI, Anthropic, закликавши до добровільного впровадження практик безпеки, а 21 липня 2023 р. Білий дім узгодив із сімома найбільшими компаніями США добровільні зобов'язання щодо тестування, прозорості, кібербезпеки та маркування контенту - "м'який" формат, який підняв планку очікувань, але не створив юридичної відповідальності [179; 180; 181]. У Сенаті лідер більшості Чак Шумер ініціював серію "AI Insight Forums", з вересня 2023 р., за участю CEO та експертів для вироблення базових принципів майбутнього закону; однак конвертації дискусій у нормотворчі тексти поки не відбулося, що зафіксовано у незалежних треках [182; 183].

На тлі цього стратегічна лінія США залишалася подвійною: з одного боку, декларативне стимулювання інновацій і дерегуляційний наратив, ще з EO-13859 "American AI Initiative" від 11 лютого 2019 р., який прямо ставив ціль зменшення бар'єрів до використання ШІ, з іншого - лінія на безпеку і підзвітність 2023 р. через керівні документи та виконавчі дії; у 2025 р. нова адміністрація частково відкотила регуляторні орієнтири, зберігши натомість вагу добровільних стандартів і секторального нагляду [184; 179; 180; 144]. Узагальнюючий індикатор полягає в тому, що за 118-го скликання Конгресу, 2023-2024 рр., зареєстровано понад 150 AI-біллів, жоден із яких не став законом: структурні причини - політична поляризація, побоювання нашкодити конкурентоспроможності США в перегонах із КНР (Китайською Народною Республікою), сильні лобістські позиції індустрії та висока швидкість технологічної еволюції [162].

На міжнародній арені персоніфіковані ініціативи поєднувалися з "м'яким" інституційним дизайном: Сполучені Штати підтримали Принципи ОЕСР (2019) і стали співзасновниками GPAI (Global Partnership on Artificial Intelligence, Глобальне партнерство зі штучного інтелекту) у червні 2020 р., а в 2023-2024 рр. підтримали процес G7 Hiroshima AI Process, Блетчлійську декларацію та "Frontier AI Safety Commitments" у Сеулі; паралельно створено U.S. AI Safety Institute та консорціум AISIC для методик тестування безпеки, що віддзеркалює ставку на стандарти й оцінювання, а не на "жорсткі" договори [15; 16; 167-169; 165; 166]. У військово-гуманітарному вимірі Держдеп просуває Політичну декларацію щодо відповідального військового використання ШІ та автономії, наполягаючи на людському контролі/судженні; однак у межах КЗЗЗ (Конвенції про заборону або обмеження застосування конкретних видів звичайної зброї, CCW, Convention on Certain Conventional Weapons) США, як і низка союзників, не підтримують негайного укладення юридично зобов'язуючого договору про заборону ЛАСО (летальних автономних систем озброєння, LAWS, lethal autonomous weapon systems), пропонуючи концентруватися на застосовності чинного МГП (міжнародного гуманітарного права) та статті 36 ДП I (Додаткового протоколу I до Женевських конвенцій), кращих практиках і прозорості. Така позиція разом із

позиціями інших великих держав стримує договірну кодифікацію і підтримує формат політичних принципів [170-174].

На глобальному рівні США послідовно просувають архітектуру "м'якого" врядування ІІІ: долучилися до Принципів ОЕСР у травні 2019 р. як першої міжурядової рамки довірчого, людиноцентричного ІІІ; підтримали запуск у червні 2020 р. Глобального партнерства з питань ІІІ під егідою G7 (Group of Seven, Група семи) як майданчика для координації політик і практик; у 2023 р. в межах G7 підтримали Hiroshima AI Process - керівні принципи та Міжнародний кодекс поведінки для розробників передових систем; у листопаді 2023 р. приєдналися до Блетчлійської декларації на Саміті з безпеки ІІІ у Великій Британії, що зафіксувала спільне бачення ризиків "frontier AI" і необхідність оцінювання моделей до та після розгортання; у 2024 р. на AI Seoul Summit американські компанії були серед підписантів "Frontier AI Safety Commitments", які конкретизують зобов'язання з тестування, управління ризиками та прозорості [15; 16; 167-169]. У самій інституційній інфраструктурі США створено U.S. AI Safety Institute при NIST і багатосторонній AISIC-консорціум для випробувань і методик безпеки, що слугує трансатлантичній конвергенції зі спорідненими ініціативами у партнерів [165; 166].

У безпеково-гуманітарному вимірі позиція США прагматично обережна: Вашингтон активно просуває Політичну декларацію про відповідальне військове використання ІІІ та автономії, State Department, підтримує "людський контроль/судження" як принцип розроблення і застосування систем, але не схиляється до негайних переговорів про юридично зобов'язуючий договір у межах КЗЗЗ/CCW щодо повної заборони летальних автономних систем; офіційні виступи США вказують на достатність застосування чинного міжнародного гуманітарного права з актуалізацією правових оглядів за статтею 36 ДП І та виробленням кращих практик [170; 171; 172]. На майданчиках ООН, зокрема ПГЕ (Група урядових експертів) КЗЗЗ щодо ЛАСО, регулярні сесії 2024-2025 рр., триває робота над "meaningful/appropriate human control", проте консенсусу щодо договірної моделі немає; огляди та репортажі фіксують інерцію дискусій і політичні розбіжності провідних держав, попри риторику

невідкладності [173; 174]. Такий підхід віддзеркалює стратегічний баланс США: підтримувати конвергенцію принципів і технічних стандартів, посилювати інститути безпеки, зокрема тестування, доступ регуляторів до оцінювання моделей, але уникати обмежень, здатних стримати інноваційний потенціал або створити асиметричні зобов'язання.

Узагальнення причин "зависання" регулювання доцільно інтегрувати до загальної характеристики американської моделі. По-перше, діє регуляторна економія, тобто небажання створювати асиметричні обмеження для власних виробників у глобальній конкуренції. По-друге, США роблять інституційну ставку на стандарти NIST, AISIC і "добровільні зобов'язання", які швидше оновлюються, але слабше прив'язують відповідальність. По-третє, політичний цикл і поляризація ускладнюють ухвалення єдиного федерального закону. По-четверте, невизначеність дефініцій і критеріїв ризику ускладнює написання технологічно "стійкого" закону. У результаті "регулювання через практику" - через відомчі допуски, відкликання, прецеденти - залишається головним каналом нормоутворення, тоді як всеосяжний федеральний акт і надалі перебуває поза досяжністю [134; 136; 162; 165-166].

Військова сфера - ключова роль ІІІ

Військова сфера у США є одним із головних векторів розвитку та інституціоналізації ІІІ, де технологічні експерименти йдуть у зв'язці з нормативними рамками і відомчими процедурами контролю. На рубежі 2000-х сформувався оперативний шаблон "розвідка-цілевказання-удар" із використанням безпілотних платформ і алгоритмічної аналітики; символічним маркером став перший зафіксований випадок позасудового ураження цілі з борта MQ-1 у Ємені в листопаді 2002 р., коли дистанційно керований апарат із високоточною боєголовкою застосували в антитерористичній операції [193]. Хоч цей епізод не був "повністю автономним", він запустив стійку траєкторію переходу до рішень, де машинне навчання підтримує розпізнавання об'єктів, фільтрацію потоків даних і швидке цілепокладання для людини-оператора. Далі ця лінія розвинулася в сімейства "loitering munitions", зокрема Switchblade 300/600, та інші комплекси, здатні тривалий час патрулювати й за командою

оператора здійснювати ураження, що радикально зменшило часовий розрив між виявленням і ударом [197; 198]. Паралельно Пентагон інвестував у автономію "вищих рівнів" - від керованих повітряних боїв до флотів безкіпажних кораблів; у квітні 2024 р. програма DARPA ACE (Air Combat Evolution, еволюція повітряного бою) разом із USAF (United States Air Force, Військово-повітряні сили США) зафіксувала історичний факт автономного керування винищувачем F-16, X-62A, у повітряному маневровому бою проти пілотованого F-16, що підтвердило зрілість алгоритмів у сценаріях "within-visual-range" і зрушило дискусію про межі довіри до бортового ШІ з теоретичної у практичну площину [191; 192].

Ключовою інституційною фігурою раннього "бойового" ШІ став генерал-лейтенант Джек Шенеган, який очолював Algorithmic Warfare Cross-Functional Team, тобто "Project Maven", і публічно рефлексував уроки конфлікту індустріальної та етичної оптики після резонансного виходу Google з контракту 2018 р.; саме цей кейс привів до ширшої відкритої дискусії щодо прозорості військових застосувань ШІ і необхідності чітких принципів [200; 201]. На рівні принципів у 2019 р. Defense Innovation Board (Рада з оборонних інновацій) під головуванням Еріка Шмідта запропонував етичні орієнтири responsible, equitable, traceable, reliable, governable, а в лютому 2020 р. Міністерство оборони формально їх ухвалило рішенням міністра Марка Еспера як обов'язкові до імплементації в закупівлі, випробування і бойове застосування [188; 187].

Наступним кроком стала нормативна кодифікація автономії в критичних функціях: оновлена 25 січня 2023 р. Директива DoD 3000.09 встановила політику, процедури тестування/верифікації та механізми зменшення ймовірності "небажаних уражень" для автономних і напіваавтономних функцій озброєння, інституціалізувавши вимогу достатнього людського контролю над застосуванням сили та створивши робочу групу з автономних систем [185; 186]. Інституціональну координацію з 2022 р. забезпечує CDAO (Chief Digital and Artificial Intelligence Office, Офіс головного посадовця з цифрових технологій і ШІ), який об'єднав JAIC (Joint Artificial Intelligence Center, Об'єднаний центр штучного інтелекту), Defense Digital Service та ADVANA; у

2025 р. публічні повідомлення зафіксували підготовку до зміни керівництва як прагнення посилити оперативну складову інтеграції III у JADC2/CJADC2 (Joint All-Domain Command and Control / Combined Joint All-Domain Command and Control, об'єднане багатодоменне командування і управління) та експериментальні контури бойового управління [189; 4]. Офіційне оновлення DoD Directive 3000.09 підтверджує, що документ установлює політику та відповідальність щодо розроблення і використання автономних та напівавтономних функцій у системах озброєння і спрямований на мінімізацію ризиків ненавмисних уражень.

На практичному рівні стратегічну ставку США на "масову, доступну, відновлювану" автономію кристалізувала ініціатива Replicator, анонсована заступницею міністра оборони Кетлін Гікс у серпні 2023 р.: за 18-24 місяці - виведення "тисяч" недорогих, мережево зв'язаних безкіпажних систем різних доменів із високим рівнем автономії, доповнених програмними "зв'язуючими тканинами"; 2024-го оголошено другу "хвилю" спроможностей, Replicator 1.2, для пришвидшеного розгортання [194; 195; 196]. Цей курс узгоджується з тенденціями останніх кампаній: безпілотні платформи й алгоритми аналітики даних стали центральними для темпу рішень і стійкості до РЕБ (радіоелектронної боротьби), що підтверджують і нові великі армійські контракти на польову аналітику "на краю" мережі, edge, та інтеграцію сенсорів у реальному часі [205; 204]. Водночас у повітряному бою експерименти на кшталт ACE показують рух до "людино-центричної автономії": машина виконує маневр і веде бій у рамках дозволених політик ризику, але людина зберігає контроль над цілями, правилами застосування сили та ескалацією [191; 192; 185].

Нормативно-політична рамка військового III у США має три опорні рівні. Перший - етичні принципи та відповідальний життєвий цикл, RAI (Responsible Artificial Intelligence, відповідальний штучний інтелект), що перекладені у процедури тестування, валідації, експлуатаційних обмежень і навчання персоналу згідно з "Responsible AI Strategy & Implementation Pathway" від червня 2022 р. та наступними документами відповідності OMB; це забезпечує зв'язок між принципами і закупівлею/бойовим застосуванням [202; 203]. Другий - "жорсткі" відомчі приписи для

озброєнь: DoD 3000.09 вимагає юридично й технічно забезпечуваного людського контролю над критичними функціями ураження, комплексних аналізів безпеки та мінімізації наслідків збоїв [185; 186]. Третій - зовнішній вимір легітимності: Державний департамент у лютому 2023 р. презентував Політичну декларацію щодо відповідального військового використання ШІ та автономії на саміті REAIM (Responsible AI in the Military Domain, відповідальний ШІ у військовій сфері) у Гаазі; декларація закріплює дотримання міжнародного права, включно з МГП, вимоги до випробувань, прозорості, управління ризиками і людського контролю, і слугує для США матрицею "soft law" у діалозі з партнерами та міжнародними процесами, зокрема КЗЗЗ/ООН [199; 170; 13].

На переговорах у межах КЗЗЗ США послідовно обґрунтовують застосовність чинного гуманітарного права та необхідність кращих практик, у тому числі правових оглядів за статтею 36 ДП І, замість негайної тотальної заборони ЛАСО, що віддзеркалює прагнення уникнути регулювання, яке створювало б асиметричні обмеження та гальмувало інноваційний цикл [170-174; 185].

Сукупний ефект цієї політики видно на рівні структур оборонного управління і ринку. У ЗС США (Збройних силах США) діє "людина в/на контурі" як незмінний принцип ухвалення летальних рішень, але сам контур стає "густішим": на тактичному рівні - портативні алгоритми на пристроях військових; на оперативному - об'єднані мережі даних і автономні носії, здатні діяти під РЕБ і деградацією каналів; на стратегічному - інститути перевірки безпеки та стандартів, які задають "технічні скоби" для правових норм [205; 195; 202]. Внаслідок цього саме військова сфера стала каталізатором для міжнародного порядку денного: союзники по НАТО адаптують власні принципи відповідального використання, а дискусія в ООН про "значущий людський контроль" над автономними функціями дедалі більше спирається на напрацьовані США процеси тестування, сертифікації та операційної підзвітності [100; 170; 199]. Із науково-практичного погляду американський кейс демонструє "регулювання через практику": технічні прориви, АСЕ, edge-аналітика, "масова автономія", запускають хвилю внутрішніх стандартів і зовнішніх декларацій; ці

інструменти не замінюють договори, але "цементують" мінімальні гарантії - дотримання МГП, людське судження, контрольованість, аудит слідів рішень, управління ризиками по всьому життєвому циклу [185; 187; 199; 202].

Військовий вимір ІІІ критичний для США через його прямий вплив на стратегічний баланс сил, темпи прийняття рішень і спроможність проєктувати силу в багатодомених операціях. Пентагон розглядає ІІІ як ключ до "переваги в циклі рішень": прискорене збирання та злиття розвідданих, зокрема спецслужбами, автоматизоване виявлення й пріоритизація цілей, керування безкіпажними платформами, повітряними, морськими, наземними, та кіберзасобами - всі ці компоненти зменшують часовий лаг між спостереженням і дією та підвищують живучість у середовищі перешкод і РЕБ [202; 205]. Конкуренти США, насамперед КНР і РФ (Російська Федерація), також інвестують у військовий ІІІ, що актуалізує проблему асиметрії зобов'язань: Вашингтон не готовий до односторонніх обмежень без гарантій взаємності, аби не втратити перевагу у швидкості, дальності та точності удару [172; 204]. Тому американська доктрина робить ставку на "відповідальний ІІІ" і уніфіковані процедури контролю ризиків у життєвому циклі військових систем, а не на негайні заборони, які можуть законсервувати технологічну нерівновагу на користь опонентів [199; 170-174].

Юридичне підґрунтя цієї позиції - застосовність чинного міжнародного гуманітарного права до всіх нових технологій: принципи розрізнення, пропорційності й запобігання зайвим стражданням мають виконуватися і в алгоритмічно керованих системах; стаття 36 Додаткового протоколу I до Женевських конвенцій вимагає від держави правового огляду кожного нового виду озброєнь, що у США інституційовано в практиках правової та технічної експертизи перед допуском до застосування [4; 173]. Політично й нормативно це закріплено в оновленій Директиві DoD 3000.09 від 25 січня 2023 р., яка встановлює вимоги до тестування, верифікації та експлуатаційних обмежень автономних і напіваавтономних функцій, фіксуючи зобов'язання забезпечити достатній людський контроль над застосуванням сили та мінімізувати ризик небажаних уражень [185; 186]. На рівні принципів Міністерство оборони офіційно ухвалило етичні

засади використання III, responsible, equitable, traceable, reliable, governable, запропоновані Defense Innovation Board, і інтегрувало їх у стратегію Responsible AI та процедури закупівель і випробувань, що перетворює абстрактні вимоги на перевірювані процеси, зокрема аудит слідів рішень, сценарне тестування, навчаність персоналу [188; 202]. Оновлений текст DoD Directive 3000.09 прямо пов'язує автономні та напіваавтономні функції у системах озброєння з вимогами політики, відповідальності, перевірки та зменшення наслідків збоїв.

У багатосторонній площині США просувають підхід "спочатку етика і стандарти, далі - норми": у рамках CCW/ООН американська делегація підтримує вироблення загальних принципів, зокрема "людське судження/контроль", прозорість, надійність, випробовуваність, технічних методик оцінювання і процедур правових оглядів, залишаючи договірні обмеження предметом майбутньої політичної доцільності. Перевага цього курсу - час на доведення і перевірку технологій без зупинки інноваційного циклу; його ризик - можливе відставання договірних рамок від практики, якщо автономні функції швидко поширюватимуться без узгоджених "запобіжників" [170-174]. Щоб зменшити цей ризик, Держдеп у 2023 р. представив Політичну декларацію щодо відповідального військового використання III та автономії з конкретизацією вимог до тестування, управління ризиками, прозорості та людського контролю - документ "м'якого права", який США пропонують як спільну мінімальну рамку до формальної кодифікації [199]. У паралельному союзницькому контурі НАТО у 2021-2024 рр. ухвалено Стратегію та принципи відповідального застосування III: вони синхронізовані з підходом США і створюють сумісні орієнтири для планування, інтероперабельності, обміну практиками і захисту від ворожого використання алгоритмів у багатонаціональних операціях [100; 101].

Операційний вимір підтверджує, чому саме військова сфера стала "лакмусовим папірцем" інституціоналізації III. Експерименти DARPA/USAF ACE із повітряним боєм на X-62A, F-16, показали, що автономні агенти здатні виконувати маневрові задачі в реальному небі за політиками ризику, залишаючи людині рішення щодо ескалації та правил застосування сили; це суттєво підняло планку обговорення допустимості

автономії в критичних функціях і водночас зміцнило вимоги до валідації, сертифікації й простежуваності алгоритмів [191; 192; 185]. Ініціатива Replicator, яку просуває заступниця міністра оборони Кетлін Гікс, орієнтує оборонно-промислову базу на швидке розгортання "масової, доступної, відновлюваної" автономії в усіх доменах, що відповідає логіці сучасних конфліктів і підштовхує союзників до сумісних стандартів керування ризиками, кіберзахисту та взаємодії в умовах деградації зв'язку [194-196]. У підсумку військова сфера виконує роль прискорювача для міжнародно-правових інститутів ІІІ: практичні вимоги, людський контроль, випробовуваність, аудит рішень, управління ризиками, переносяться у багатосторонні декларації, керівництва і стандарти, формуючи стримувальний контур без негайних універсальних заборон [199; 170-174; 188; 202].

У підсумку американська траєкторія поєднує технологічне лідерство з інституційною рамкою "відповідального ІІІ": у військовому сегменті пріоритет полягає у збереженні темпу інновацій і переваги в циклі рішень, водночас із забезпеченням виконання міжнародного гуманітарного права через правові огляди, статтю 36 ДП І, людський контроль над застосуванням сили та перевірюваність алгоритмів. На багатосторонніх майданчиках США просувають конвергенцію принципів і стандартизованих процедур випробувань як передумову для потенційних договірних рішень; у союзницькому контурі НАТО - уніфікують підходи до інтероперабельності та безпеки. Цей баланс пояснює і повільність загальнофедеральної кодифікації: за відсутності "великого" закону функцію нормотворення виконують відомчі директиви, політичні декларації та стандарти, які швидше адаптуються до еволюції технологій і зменшують ризик асиметричних обмежень у конкуренції з противниками.

2.2. Європейські підходи до міжнародно-правового регулювання використання [технологій] штучного інтелекту у військовій та безпековій сферах

Європейські підходи до міжнародно-правового регулювання використання технологій штучного інтелекту у військовій та безпековій сферах мають складну, багаторівневу і неоднорідну природу. На відміну від американської моделі, де визначальним чинником виступає поєднання технологічного лідерства, оборонних агентств, приватного сектору і відомчих механізмів відповідального ШІ, європейська модель формується через взаємодію кількох правових і політичних площин. До них належать право Європейського Союзу, стандарти Ради Європи, національні стратегії провідних європейських держав, підходи НАТО як союзницького оборонного середовища, позиції держав у межах ООН і Конвенції про конкретні види звичайної зброї, а також спеціальні політико-правові процеси, зокрема REAIM. Тому європейський підхід не може бути зведений до однієї моделі. Він є сукупністю взаємопов'язаних підходів, у яких поєднуються права людини, технологічний суверенітет, оборонна модернізація, етична кодифікація, технічна стандартизація та поступова юридизація процедур відповідального використання ШІ.

У межах цього дослідження європейську модель доцільно розглядати насамперед на прикладі Франції та Великої Британії. Такий підхід є обґрунтованим з огляду на те, що обидві держави належать до кола провідних європейських військово-політичних акторів, мають розвинені наукові школи у сфері штучного інтелекту, сформовану індустріальну базу, власні оборонні стратегії, активну участь у НАТО та помітну присутність у міжнародних дискусіях щодо автономних систем, відповідального ШІ і правового контролю за новітніми військовими технологіями. Водночас Франція і Велика Британія представляють два різні стилі європейського врядування ШІ. Французький підхід тяжіє до державного патронажу, технологічного суверенітету, етичної кодифікації та оборонної індустріалізації. Британський підхід більшою мірою спирається на проінноваційне регулювання, випробування передових моделей, секторальний нагляд, технічну експертизу та міжнародну модерацію ризиків frontier AI.

Історична траєкторія Франції та Великої Британії у становленні штучного інтелекту має спільний виток у фундаментальних роботах середини XX століття, але надалі розходиться на дві моделі інституціоналізації. У Великій Британії теоретичні

засади розвитку ШІ традиційно пов'язуються з Аланом Тюрінгом, який у статті 1950 року запропонував експериментальну процедуру оцінювання машинного інтелекту, тобто те, що згодом дістало назву тест Тюрінга [148]. Саме британська наукова традиція заклала одну з перших доктринальних рамок осмислення машинного інтелекту як здатності системи імітувати або відтворювати окремі форми людського мислення, комунікації і розв'язання задач. У 1980-х роках уряд Великої Британії відповів на глобальну технологічну конкуренцію, зокрема японську програму п'ятого покоління, масштабною державно-приватною ініціативою Alvey Programme, що профінансувала дослідження експертних систем, паралельних обчислень і засобів інженерії знань та заклала підґрунтя для комерціалізації академічних напрацювань [149].

Наступним важливим етапом британської траєкторії стало створення у 2015 році Alan Turing Institute, тобто національного інституту науки про дані й штучного інтелекту. Ця інституція об'єднала провідні університети, централізувала наукові інвестиції, сформувала міст між базовою наукою, державним управлінням і приватним сектором, а також стала одним із головних центрів вироблення прикладної експертизи щодо даних, алгоритмів і безпечного впровадження ШІ [150]. Паралельно британський уряд запустив політику прискорення інновацій, що включала урядовий огляд Hall-Pesenti 2017 року, AI Sector Deal та подальші інструменти фінансування стартапів, дослідницьких центрів і прикладних технологічних програм [141; 142]. Так поступово сформувалася британська модель, у якій держава не намагається одразу створити всеохоплюючий закон про ШІ, а вибудовує середовище для поєднання наукової експертизи, галузевого регулювання, ринкової інновації та секторального нагляду.

Французька траєкторія має іншу логіку. Вона спирається на сильні традиції математичних, інженерних і державницьких шкіл, зокрема ENS, INRIA, CNRS, а також на властиву французькій правовій і політичній культурі ідею стратегічної ролі держави у розвитку критичних технологій. У 2017-2018 роках ця траєкторія отримала політичну рамку AI for Humanity. Доповідь Седріка Вілані запропонувала державі комплексну стратегію, яка охоплювала розвиток національних центрів досліджень, відкритих даних, освіти, інновацій, етики та прав людини. Президент Емманюель Макрон у

березні 2018 року публічно анонсував інвестиції обсягом 1,5 млрд євро на 2018-2022 роки, підкресливши необхідність поєднання наукової першості з суспільною довірою, економічною конкурентоспроможністю і цифровим суверенітетом [151; 152]. За даними європейського огляду AI Watch, французький уряд справді визначив 1,5 млрд євро на розвиток ШІ до кінця 2022 року, зокрема близько 700 млн євро на дослідження.

Французька програма дала старт екосистемі інститутів, зокрема ANR-грантам, мережам лабораторій типу PRAIRIE, залученню індустріальних партнерів, посиленню ролі INRIA та CNRS, а також формуванню суверенних цифрових потужностей навколо французьких хмарних і обчислювальних ініціатив [151]. У цьому полягає одна з ключових відмінностей французької моделі: ШІ розглядається не лише як технологічний ресурс, а як елемент державної спроможності, наукового суверенітету, промислової політики і стратегічної автономії. У подальшому ця логіка безпосередньо вплинула на оборонну сферу, де питання ШІ почало розглядатися не тільки через призму інновацій, а й через призму військового планування, автономізації, контролю над озброєннями, захисту національного технологічного стеку та здатності держави не залежати від зовнішніх платформ у критичних функціях.

На перетині британської і французької траєкторій виник загальноєвропейський тренд науково-державного патронажу. Його зміст полягає в тому, що держава фінансує базову науку, обчислювальну інфраструктуру, дослідницькі центри та правову рамку, тоді як приватний сектор масштабує продукти, платформи, прикладні сервіси та індустріальні рішення. У цивільному сегменті цей тренд реалізується через політику даних, захист приватності, недискримінацію, прозорість алгоритмів, управління ризиками та відповідальність за автоматизовані рішення. У військовому сегменті ті самі елементи набувають більш складного значення, оскільки доповнюються вимогами міжнародного гуманітарного права, правової експертизи озброєнь, людського контролю, верифікації, валідації, аудиту, простежуваності і допуску до експлуатації.

Цивільні застосування та інституційні драйвери в обох країнах набули системної форми через цільові інструменти політики даних і нагляду. У Великій Британії з 2017 року формується зв'язка наука, норми, впровадження. Інститут Алана Тюрінга

продукує відкриті методики, наукову експертизу і кадровий потенціал; орган із захисту даних ICO та Центр етики даних та інновацій CDEI адаптують принципи GDPR до алгоритмічних систем; Національна служба охорони здоров'я NHS розгортає AI-пілоти, поєднуючи клінічні стандарти з оцінюванням ризиків; урядова структура DSIT координує національні пріоритети та у 2023 році провела перший глобальний Саміт із безпеки ШІ у Блетчлі [140; 143; 146]. Ця архітектура підтримується приватною школою практики, зокрема DeepMind, пов'язаною з Демісом Хассабісом, Google Research, а також іншими британськими осередками, що дали приклади масштабних платформних впроваджень і відкритих публікацій [146].

У Франції цивільне поле рухається двома взаємопов'язаними напрямками. З одного боку, державні інституції, зокрема INRIA, CNRS, Etalab і Міністерство трансформації та державної служби, формують політику даних, відкритості, етики і цифрового врядування. З іншого боку, промислові кластери, зокрема автомобілебудування, авіакосмічна галузь, фінансовий сектор, телекомунікації та оборонно-промисловий комплекс, інтегрують комп'ютерний зір, обробку природної мови, прогнозну аналітику і автоматизовані системи підтримки рішень у виробничі та управлінські процеси. Важливо, що в обох країнах етика за замовчуванням поступово зміцнюється через стандарти й вимоги до управління ризиками, оцінки впливу, аудит алгоритмів, пояснюваність і контрольованість, які у Великій Британії конвертуються в настанови ICO/CDEI, а у Франції, у відомчі етичні кодекси, керівні документи для державних сервісів і принципи цифрового суверенітету [140; 151].

У такій перспективі причини й мотивації держав є частково симетричними. Для обох держав важливими залишаються утримання наукової першості, комерціалізація досліджень, забезпечення прав людини, підтримка конкурентоспроможності, захист критичних даних і збереження контролю над обчислювальними ресурсами. Для Великої Британії додатковим чинником стала роль глобального модератора, тобто організація Блетчлійського саміту та спроба задати рамку безпечності передових моделей до появи всеосяжних міжнародних договорів [146]. Для Франції визначальним виступає постулат наукового і технологічного суверенітету, який від доповіді Вілані до

президентських звернень поєднує етичну відповідальність, захист персональних даних, індустріальний розвиток і контроль над критичною інфраструктурою [151; 152]. Саме ці мотиви визначили подальший перехід до безпеково-військового виміру, де обидві держави синхронізують національні політики з рамками НАТО та ширшими європейськими підходами.

Від початку 2010-х років Франція і Велика Британія послідовно переводять цивільні інструменти керованості ШІ в оборонний контекст. У Великій Британії це відбувається через Міністерство оборони, Defence AI Strategy 2022 року, Об'єднане командування збройних сил, Defence AI Centre, а також поступову уніфікацію процесів впровадження responsible AI у військовій сфері. У Франції відповідна лінія простежується через документ AI in support of defence 2019 року, створення етичної структури при Міністерстві збройних сил, посилення ролі DGA, а у 2024-2025 роках, через формування спеціалізованих інституційних інструментів оборонного ШІ, включаючи AMIAD [153; 154; 155]. Defence AI Strategy Великої Британії була офіційно оприлюднена 15 червня 2022 року і закріпила амбіцію перетворити британську оборону на AI ready організацію, що використовує ШІ для переваги, але з дотриманням стандартів, цінностей і норм суспільства.

Обидві країни, будучи провідними союзниками НАТО, брали участь у формуванні Альянсом принципів відповідального військового ШІ, закріплених у Стратегії НАТО щодо ШІ 2021 року та подальшому оновленні 2024 року. Ці документи інституційно пов'язують технічні стандарти, людський контроль, випробування, правову відповідність і взаємосумісність у єдину політику оборонного застосування [100; 101]. У Великій Британії інституційними вузлами цивільного і безпекового контуру виступають Alan Turing Institute, ICO/CDEI, NHS AI Lab, DSIT, AI Safety Institute та Defence AI Centre. У Франції таку роль виконують INRIA, CNRS, мережі AI-лабораторій, урядова політика AI for Humanity, Міністерство збройних сил, DGA та AMIAD [140; 143; 146; 151; 152; 154]. Саме через ці інституції абстрактні принципи етики, законності, прозорості та відповідальності поступово перетворюються на процедури державного управління, закупівель, випробувань, оцінки ризиків і допуску

технологій до використання в безпековій сфері спецслужбами та збройними формуваннями.

Доречно додати ще кілька вузлових ланок, які поглиблюють уже прокладену траєкторію Франції та Великої Британії від фундаментальної науки до інституційної спроможності й безпекового застосування. У Великій Британії після 2023 року науково-політичний вектор було зібрано в окрему державну інституцію: з Frontier AI Taskforce виріс постійний AI Safety Institute, покликаний проводити незалежні випробування передових моделей, розробляти протоколи оцінювання та забезпечувати доступ уряду до результатів тестів. У такий спосіб було створено техніко-правовий міст між лабораторіями, регуляторами і державними органами [158]. Офіційні матеріали уряду Великої Британії підтверджують, що AI Safety Institute було запущено 2 листопада 2023 року як державний центр тестування безпеки нових типів ШІ, а попереднім етапом була Frontier AI Taskforce.

Цей крок пов'язаний із проінноваційною рамкою Білого документа 2023 року та урядовою відповіддю 2024 року, де закладено п'ять принципів ризик-орієнтованого регулювання і центральну координаційну функцію держави, яка має узгоджувати практики галузевих регуляторів у цілісну систему без надмірного нормативного навантаження [159]. Ця модель демонструє характерну рису британського підходу: держава не встановлює одразу універсальний закон для всіх систем ШІ, а посилює спроможність існуючих регуляторів, створює державну експертизу, вводить протоколи тестування, підтримує інноваційний сектор і намагається впливати на міжнародний порядок денний через дипломатичні та технічні ініціативи. Для військової сфери така логіка є особливо важливою, оскільки вона дозволяє поєднати швидкість технологічної адаптації з вимогами безпеки, підзвітності і контролю.

З французького боку стратегія AI for Humanity поступово трансформувалася у політику суверенітету даних, моделей і обчислень. Поруч з академічними кластерами INRIA/CNRS з'явилися ініціативи навколо власних моделей, дата-центрів, хмарних рішень і стратегічної інфраструктури. Водночас кейс Health Data Hub і юридичні суперечки щодо розміщення державних медичних даних на хмарі нерезидента Azure

виявили напругу між інноваційністю, вимогами GDPR, європейською юрисдикцією та контролем над критичними даними [160; 161]. Цей приклад має значення не лише для сфери охорони здоров'я. Він демонструє ширшу проблему європейського регулювання ІІІ: технологічна залежність від неєвропейських провайдерів може мати правові наслідки для приватності, безпеки, суверенітету даних і стратегічної автономії. У військовій сфері ця проблема набуває ще більшої ваги, оскільки залежність від зовнішніх обчислювальних платформ, моделей або компонентів може впливати на безпеку військових операцій, захист даних, контроль над алгоритмічними рішеннями і можливість держави самостійно перевіряти систему.

Символом французької лінії стала поява Mistral AI та її суверенного позиціонування. За політичної підтримки Єлисейського палацу і партнерств із великими виробниками апаратури та інвесторами компанія перетворилася на один з інструментів консолідації французького і ширше європейського стеку для великих мовних моделей та дата-центрів, покликаних зменшити критичні залежності від неєвропейських постачальників [162]. Водночас таке позиціонування не означає відмови від міжнародної кооперації. Навпаки, французька модель демонструє спробу поєднати відкритість до глобального ринку з вимогою стратегічного контролю над критичними технологіями. У військовій сфері це перетворюється на вимогу не лише закуповувати інноваційні системи, а й мати власні механізми їхньої перевірки, пояснюваності, сертифікації, аудиту та правового контролю.

У сумі це означає, що і Велика Британія, і Франція виводять цивільну інноваційну петлю зворотного зв'язку, яка охоплює дослідження, стандарти, випробування і відповідальне впровадження, на рівень державної інфраструктури. Саме така інституційна щільність робить природним наступний крок: проєкцію напрацьованих підходів на оборону й безпеку, де вимоги до верифікації моделей, доступу держави до тестів, людського контролю, нагляду і правової оцінки вже інтегруються в оборонні стратегії та спільні рамки НАТО [153; 154; 155; 157]. У цьому контексті європейська модель відрізняється від суто технологічної логіки тим, що вона прагне вбудувати

правові гарантії не після розгортання системи, а ще на етапі її проєктування, закупівлі, навчання, тестування і допуску до експлуатації.

Ключові напрями застосування ІІІ в обороні та безпеці Франції і Великої Британії охоплюють кілька блоків. У межах цих блоків доцільно виокремити не лише загальні сфери використання штучного інтелекту, а й конкретні технологічні рішення, програми та інституційні інструменти, які демонструють практичну спрямованість європейської моделі:

- TORNADO, розвідувально-аналітичне рішення французького походження, пов'язане з обробкою геопросторових, супутникових і візуальних даних, яке використовується у логіці посилення JISR-спроможностей, тобто об'єднаної розвідки, спостереження і рекогносцировки;
- Fortion, аналітична платформа Airbus, що використовується у сфері оборонної розвідки, ситуаційної обізнаності, обробки великих масивів даних і підтримки прийняття рішень у складному оперативному середовищі;
- JISR-інтеграція, тобто інтеграція розвідувальних, спостережних і рекогносцирувальних даних у єдину систему аналізу, що має значення для скорочення часу між отриманням інформації, її алгоритмічною обробкою та подальшим командним рішенням;
- Rafale F5 + UCAV / remote carriers, напрям французького розвитку бойової авіації, що передбачає алгоритмічне підсилення пілота, взаємодію пілотованої платформи з безпілотними носіями та поступовий перехід до більш складних моделей повітряної автономії;
- MUM-T, Manned-Unmanned Teaming, тобто взаємодія пілотованих і безпілотних систем, яка у британському контексті відпрацьовується через полігонні тести, зокрема QinetiQ, і має значення для визначення меж автономії, людського контролю та розподілу відповідальності між оператором, командиром і технічною системою;
- Thales Ground Master, сенсорні та радіолокаційні рішення, пов'язані з алгоритмічною класифікацією об'єктів, підтримкою протиповітряної оборони,

обробкою сигналів і посиленням ситуаційної обізнаності в умовах високої швидкості надходження даних;

- C2-інтеграція, тобто включення алгоритмічних рішень у системи command and control, що має правове значення через вплив ШІ на інформаційну основу командного рішення, межі дискреції людини та можливість подальшої перевірки правомірності дій;

- AI Safety Institute, британський інституційний механізм тестування передових моделей ШІ, який демонструє перехід від декларативної безпеки до державної технічної експертизи, незалежного оцінювання ризиків, перевірки можливостей моделей і розроблення протоколів тестування;

- Defence AI Centre / DAIC, британський центр компетенцій у сфері оборонного ШІ, через який координуються питання впровадження ШІ у військове середовище, підготовки персоналу, взаємодії з індустрією та формування процедур відповідального застосування;

- AMIAD, французький інституційний інструмент координації оборонного штучного інтелекту, який пов'язує дослідження, випробування, закупівлі, промислові спроможності, правові гарантії і практичне впровадження алгоритмічних систем у військовій сфері;

- DGA, Генеральна дирекція з озброєнь Франції, що виступає ключовим інституційним вузлом перевірки, закупівель, тестування і допуску оборонних технологій, включаючи системи з елементами ШІ;

- JSP 936, британська техніко-правова директива, яка уніфікує вимоги до безпечного розгортання ШІ, навчання персоналу, процедурних допусків і контролю перед оперативним застосуванням;

- V&V, verification and validation, тобто верифікація і валідація систем ШІ, що охоплює перевірку правильності роботи моделі, відповідності заявленому призначенню, стійкості до помилок, якості даних і придатності для використання у конкретному оперативному контексті;

- MLOps та LLMOps, операційне управління системами машинного навчання і великими мовними моделями, що має значення для безпечного оновлення моделей, контролю їхньої поведінки, документування змін, моніторингу після розгортання та запобігання неконтрольованому використанню;
- аудит даних і моделей, який передбачає перевірку джерел даних, якості навчальних наборів, можливих упереджень, точності класифікації, кіберстійкості, пояснюваності результатів і відповідності системи вимогам прав людини та міжнародного гуманітарного права;
- простежуваність даних, моделей і рішень, що забезпечує можливість встановити, які дані були використані, яким чином система сформувала результат, хто ухвалив остаточне рішення і як може бути перевірена правомірність застосування відповідної системи;
- тести передових моделей, які у британській моделі пов'язані з AI Safety Institute та міжурядовими протоколами тестування, а у французькій моделі - з відомчими процедурами допуску, оборонною експертизою і контролем за використанням систем у критичних функціях;
- системи протидії безпілотним платформам і сенсорика ППО, що охоплюють алгоритмічне виявлення, класифікацію, супровід і пріоритизацію повітряних об'єктів, а також інтеграцію таких даних у командно-контрольні системи;
- правова експертиза систем ШІ, яка у військовій сфері має охоплювати відповідність міжнародному гуманітарному праву, оцінку меж автономії, наявність людського контролю, пропорційність, передбачуваність, технічну надійність і можливість аудиту після застосування.

Перший блок становить розвідка, спостереження, рекогносцировка, аналіз великих масивів даних і підтримка ситуаційної обізнаності. У цих сферах ШІ використовується для обробки супутникових зображень, відеопотоків, сигналів, відкритих джерел, кіберданих і розвідувальної інформації. Юридичне значення цього напряму полягає в тому, що алгоритмічні системи не застосовують силу безпосередньо, але впливають на інформаційну основу подальших рішень. Якщо система неправильно

класифікує об'єкт, не врахує контекст або відтворить упередженість даних, помилка може перейти у подальший ланцюг військового планування. Тому навіть аналітичні системи ШІ потребують перевірки, документування, оцінки точності, людського контролю і процедурного аудиту.

Другий блок охоплює системи підтримки прийняття рішень. Вони можуть використовуватися для планування операцій, логістики, розподілу ресурсів, прогнозування ризиків, оцінки маршрутів, управління запасами, медичного забезпечення і розрахунку сценаріїв. У цьому випадку ШІ не замінює командування, але впливає на швидкість, структуру і обсяг інформації, доступної для військового рішення, особливо це пов'язано із діяльністю спецслужб, що займаються збором та обробкою даних. Саме тому європейські підходи дедалі більше акцентують увагу на тому, що значущий людський контроль не може означати лише формальну присутність людини в контурі. Людина повинна мати реальну можливість зрозуміти логіку рекомендації, оцінити її обмеження, відмовитися від неї, змінити її або вимагати додаткової перевірки. Без цього людський контроль може перетворитися на декларативну гарантію, яка не запобігає автоматизованому перенесенню ризику на командувача або оператора.

Третій блок становлять автономні та напіваавтономні платформи, включаючи безпілотні літальні апарати, наземні роботизовані системи, морські автономні платформи, засоби протидії безпілотникам і системи автономної навігації. Саме цей напрям найближче підводить європейські держави до дискусії про летальні автономні системи озброєнь. Франція і Велика Британія визнають застосовність міжнародного гуманітарного права до таких систем, однак відрізняються щодо бажаного рівня нормативної конкретизації. Французька позиція традиційно ближча до підтримки чіткішого нормативного закріплення людського контролю та обмежень для найбільш небезпечних автономних функцій. Британська позиція більше наголошує на застосовності чинного МГП, правовій експертизі, технічних стандартах, тестуванні і відповідальному впровадженні без негайної підтримки всеохоплюючої заборони [217].

Четвертий блок стосується кібербезпеки, інформаційних операцій, протидії дезінформації, виявлення *deepfakes*, захисту критичної інфраструктури і розпізнавання аномальної поведінки в мережах. У цій сфері ІІІ має подвійний характер: він може бути інструментом оборони, але також може посилювати наступальні кібероперації, інформаційний вплив, автоматизоване створення дезінформаційного контенту і масштабування шкідливих кампаній. Для європейської моделі це створює додаткову проблему, оскільки правове регулювання тут розташовується на перетині кіберправа, міжнародної безпеки, прав людини, захисту персональних даних, свободи вираження поглядів і воєнного права. Саме тому європейські держави намагаються поєднати технічні механізми виявлення ризиків із процедурними гарантіями, щоб протидія загрозам не перетворювалася на непропорційне обмеження прав.

П'ятий блок охоплює внутрішню безпеку, правозастосування, прикордонний контроль, біометричну ідентифікацію та автоматизоване спостереження. У Великій Британії важливе значення мала справа *Bridges v South Wales Police* 2020 року, а також позиції ІСО щодо біометрії, які встановили підвищені вимоги до законності, справедливості, пропорційності та процесуальної дисципліни при розгортанні автоматизованих засобів спостереження, що використовуються військовими та спецслужбами [182; 183; 189]. У Франції аналогічну функцію виконує CNIL, який контролює дотримання вимог щодо персональних даних, біометрії, алгоритмічної обробки та публічного сектору. Хоча ці питання не є суто військовими, вони формують ширший безпековий контекст, у якому держава навчається контролювати високоризикові алгоритмічні системи, оцінювати їхню пропорційність, встановлювати межі допустимого спостереження та забезпечувати можливість оскарження.

З огляду на зазначене, правові гарантії в європейській моделі поступово вбудовуються у цикл управління бойовими діями та ширший цикл використання високоризикових систем ІІІ. Така схема має показувати не лише технологічний конвеєр, а й точки вбудовування правових гарантій: етика, верифікація і валідація, простежуваність, аудит, людський контроль, допуск до експлуатації та незалежний нагляд. Її логіка полягає в тому, що інституції, зокрема DGA, AMIAD, DAIC і AISI, не

просто супроводжують інновації, а вбудовують тестування та допуски у цикл управління бойовими діями (Додаток 11). У такий спосіб правова оцінка перестає бути зовнішнім актом, який проводиться вже після розроблення системи, і стає частиною її життєвого циклу.

У Франції військово-правова логіка відповідального ШІ спирається на поєднання оборонної стратегії, етичних принципів і централізованого інституційного управління. Міністерство збройних сил розглядає ШІ як технологію, здатну підвищити оперативну ефективність, скоротити час аналізу даних, посилити ситуаційну обізнаність, оптимізувати логістику, підтримати планування і забезпечити перевагу в складних середовищах. Водночас французькі документи зберігають акцент на відповідальності людини, неприпустимості втрати контролю над застосуванням сили, дотриманні міжнародного гуманітарного права і необхідності етичної оцінки військових систем. У цій моделі AMIAD виступає не просто технічною агенцією, а інструментом державної координації оборонного ШІ, який має пов'язати дослідження, розробки, випробування, закупівлі, промислові спроможності та правові гарантії [153; 154; 186; 187].

У Великій Британії ключовим вузлом стала Defence AI Strategy 2022 року та подальше формування Defence AI Centre як центру компетенцій. Британська модель спирається на триєдину формулу *ambitious, safe, responsible*, що дозволяє одночасно обґрунтувати необхідність швидкого впровадження ШІ, встановити вимоги безпеки та підкреслити відповідальність за його використання [181; 182]. Практичне значення цієї моделі полягає в тому, що вона намагається уникнути розриву між політичною декларацією і технічною реалізацією. Відповідальність у ній не обмежується загальними принципами, а повинна бути переведена у процедури навчання персоналу, оцінки даних, тестування моделей, правового огляду, контролю якості, управління ризиками, моніторингу після впровадження і перегляду системи у разі зміни оперативного контексту.

Обидві юрисдикції зближуються у трьох принципових моментах. По-перше, стратегічні документи перекладаються на технічні процедури верифікації та валідації, журнали рішень, тестові протоколи, вимоги до документації і правила допуску до

експлуатації. У Франції це відбувається через AMIAD, DGA та етичні висновки; у Великій Британії, через DAIC, AISI і внутрішні керівництва типу JSP 936 [153; 154; 155; 171; 174-180]. По-друге, значущий людський контроль у критичних функціях закріплюється як імператив оборонної політики із посиланням на застосовність міжнародного гуманітарного права, що структурно обмежує автономність у рішеннях щодо застосування сили [153; 154; 171]. По-третє, секторальна модель нагляду, яка включає CNIL, ICO, медичні, транспортні, кібербезпекові та інші регулятори, у поєднанні з міжнародними стандартами управління ризиками формує практичну конституцію ШІ, від даних і тренування до розгортання, моніторингу, незалежного перегляду й оскарження [155; 159; 182-187].

Ключові політичні фігури також мають значення для розуміння європейської моделі. Франція демонструє політичну центровість ШІ: імпульс зверху задає президент Емманюель Макрон, для якого ШІ інтегровано у ширшу доктрину технологічного суверенітету та індустріального перезапуску. Саме з його ініціативи у 2018 році оголошено пакет інвестицій і першу національну стратегію AI for Humanity, що зафіксувала державні пріоритети та механізми фінансування досліджень і стартапів [185]. На безпековому векторі ключову роль відіграє міністр збройних сил Себастьєн Лекорню. У 2024 році під його політичним кураторством Міністерство збройних сил формалізувало єдину рамку з питань ШІ, оприлюднило міністерську стратегію, запустило AMIAD та розгорнуло інституційні процеси для координації науково-дослідних і дослідно-конструкторських робіт, випробувань та впровадження алгоритмічних систем у видах військ [186; 187].

Паралельно французький уряд закріпив ресурсну базу цієї політики: виділення цільових коштів на обчислювальні потужності, зокрема суперкомп'ютер для оборонних потреб, та перерозподіл фінансування на проєкти з військового ШІ підтверджують зсув від пілотних проєктів до більш системного використання [188]. На рівні європейських та міжнародних дискусій французька позиція є нормотворчою. Париж просуває етичні обмеження, наполягає на значущому людському контролі, а у політичній риториці оборонне відомство артикулює амбіцію лідерства Франції у військовому ШІ та

побудову суверенних спроможностей, у тому числі через AMIAD [189]. Сукупно це формує зв'язку Єлисейський палац, Міністерство збройних сил, AMIAD, DGA, де політичні цілі транслюються в організаційні інструменти, бюджетні рішення і процедури впровадження [186-189].

У Великій Британії ШІ також винесено на рівень прем'єрської політики. Прем'єр-міністр Ріші Сунак у 2023 році ініціював глобальний AI Safety Summit у Блетчлі-Парку і публічно закріпив формат багатостороннього обговорення ризиків frontier AI. Результати цього процесу, зокрема Bletchley Declaration, запуск національного AI Safety Institute та пропозиція глобальної наукової панелі, стали маркерами британського лідерства у м'якому міжнародному врядуванні ШІ. Усередині оборонного відомства стратегічний курс визначила Defence AI Strategy від 15 червня 2022 року і практичні настанови Defence AI Playbook 2024 року, які інституціоналізували підхід амбіційності, безпеки і відповідальності та запустили операційний центр компетенцій DAIC для координації впровадження ШІ у видах збройних сил, спільних програм з індустрією та науковцями, а також уніфікації навчання персоналу [181; 182].

На рівні розвідувального співтовариства, у межах якого важливу роль відіграють спецслужби, акценти позначив директор GCHQ Джеремі Флемінг, який у публічних зверненнях 2021 року підкреслив, що ШІ стає критичним чинником національної безпеки, особливо у контексті протидії кіберзагрозам, дезінформації, інформаційним операціям і технологічній конкуренції [183; 184]. Подальша парламентська наглядова рамка, зокрема звіт Комітету з оборони про спроможності у сфері ШІ від січня 2025 року та урядова відповідь від квітня 2025 року, деталізували роль DAIC як центру гравітації для оборонного ШІ та окреслили вузькі місця інтеграції між видами військ. Це підтвердило поступову, але системну інституціоналізацію оборонного ШІ у британській моделі [7; 13]. Разом ці приклади відображають різні стилі політики, але спільну логіку: персоніфікований політичний мандат, швидке створення або посилення профільних інституцій, підкріплення ресурсом і технічними стандартами, а також зовнішню проєкцію через міжнародні ініціативи, нормативні декларації, безпекові рамки і наукові панелі [181-189].

На глобальному рівні Франція та Велика Британія послідовно інституціоналізують правила відповідального використання ІІІ в обороні через НАТО, формати REAIM і дискусії в ООН/CCW. У НАТО рамкові орієнтири задано Стратегією НАТО щодо ІІІ 2021 року, яка закріпила стратегічні цілі, вимоги до взаємосумісності та безпечної інтеграції цифрових засобів у цикл прийняття рішень, а також проголосила принципи відповідального використання, зокрема відповідальність, відстежуваність, надійність і керованість людиною для всіх союзників [206; 207]. Операційне підкріплення становлять інноваційні інститути Альянсу, зокрема мережа випробувальних центрів DIANA та NATO Innovation Fund, які фінансують подвійні й оборонні застосування, у тому числі з компонентами ІІІ, сприяючи вирівнюванню технічних вимог і процедур оцінювання ризиків між національними відомствами оборони [208; 209].

На майданчику REAIM, Гаага 2023 року і Сеул 2024 року, обидві держави підтримали політичні документи щодо відповідального використання ІІІ та автономії у військових цілях. Паралельно США висунули Політичну декларацію про відповідальне військове застосування ІІІ та автономії, до якої поступово приєднуються партнери. Ці тексти кодифікують вимогу людського контролю, прозорості тестувань і підзвітності, фіксуючи спільний знаменник практик ще до появи обов'язкових договорів [210; 211]. У цьому значенні REAIM виконує для європейських держав подвійну функцію. З одного боку, він дозволяє просувати власні підходи до відповідального військового ІІІ. З іншого боку, він створює міжнародне середовище, де європейські принципи, такі як правова відповідність, людський контроль, управління ризиками і гуманітарна чутливість, можуть бути перекладені мовою ширшого глобального консенсусу.

У 2023 році Велика Британія ініціювала Саміт із безпеки ІІІ та Блетчлійську декларацію, політичний акт 28 країн про ризики frontier systems і доступ держав до їхнього безпекового оцінювання. Цей документ фактично підсилює вектор технічних аудитів і урядового нагляду над моделями найвищого ризику [212]. Офіційні британські джерела підтверджують, що AI Safety Institute створювався саме як інструмент

розвитку урядової технічної експертизи для оцінювання можливостей і ризиків advanced AI systems. Для військової сфери це має непряме, але важливе значення. Якщо держава формує спроможність незалежно тестувати передові моделі у цивільному і загальнобезпечовому контурі, то аналогічні підходи можуть бути адаптовані до оборонних систем, де наслідки помилки є значно серйознішими.

На майданчику ООН, у Групі урядових експертів CCW щодо автономної зброї, позиції Парижа і Лондона розходяться у ступені жорсткості правового закріплення. Франція, у зв'язці з низкою європейських країн, наполягає на нормативному закріпленні значущого людського контролю та обмеженнях для летальних автономних систем. Велика Британія, подібно до США, акцентує на застосовності чинного міжнародного гуманітарного права і першочерговості технічних стандартів, прозорості тестувань та правової експертизи без негайного запровадження всеосяжної заборони [217]. Така різниця не означає відсутності спільного підходу. Навпаки, вона демонструє внутрішню багатоваріантність європейської моделі: одні держави тяжіють до більш чіткої договірної кодифікації, інші, до поетапної юридизації стандартів і процедур. Обидва підходи, однак, визнають, що автономні системи не можуть бути виведені за межі міжнародного гуманітарного права.

На рівні Європейського Союзу, що прямо релевантно для Франції і опосередковано важливо для Великої Британії як близького партнера європейського безпекового простору, ухвалений у 2024 році ризик-орієнтований Акт про ШІ містить чітке виключення для систем, призначених винятково для військових і оборонних цілей [213]. Це положення має принципове значення. Воно свідчить, що ЄС не намагається прямо регулювати суто військові системи через загальний цивільний акт про ШІ. Водночас цивільні та подвійні застосування у Франції підпадають під вимоги Акта, а суто військові регулюються національними документами з урахуванням міжнародного гуманітарного права і союзницьких стандартів НАТО [213]. Такий підхід підтверджує, що європейська модель регулювання військового ШІ формується не через одну норму, а через розмежування сфер: цивільний ШІ, високоризикові системи, подвійне

використання, військові системи, автономні функції, кібербезпека та оборонні закупівлі.

Відповідно Париж розгортає власну міністерську стратегію 2024 року і спеціалізоване агентство AMIAD для координації оборонного ШІ, а також етичні принципи й керівництва, що імплементують людину в контурі та перевірку відповідності міжнародному гуманітарному праву у процедурні вимоги закупівель і тестувань [215; 216]. Лондон через стратегічну лінійку Міністерства оборони, формулу *ambitious, safe, responsible, DAIC*, базові інструкції типу JSP 936 і AI Safety Institute інституційно зводить до купи вимоги якості, безпеки та контролю впродовж життєвого циклу оборонних ШІ-рішень [214]. Це дозволяє зробити висновок, що у британській і французькій моделях право не відділяється від техніки. Навпаки, правові принципи мають бути перекладені у технічні процедури, а технічні процедури повинні створювати докази правової відповідності.

Саме тому важливим є порівняльне узагальнення французької і британської моделей (Додаток 10). Франція демонструє підхід, у якому стратегічний суверенітет, державне фінансування, оборонна промисловість, етична експертиза і централізована інституційна координація утворюють єдину рамку. Велика Британія демонструє підхід, у якому проінноваційне врядування, секторальні регулятори, AI Safety Institute, Defence AI Centre, Блетчлійський процес і орієнтація на тестування передових моделей формують більш гнучку, але не менш інституціоналізовану модель. У першій моделі сильнішим є акцент на суверенітеті та оборонній автономії. У другій, на технічній експертизі, міжнародній модерації і ризик-орієнтованому регулюванні. У міжнародно-правовому вимірі обидві моделі є комплементарними, оскільки одна тяжіє до нормативного закріплення меж автономності, а інша, до вироблення перевірюваних процедур безпеки, які можуть бути прийняті партнерами.

Окремого значення набуває питання подвійного використання. Європейська модель виходить з того, що більшість сучасних технологій ШІ не є спочатку суто військовими. Великі мовні моделі, системи комп'ютерного зору, автономна навігація, прогнозна аналітика, робототехніка, кіберзахист, синтетичні дані, хмарна

інфраструктура і високопродуктивні обчислення виникають у цивільному або змішаному середовищі, але можуть бути інтегровані у військові системи. Звідси впливає потреба у правовому підході, який враховує весь шлях технології: від дослідження і навчання моделі до експорту, закупівлі, адаптації, військового тестування, оперативного розгортання та постійного моніторингу. Саме dual-use природа робить європейський підхід особливо складним, оскільки одна і та сама технологія може одночасно підпадати під правила захисту даних, експортного контролю, кібербезпеки, військових закупівель, міжнародного гуманітарного права і стандартів відповідального ШІ.

У цьому контексті особливого значення набуває життєвий цикл системи ШІ. Для європейської моделі недостатньо перевірити систему лише на етапі її закупівлі або разового тестування. Потрібно оцінювати якість даних, мету розроблення, архітектуру моделі, процес навчання, валідацію, можливі упередження, кіберстійкість, пояснюваність, сценарії відмови, можливість людського втручання, процедури оновлення, умови оперативного застосування і постійний моніторинг після розгортання. У військовому домені ці елементи мають бути пов'язані з правовою експертизою відповідно до міжнародного гуманітарного права. Особливо це стосується систем, які впливають на вибір цілей, пріоритизацію об'єктів, оцінку шкоди цивільним особам, прогнозування поведінки противника або автоматизовану підтримку рішення про застосування сили.

Саме тут формується спільне нормативне ядро європейської моделі. До нього належать законність, підзвітність, людський контроль, верифікація, валідація, аудит, простежуваність, управління ризиками, захист даних, недискримінація, пропорційність, кіберстійкість і правова експертиза протягом життєвого циклу системи. Ці вимоги не завжди мають форму юридично обов'язкової міжнародної норми. Часто вони існують як політичні стандарти, технічні настанови, етичні принципи, відомчі правила, критерії закупівлі або практики регуляторів. Однак їхня повторюваність у документах ЄС, Ради Європи, НАТО, національних стратегіях

Франції і Великої Британії, а також у процесах REAIM і CCW свідчить про поступову юридизацію відповідального військового ІІІ.

У цьому процесі важливо не ототожнювати юридизацію з негайним прийняттям універсального договору. Європейський досвід показує, що міжнародно-правове регулювання може формуватися через накопичення процедурних стандартів, які спочатку мають м'який характер, але згодом стають практичними критеріями належної поведінки держави. Якщо держава впроваджує систему військового ІІІ без тестування, без документації, без оцінки ризиків, без можливості людського втручання і без правової експертизи, то навіть за відсутності спеціального договору може виникати питання про порушення чинних міжнародно-правових обов'язків. У цьому сенсі процедурна відповідальність стає одним із головних напрямів розвитку майбутнього режиму військового ІІІ.

Водночас європейська модель має об'єктивні межі. По-перше, вона не є повністю уніфікованою. Франція, Велика Британія, Німеччина, Нідерланди, держави Північної Європи та інші європейські країни мають різні правові традиції, оборонні спроможності, технологічні ресурси і політичні підходи до автономії. По-друге, Європейський Союз прямо не регулює суто військові системи через AI Act, тому національні оборонні підходи зберігають значний простір автономії. По-третє, НАТО створює союзницькі стандарти, але вони не мають універсальної сили для всіх держав світу. По-четверте, міжнародні дискусії в межах ООН/CCW досі не призвели до прийняття всеохоплюючого договору щодо летальних автономних систем озброєнь. По-п'яте, стрімкий розвиток генеративного ІІІ, автономних платформ і військово-цивільних технологій постійно випереджає темп нормативної конкретизації.

Попри це, європейська модель має важливе значення для становлення міжнародно-правового регулювання військового ІІІ. Вона демонструє, що регулювання новітніх військових технологій не може обмежуватися заборонаю або дозволом. Потрібна складніша структура, яка поєднує принципи, інституції, процедури, технічні стандарти, етичну експертизу, правовий контроль, людський нагляд і міжнародну координацію. Французький підхід показує, як держава може

будувати оборонний ШІ як елемент технологічного суверенітету і стратегічної автономії. Британський підхід показує, як можна формувати гнучку систему тестування, нагляду і міжнародного обговорення ризиків передових моделей. Разом вони створюють європейський внесок у майбутній міжнародно-правовий режим військового ШІ.

Отже, європейські підходи до міжнародно-правового регулювання використання технологій штучного інтелекту у військовій та безпековій сферах слід розглядати як конвергентну, але не однорідну модель. Франція тяжіє до нормативного лідерства, державного патронажу, етичної кодифікації, технологічного суверенітету та оборонної індустріалізації. Велика Британія тяжіє до проінноваційного soft law, секторального нагляду, тестування frontier AI, розвитку державної технічної експертизи та міжнародної модерації ризиків. Обидві держави синхронізують свої підходи в НАТО, підтримують політичні рамки REAIM, беруть участь у дискусіях ООН/CCW і визнають ключове значення людського контролю, підзвітності, простежуваності, правової експертизи та відповідального застосування ШІ у військовій сфері. Саме тому європейська модель, на прикладі Франції та Великої Британії, є важливим проміжним етапом між національними стратегіями і майбутнім універсальним міжнародно-правовим режимом військового штучного інтелекту.

2.3. Далекохідні підходи до міжнародно-правового регулювання використання [технологій] штучного інтелекту у військовій та безпековій сферах

Далекохідні підходи, на нашу думку, варто розглянути на прикладі двох країн - КНР (Китайської Народної Республіки) та Південної Кореї, тобто Республіки Корея. Саме ці дві держави демонструють різні, але взаємопов'язані моделі інституціоналізації ШІ (штучного інтелекту): КНР вибудовує централізовану, державно керовану й технологічно суверенну модель, тоді як Республіка Корея формує модель "відповідального інноватора", у якій інтенсивний розвиток цифрової економіки поєднується з демократичними стандартами, міжнародною координацією та поступовою юридизацією етичних принципів. Обидві моделі мають безпосереднє

значення для міжнародно-правового регулювання військового і безпекового використання ШІ, оскільки поєднують цивільні інновації, оборонні програми, стандартизацію, дипломатичну активність і позиції щодо автономних систем озброєння.

Китай пройшов шлях від точкових індустріальних програм до всеосяжної державної стратегії розвитку штучного інтелекту. У липні 2017 р. Державна рада ухвалила "План розвитку ШІ нового покоління" (新一代人工智能发展规划), який закріпив триступеневі цілі: до 2020 р. - наздогнати провідні країни, до 2025 р. - здійснити прориви світового рівня, до 2030 р. - посісти провідне місце у світі [207; 218]. План визначив штучний інтелект як стратегічну технологію для інновацій та національної безпеки й сформував модель, де центральна влада задає орієнтири, а провінції та приватні корпорації несуть основний тягар реалізації [218]. У цьому аспекті китайський підхід від самого початку мав не лише економічний, а й безпековий характер, оскільки розвиток ШІ розглядався як умова технологічної конкурентоспроможності, інформаційного контролю, оборонної модернізації та міжнародного впливу.

Передумови цього курсу закладено в програмі "Made in China 2025", яка визначила "інтелектуальне виробництво" одним із ключових напрямів та інтегрувала ШІ в десятирічну дорожню карту модернізації промисловості [210; 219]. У 2018 р. Міністерство промисловості та інформатизації опублікувало "Трирічний план дій" 2018-2020 рр., що деталізував розвиток автономного транспорту, робототехніки, систем комп'ютерного зору та медичних застосувань ШІ [209; 220]. Подальший етап передбачав створення "пілотних зон інновацій" у Пекіні, Шанхаї та Шеньчжені, де тестувалися алгоритми, регуляторні підходи й механізми відкриття державних даних для бізнесу [211; 221; 222]. Саме через ці зони відпрацьовувалася модель практичного регулювання: держава формує політичну рамку, місцеві органи влади створюють простір експерименту, а корпорації забезпечують швидке технологічне масштабування.

У 2021 р. ухвалено базові закони - "Про безпеку даних" (DSL, Data Security Law) та "Про захист персональної інформації" (PIPL, Personal Information Protection Law), які

стали правовою основою регулювання індустрії ШІ [223; 224]. У 2022-2023 рр. запроваджено спеціальні положення щодо алгоритмічних рекомендацій, deep synthesis, тобто технологій глибокого синтезу, та генеративних сервісів, що закріпили обов'язкове маркування контенту, вимоги до прозорості та механізми відповідальності [225-227]. У такий спосіб КНР перейшла від загальних стратегій до каскадного регуляторного режиму, у якому дані, алгоритми, контент, провайдери сервісів і платформи поступово включаються в систему державного контролю.

У 14-му п'ятирічному плані 2021-2025 рр. ШІ визначено пріоритетом поряд із напівпровідниками та телекомунікаціями, а в межах оборонної стратегії - як компонент модернізації ОПК (оборонно-промислового комплексу) і засіб забезпечення "технологічного суверенітету" [214; 228]. Дослідники Джеффри Дінг і Тай Мін Чеунг підкреслюють, що цей план означає не лише декларацію, а й безпрецедентне масштабування фінансування фундаментальних досліджень, розбудову національних лабораторій та пришвидшення трансферу технологій [228]. Важливо, що китайська модель не розмежовує різко цивільний і військовий виміри ШІ. Навпаки, вона виходить із того, що інноваційні прориви в цивільному секторі мають бути придатними для оборонної модернізації, а оборонні потреби, у свою чергу, стимулюють розвиток даних, сенсорів, обчислювальних потужностей і автономних систем.

Китай офіційно визначає "інтелектуалізацію" (智能化) збройних сил одним із ключових напрямів модернізації. У Білій книзі з оборони 2019 р. прямо зазначалося, що новітні технології, зокрема штучний інтелект, автономні системи, великі дані, змінюють характер війни, і НОАК (Народно-визвольна армія Китаю) має "прискорити інтелектуалізацію" своєї підготовки та озброєнь [229]. Цей курс спирається на політику "військово-цивільної інтеграції" (军民融合), яка дозволяє залучати до оборонних програм ШІ провідні приватні компанії. У розробках беруть участь державні гіганти, зокрема NORINCO (China North Industries Corporation) та AVIC (Aviation Industry Corporation of China), а також нові приватні стартапи. Китайські підприємства демонструють безпілотні платформи для всіх середовищ: від роїв дронів до автономних

підводних апаратів. У 2020 р. компанія Ziyuan представила дрони-камікадзе з елементами рою та комп'ютерного зору [230].

На полігонах НОАК проводяться випробування роїв БпЛА (безпілотних літальних апаратів), що координуються ІІІ-алгоритмами, тоді як корпорації AVIC та NORINCO демонструють прототипи "розумних" танків і бойових роботів [231]. Паралельно ІІІ інтегрується у системи командування та управління боєм: формується "єдина інформаційна платформа", що аналізує дані у реальному часі й формує рекомендації для командирів [232]. Відомо про китайські проєкти створення алгоритмів для підтримки бойових рішень, тобто своєрідних "цифрових радників штабів" [233]. Для міжнародного права це має окреме значення, оскільки алгоритмічна підтримка командування створює новий рівень посередництва між людиною-командиром, даними, автоматизованою аналітикою і фактичним рішенням про застосування сили.

Окремий напрям становлять автономні системи ураження. Китай є одним із світових лідерів у розробці автономних ударних дронів і ракет з елементами самонаведення. Моделі серій CH (Caihong) і Wing Loong можуть діяти в напіваавтономному режимі, використовуючи комп'ютерний зір і алгоритми розпізнавання цілей [234]. За даними SIPRI (Stockholm International Peace Research Institute, Стокгольмський міжнародний інститут дослідження проблем миру) та HRW (Human Rights Watch), Китай поряд із США, Росією, Ізраїлем та Південною Кореєю активно розвиває різні види автономної зброї, незважаючи на публічну підтримку ідеї обмеження повністю автономних систем [59; 63; 235]. Саме ця двоїстість, тобто поєднання дипломатичної підтримки обмежень із практичним розвитком автономних військових спроможностей, є однією з ключових рис китайського підходу.

Серед ключових акторів варто назвати генерала Лю Гоцзі (刘国治), колишнього голову Науково-технічної комісії Центральної військової ради, який наголошував: "Хто володіє штучним інтелектом, той отримає перевагу на полі бою" [236]. У 2018 р. за особистою ініціативою Сі Цзіньпіна при Центральній військовій раді створено спеціальний підрозділ з інтеграції високих технологій у армію [229]. Таким чином, КНР

цілеспрямовано трансформує НОАК у напрямі "інтелектуальної війни": основними елементами стають безпілотні платформи, алгоритмічна обробка розвідданих і високий рівень автоматизації ударних систем. Цей курс викликає занепокоєння міжнародної спільноти: гонка автономного озброєння за участю Китаю ставить питання про межі допустимості бойової автономії та перспективи міжнародного контролю [59; 67; 235].

У Китаї діє модель "державні орієнтири - приватна реалізація - регіональні пілоти", закріплена в Плані розвитку III нового покоління 2017 р. та подальших рішеннях MOST (Ministry of Science and Technology, Міністерство науки і технологій КНР) про Національні відкриті інноваційні платформи III, AIOIP (Artificial Intelligence Open Innovation Platforms): Baidu - автономне водіння, Alibaba Cloud - "розумне місто", Tencent - медична візуалізація, iFlytek - мовні технології, SenseTime - комп'ютерний зір [218; 237-238]. Цей механізм системно пронизує державні пріоритети в корпоративні дорожні карти й міські пілоти, зокрема Пекін, Шанхай, Шеньчжень [221-222].

Приклад "розумного міста": ET City Brain від Alibaba Cloud у Ханчжоу - алгоритмічне керування світлофорами, аналітика потоків, оперативне реагування; за офіційними матеріалами Alibaba Cloud, пілоти зменшували затори та пришвидшували виявлення інцидентів [239]. У медичній сфері Tencent просуває Miying, тобто інструмент підтримки діагностики, зокрема передракових станів шийки матки, а YouTu Lab демонструє результати у сегментації печінки та пухлин [241]. Для автономного транспорту діє Baidu Apollo, open-platform із стеком perception, prediction, planning, симуляціями, HD-картами, пайплайнами для роботаксі та мінібусів [240]. У мовних технологіях iFlytek, заснована Лю Цінфенгом, перетворилася на індустріальний стандарт розпізнавання і синтезу китайської мови та вивела на ринок екосистему продуктів і LLM-лінійку Spark (large language model, велика мовна модель) [242]. У споживчих і dual-use БПЛА глобальну частку зберігає DJI, заснована Франком Ваном, або Ван Тао, виробник, який стимулює "просочення" комп'ютерного зору та навігації в масовий сегмент [243].

Сегмент комп'ютерного зору представляють компанії-"єдинороги" SenseTime, співзасновники Тан Сяо'оу і Сюй Лі, Megvii, співзасновники Інь Ці, Тан Веньбін, Ян

My, CloudWalk та Yitu, співзасновник Чжу Лунг; їхні стеки охоплюють розпізнавання облич/об'єктів, відеоаналіз, "смарт-сіті" та прикладні рішення для безпеки [238; 244-246]. Масштабне впровадження відеоаналітики та FR (facial recognition, розпізнавання облич) у державних сервісах одночасно підсилило правозахисний порядок денний: ризики упередженості, помилкових ідентифікацій, необхідність прозорості й підзвітності. У цьому аспекті китайська модель демонструє, що технологічна ефективність у сфері громадської безпеки може супроводжуватися суттєвими ризиками для приватності, свободи пересування, свободи вираження поглядів і недискримінації.

Оркестрація екосистеми (об'єднання систем) відбувається через пілотні зони інновацій ШІ, відкриття даних, тестові режими, спільні лабораторії ЗВО (закладів вищої освіти) й індустрії, та державне призначення "чемпіонів" під окремі домени, АІОІР. Такий розподіл ролей підтримує швидке масштабування сервісів, зокрема міське керування, фінанси, е-комерція, охорона здоров'я, і зменшує транзакційні витрати інтеграції ШІ [218; 221-222; 237-240].

Правове та етичне регулювання

Китай досить тривалий час дотримувалась підходу, який визначається як "інновації попереду регулювання", однак із 2019 року в країні почала формуватись багаторівнева система норм етики та права ШІ. У червні 2019 р. Міністерство науки і технологій КНР оприлюднило "Принципи управління ШІ нового покоління" (新一代人工智能治理原则), підготовлені групою експертів під керівництвом Чжан Яоцю та інших. Вони закріпили 8 принципів: гармонія, справедливість, інклюзивність, приватність, безпека, контрольованість, спільна відповідальність, довіра [247, с. 3-4].

У вересні 2021 р. Національний комітет з управління ШІ затвердив "Кодекс етичних норм для ШІ" (新一代人工智能伦理规范), який визначає 6 базових цінностей: підвищення добробуту людини; справедливість і неупередженість; захист приватності та безпеки; контрольованість і довіра; відповідальність; етична грамотність і самодисципліна [248, с. 6]. Документ деталізує 18 вимог для всього життєвого циклу систем ШІ, від фундаментальних досліджень і розробки до впровадження і контролю

[248, с. 7-10]. Водночас норми мають рекомендаційний характер: санкційних механізмів поки не передбачено, але очікується їхня імплементація через галузеві стандарти й сертифікацію.

Китай поступово створив каскадний режим правового регулювання: Закон про кібербезпеку 2017 р. встановив базові вимоги до мережевої безпеки й локалізації даних; Закон про безпеку даних 2021 р. установлює категорії даних, їхню "чутливість" і режими доступу [223]; Закон про захист персональної інформації 2021 р. регламентує збір, зберігання й транскордонну передачу даних [224]. На основі цих "фундаментів" вводяться секторальні норми: Правила управління алгоритмічними рекомендаціями, чинні з 1 березня 2022 р., встановлюють обов'язок прозорості алгоритмів, можливість відмови користувача, заборону маніпуляцій [225]; Положення про глибокі синтетики, січень 2023 р., встановлюють вимогу маркування deepfake-контенту та відповідальність провайдерів за недопущення фальсифікацій [226]; Тимчасові заходи з управління генеративним ШІ, серпень 2023 р., передбачають зобов'язання для розробників LLM щодо реєстрації, фільтрації забороненого контенту та гарантій "точності" [227].

Китайські фахівці також активно беруть участь у роботі ISO/IEC JTC 1/SC 42 (International Organization for Standardization / International Electrotechnical Commission, Joint Technical Committee 1, Subcommittee 42, тобто Міжнародна організація зі стандартизації / Міжнародна електротехнічна комісія, спільний технічний комітет 1, підкомітет 42 з питань ШІ); у документах КНР прямо згадується стандарт ISO/IEC 42001:2023 як орієнтир для побудови систем менеджменту ШІ [108]. У політичній риториці Пекіна акцент робиться на концепті "гармонійного ШІ" (和谐人工智能), що має "служити суспільству й не загрожувати стабільності" [247]. Особливо наголошується принцип "керованого ШІ" (可控), який вимагає збереження значущого людського контролю над алгоритмами як у цивільній, так і у військовій сфері.

Основні документи етичного та правового регулювання ШІ у КНР доцільно винести у додатки як узагальнену таблицю за період 2017-2023 років (Таблиця 5)

(Додаток 12). У ній мають бути відображені Закон про кібербезпеку 2017 р., Принципи управління ШІ нового покоління 2019 р., Закон про безпеку даних 2021 р., Закон про захист персональної інформації 2021 р., Кодекс етичних норм ШІ 2021 р., Правила управління алгоритмічними рекомендаціями 2022 р., Положення про deep synthesis 2023 р. та Тимчасові заходи для генеративного ШІ 2023 р. Такий формат дозволяє не перевантажувати основний текст, але зберегти систематизовану картину правового розвитку КНР [247-250].

Міжнародно-правовий вимір і МГП

КНР офіційно визнає застосовність міжнародного гуманітарного права до систем зі штучним інтелектом. На майданчиках ООН Китай закликав заборонити "невідповідальні" автономні системи, але у своїх офіційних пропозиціях обмежується лише заборонаю застосування повністю автономної летальної зброї, не поширюючи її на дослідження та виробництво [235; 249]. Така стратегічна двозначність дозволяє Пекіну інвестувати у військові розробки, уникаючи прямого звинувачення в ігноруванні міжнародно-правового порядку денного. Для міжнародного права це означає наявність розриву між дипломатичною риторикою про відповідальність і фактичним збереженням свободи технологічного маневру.

КНР є активним учасником Групи урядових експертів CCW (Convention on Certain Conventional Weapons, Конвенція про заборону або обмеження застосування конкретних видів звичайної зброї) і формально підтримує ідею нової угоди про LAWS (lethal autonomous weapon systems, летальні автономні системи озброєння), проте наполягає на її "обмеженому" характері [67]. Важливий сигнал - участь КНР у процесах ООН щодо військового ШІ, включно з резолюцією Генеральної Асамблеї ООН A/RES/79/239 щодо ШІ у військовій сфері та його наслідків для міжнародного миру і безпеки [114; 250]. Це засвідчує готовність до діалогу, але в практичній площині Пекін зберігає курс на власну дорожню карту розвитку військових ШІ-систем.

Китайська Народна Республіка прагне посісти позицію одного з головних архітекторів глобального врядування у сфері штучного інтелекту. Водночас офіційний Пекін діє виважено: підтримує міжнародні платформи під егідою ООН та ЮНЕСКО

(Організації Об'єднаних Націй з питань освіти, науки і культури), але утримується від участі у західних ініціативах на кшталт GPAI (Global Partnership on Artificial Intelligence, Глобальне партнерство зі штучного інтелекту), створеного країнами ОЕСР (Організації економічного співробітництва та розвитку) і G7 (Group of Seven, Групи семи) [16; 51-54].

У листопаді 2021 р. Китай підтримав ухвалення Рекомендації ЮНЕСКО з етики ШІ, першого універсального документа, який визначає принципи етичного розвитку ШІ [13; 66]. Цей крок був важливим, оскільки саме тоді США й Ізраїль не входили до складу ЮНЕСКО й не брали участі у процесі. Крім того, китайські експерти з 2020 р. беруть участь у роботі Глобальної групи експертів ВООЗ (Всесвітньої організації охорони здоров'я) з питань управління медичним ШІ, просуваючи власні підходи до використання алгоритмів у сфері охорони здоров'я.

У структурах ООН Пекін виступає одним із провідних акторів. Китай був співспонсором резолюції Генеральної Асамблеї ООН A/RES/79/239 2024 р. "Штучний інтелект у військовій сфері та його наслідки для міжнародного миру і безпеки" [114; 250]. Ця резолюція підтвердила застосовність міжнародного права й міжнародного гуманітарного права до технологій ШІ, включно з автономними озброєннями. У межах дискусій CCW Китай неодноразово подавав робочі документи, зокрема у 2021 р. запропонував "поетапний підхід" до заборони летальних автономних систем: спершу визначення спільних принципів, а вже потім - юридичні обмеження [67]. Така стратегія дозволяє КНР уникати блокування переговорів, водночас зберігаючи свободу у власних науково-технічних розробках.

КНР активно працює і у сфері міжнародної стандартизації: китайські експерти очолюють підкомітети ISO/IEC JTC 1/SC 42 з питань життєвого циклу ШІ та управління даними [70; 108]. Просування китайської термінології й технічних стандартів має подвійне значення - внутрішня уніфікація та зовнішня експансія стандартів як інструменту "м'якої сили". Пекін уважно стежить за ініціативами НАТО (Організації Північноатлантичного договору) та G7. Після Хіросімського процесу G7 з ШІ 2023 р. Міністерство закордонних справ КНР виступило із заявою, що правила мають

формуватися всіма країнами на рівних, а не "вузькими клубами" [16]. У вересні 2023 р. Китай представив власну "Ініціативу глобального управління ШІ", яка була презентована Сі Цзіньпіном на саміті G77+Китай. Документ закликає створити інклюзивну міжнародну платформу з участю країн Глобального Півдня, а не лише розвинених держав [103; 115].

Варто відзначити, що у сфері міжнародної публічної дипломатії Китай діє вибірково: у 2023 р. він підписав Блетчлійську декларацію разом із близько 30 державами [49; 190-192], демонструючи готовність до діалогу у сфері безпечного розвитку ШІ. У той же час Пекін робить ставку на ШОС (Шанхайську організацію співробітництва) та БРІКС, де просуває тематику контролю над даними й інформаційною безпекою як ключовий елемент ШІ-політики.

Політика у сфері штучного інтелекту в КНР визначається особисто Сі Цзіньпіном. Він не лише включив ШІ до стратегічних національних пріоритетів, але й ініціював колективні навчання Політбюро КПК (Комуністичної партії Китаю) з питань ШІ у 2018 та 2020 роках. У березні 2023 р. створено Центральну комісію з науки і технологій при ЦК КПК, очолювану самим Сі, яка покликана централізувати управління стратегічними технологіями, включно з ШІ. На рівні уряду головним координатором залишалося Міністерство науки і технологій, яке розробило План 2017 р. і курує національні проєкти ШІ [207].

У дорадчих органах діє Державний комітет з питань нової генерації ШІ, тобто платформа для експертів і урядовців. До його складу входять провідні науковці, серед яких Ян Сюецзюнь, директор Інституту автоматики Китайської академії наук, та підприємці, зокрема керівники Baidu, Alibaba, Tencent. У військовій сфері ключову роль у впровадженні ШІ до 2021 р. відіграв генерал Лю Гоцзі, голова Науково-технічної комісії Центральної військової ради [236]. Пізніше його структуру було інтегровано в інші органи ЦВР (Центральної військової ради), що свідчить про перехід до більш централізованої моделі прийняття рішень.

У Пекіні створено Академію ШІ, BAAI (Beijing Academy of Artificial Intelligence), яку очолює Чжан Хунцзянь. Вона стала центром досліджень та формування політики,

зокрема у 2019 р. ініціювала "Пекінські принципи ІІІ" у співпраці з індустрією. Китайська академія наук відкрила спеціальні лабораторії з етики ІІІ, підтримані урядовими грантами. З-поміж бізнес-лідерів, які мають вплив на політичні процеси, варто згадати Кай-Фу Лі, колишнього президента Google China та інвестора у сфері ІІІ, Ма Хуатена, Pony Ma, з Tencent та Ма Юня, Jack Ma, з Alibaba. Вони брали участь у консультативних органах із питань цифрової економіки. Проте після кампанії 2020-2021 рр. щодо обмеження впливу техногігантів їхня роль стала другорядною, а основний акцент змістився на державні органи. На регіональному рівні діють міські комітети з ІІІ, наприклад у Шанхаї, де розробляються локальні програми "смарт-сіті" та кластерного розвитку.

Модель розвитку ІІІ у Китаї поєднує масштабність і централізацію, державно-приватне партнерство, техно-націоналізм, тобто ставку на власні чипи, алгоритми, стандарти. КНР водночас просуває концепт "керованого, гармонійного ІІІ" у міжнародних організаціях і впроваджує у себе системи, що дають безпрецедентний рівень контролю над суспільством. В оборонній сфері Пекін комбінує розвиток автономних систем з дипломатичною риторикою про відповідальність і міжнародне право. У глобальному контексті Китай діє гнучко: він підтримує резолюції ООН, підписує декларації на кшталт Блетчлійської, але водночас розбудовує власні ініціативи й просуває свої стандарти у сфері ISO/IEC. Це робить КНР одночасно партнером і конкурентом західних держав у боротьбі за визначення правил ІІІ.

Південна Корея

Південна Корея має потужний фундамент у сфері інформаційних і комунікаційних технологій, що зумовило відносно швидкий перехід до епохи штучного інтелекту. Перші кроки держави у напрямку регулювання і підтримки інтелектуальних технологій були зроблені ще у 2008 році із прийняттям Закону про інтелектуальні роботи, Intelligent Robots Development and Distribution Promotion Act, який заклав правові основи розвитку робототехніки та створив умови для появи перших "розумних" систем у промисловості та побуті [251]. Наступним етапом стала урядова програма Smart Korea 2013 р., яка була орієнтована на цифровізацію державного управління та

економіки і містила окремі елементи застосування алгоритмів для аналізу великих даних та автоматизації процесів.

Вирішальним поворотним моментом для формування системної політики у сфері ІІІ стала знаменита поразка корейського гросмейстера Лі Седоля від програми AlphaGo компанії DeepMind у березні 2016 року. Це викликало суспільний резонанс і привернуло увагу політичної еліти до необхідності державної стратегії, яка б дозволила Кореї не відставати у глобальній технологічній конкуренції [252, р. 150]. У 2017 році новообраний президент Мун Чже Ін створив Президентський комітет з Четвертої промислової революції, PCFIR (Presidential Committee on the Fourth Industrial Revolution), головним завданням якого стало вироблення дорожньої карти цифрової трансформації та розвитку штучного інтелекту. Уже в 2018 році комітет опублікував документ "Mid-to-Long-Term Master Plan for the Intelligent Information Society", що передбачав масштабні інвестиції в дослідження, освіту та інфраструктуру для ІІІ [253].

Кульмінацією цього процесу стала публікація у жовтні 2019 року Національної стратегії зі штучного інтелекту, National AI Strategy, яку представило Міністерство науки та ІКТ, MSIT (Ministry of Science and ICT). У документі було закріплено амбітну мету - перетворити Республіку Корея на одного з п'яти світових лідерів у сфері штучного інтелекту до 2030 року [254]. У 2020 році уряд прийняв план дій із реалізації стратегії, що включав створення національних центрів обробки даних, розвиток обчислювальних потужностей і формування дослідницьких кластерів. У 2021 році було засновано Урядовий комітет з питань ІІІ та ухвалено Хартію етичних принципів ІІІ, яка закріпила прозорість, підзвітність і збереження людського контролю як ключові цінності.

Подальший розвиток відбувався вже за адміністрації президента Юн Сок Йоля, який у 2022-2023 роках підтвердив курс на глобальне лідерство Кореї у сфері штучного інтелекту. У січні 2023 року до Національної асамблеї було подано законопроект "Основи ІІІ" (AI Basic Act), спрямований на створення всеосяжної правової бази. Документ передбачав регулювання безпеки алгоритмів, етичної відповідальності розробників і стандартизації у міжнародному контексті [255]. Надалі цей напрям

завершився ухваленням комплексного рамкового акта у січні 2025 р., який набуває чинності у січні 2026 р. і закріплює інституційну основу для розвитку та довіри до ШІ. Таким чином, за два десятиліття Південна Корея пройшла шлях від точкових ініціатив у сфері робототехніки та цифровізації до формування комплексної національної стратегії і нормативно-правової системи, що визначає її як одного з глобальних гравців у сфері штучного інтелекту.

Національна стратегія зі штучного інтелекту, оприлюднена урядом Республіки Корея у жовтні 2019 року, стала основоположним документом, що визначив бачення: "стати глобальним лідером ери ШІ, підвищуючи конкурентоспроможність економіки та якість життя громадян" [256]. Стратегія закріпила три головні цілі до 2030 року: по-перше, вивести країну до топ-3 світових держав за конкурентоспроможністю у сфері ШІ; по-друге, досягти економічного ефекту в 455 трлн вон, близько 380 млрд доларів США, і створити два мільйони робочих місць; по-третє, підвищити соціальну ефективність та добробут населення шляхом інтеграції ШІ у всі сектори суспільного життя [256]. Для реалізації цих цілей було визначено сто конкретних завдань, згрупованих у дев'ять стратегічних напрямів, які об'єднані у три категорії: розбудова екосистеми ШІ, інтеграція ШІ в економіку та державне управління, а також орієнтація на людину та етичні принципи [256].

Серед ключових ініціатив варто відзначити розвиток інфраструктури даних, створення національного порталу відкритих даних, розгортання хмарних платформ для ШІ та будівництво потужних дата-центрів для тренування моделей. Значні кошти були спрямовані на дослідження та розробки: уряд виділив 2,2 трлн вон на розробку власних AI-напівпровідників і підтримку фундаментальних досліджень [257]. У сфері регуляторної політики Корея запровадила принцип "негативного регулювання", за яким усі інноваційні сервіси дозволені, якщо вони прямо не заборонені законом [256]. У галузі підготовки кадрів планується навчити щонайменше 100 тисяч спеціалістів з ШІ, оновити освітні програми, створити шість національних дослідницьких інститутів ШІ та мережу AI-коледжів [256].

Важливим компонентом стратегії стала підтримка стартапів і підприємництва. Для цього створено Фонд інвестицій в ІІІ обсягом 1 трлн вон, а також запущено національні конкурси AI Grand Challenge, спрямовані на вирішення соціальних проблем за допомогою інноваційних алгоритмів. Паралельно держава стимулює цифрову трансформацію підприємств шляхом субсидій на впровадження ІІІ-рішень у виробництві, фінансовому секторі та сільському господарстві. У сфері державних послуг діє програма "Держава, що найповніше використовує ІІІ", за якою до 2030 року планується впровадити AI-ботів у всі центри державних послуг, автоматизувати документообіг і забезпечити переклад офіційних матеріалів двома мовами - корейською та англійською [256].

Для соціального захисту запроваджено систему "мережі безпеки робочих місць", яка включає перенавчання кадрів і страхування від втрати роботи через автоматизацію. У фінансовому плані у 2020 році уряд оголосив про виділення 1,7 трлн вон, приблизно 1,5 млрд доларів США, на реалізацію перших етапів стратегії до 2022 року. Бюджетні видатки на сферу DNA (Data-Network-AI, дані, мережі та штучний інтелект) постійно зростали: у 2021 році 1 трлн вон було спрямовано лише на розвиток інфраструктури даних [258]. Приватний сектор також активно долучився: великі корпорації пообіцяли інвестувати близько 2 трлн вон у дослідження й розробки до 2023 року [259].

Додатковим напрямом став розвиток мережевої інфраструктури для ІІІ. У лютому 2023 року уряд представив стратегію K-Network 2030, яка передбачає залучення інвестицій у розмірі 100 трлн вон, приблизно 75 млрд доларів США, у розвиток 6G-мереж та дата-інфраструктури, орієнтованих на підтримку штучного інтелекту [260]. На міжнародному рівні Південна Корея бере участь у OECD AI Policy Observatory, а також розвиває співпрацю з демократичними партнерами, зокрема Сінгапуром і Великою Британією, у сфері регулювання та етики ІІІ. Таким чином, національна стратегія Кореї вирізняється всебічністю: вона охоплює освіту, науку, економіку, правове поле, інфраструктуру та міжнародну співпрацю, що у поєднанні зі значними державними та приватними ресурсами забезпечує країні позицію одного з глобальних лідерів у сфері штучного інтелекту.

Військово-безпекове застосування ІІІ в Республіці Корея

У відповідь на ракетно-дронові загрози КНДР (Корейської Народно-Демократичної Республіки) і потребу в технологічному "мультиплікаторі сили" Сеул вибудував цілісну лінію "Defense Innovation 4.0" 2022 р., що прямо ставить ІІІ, автономні платформи та МУМ-Т (Manned-Unmanned Teaming, взаємодія пілотованих і безпілотних систем) у центр модернізації збройних сил. Офіційне бачення Міністерства оборони РК: "сильна армія, заснована на науці й технологіях", з фізичним скороченням чисельності, компенсованим інтелектуальними системами управління, розвідки, ураження і ППО/ПРО (протиповітряної / протиракетної оборони) [261].

На рівні формувань уже запущено "дроноботизацію": Армія РК створила підрозділ Dronebot Combat Unit у 2018 р. для експериментів із роями БпЛА, роботизованою розвідкою та ударними сценаріями; до 2021 р. підрозділ розширив випробування до розмінування й логістики, що підтверджено корейською національною пресою [262]. На Східному та Західному узбережжях відпрацьовуються автономні й дистанційно керовані катери для патрулювання та ППО корабельних з'єднань; на суходолі індустрія, зокрема Hyundai Rotem, Hanwha Defense, просуває багатоцільові безпілотні наземні платформи UGV (unmanned ground vehicle, безпілотний наземний апарат) з модульними сенсорами/озброєнням і функціями напівавтономного руху та супроводу, які перебувають у дослідній експлуатації Армії РК [263; 268]. На кордоні історично випробовувалися стаціонарні охоронні системи на кшталт SGR-A1 з ІЧ-сенсорами (інфрачервоними сенсорами) та автоматизованим виявленням/ідентифікацією цілей. Заявлений режим передбачав нагляд оператора з можливістю дистанційного рішення про вогонь; це один із ранніх показових кейсів алгоритмічного нагляду в зоні ДМЗ (демілітаризованої зони), зафіксований у технічній пресі ще від 2007 р. [269].

Пріоритетом є протидія маловисотним, масованим загрозам. Поряд із розвитком ракетної LAMD (Low Altitude Missile Defense, система низьковисотної протиракетної оборони) для перехоплення низьковисотних крилатих ракет і БпЛА, оборонна промисловість поставила військам перші лазерні системи ураження БпЛА, Block-I, із

автоматизованим спостереженням і супроводом цілей; постачання стартували у 2023 р., а у 2024 р. було оголошено про розгортання наступних серій і планів інтеграції в багаторівневу систему ППО міст і баз [266; 265; 264]. На авіаційному й сухопутному напрямках триває перехід до "розумних" БпЛА: від тактичного KUS-FT, офіційної MALE/тактичної платформи з розвідувальним і ударним потенціалом, до "роєвих" концептів, у яких алгоритми автономної навігації, маршрутного планування та розподілу цілей де-факто стають елементами C2 (Command and Control, командування і управління) [267]. Спільні навчання зі США, зокрема з 8-ю армією США, системно містять сценарії C-UAS (counter-unmanned aircraft systems, протидія безпілотним авіаційним системам) із використанням датчиків та ефекторів, що працюють під управлінням алгоритмів злиття даних; це підтягує інтероперабельність і випробовує "людину-в-контурі" на швидкісних "kill-chain" рішеннях [268].

Екосистема постачальників охоплює як корпорації, Hanwha, LIG Nex1, Hyundai Rotem, KAI (Korea Aerospace Industries), так і "дифенс-тех" стартапи з глибокими ІТ-компетенціями. Показовий кейс 2025 року - платформа Runway від MakinaRocks: уряд уклав контракт приблизно на 2 млрд вон на розгортання в замкнених мережах оборони для безпечної інтеграції даних, керування життєвим циклом моделей, MLOps/LLMOps (Machine Learning Operations / Large Language Model Operations, операційне управління моделями машинного навчання / операційне управління великими мовними моделями), автоматизованого моніторингу деградації й ретрейнінгу "на краю", edge, аби типові оборонні сценарії, від MUM-T і логістики до кібервиявлення, отримали стандартизовані, відтворювані AI-процеси [273; 272; 274]. Це вписується в державний портфель "Defense Innovation 100", де Runway позиціонують як унікальну платформу серед відібраних рішень, що підтверджує курс Міністерства оборони і DAPA (Defense Acquisition Program Administration, Адміністрація оборонних закупівель) на платформенізацію ІІІ-управління в обороні, зокрема автономізацію експериментів, керування версіями/даними, MLSecOps (Machine Learning Security Operations, безпекові операції для систем машинного навчання) [274; 272].

У ППО/ПРО та ближній протиповітряній обороні SHORAD (Short Range Air Defense) ключові гравці, LIG Nex1, Hanwha Systems, імплементують алгоритми комп'ютерного зору та класифікації для швидкого відбору цілей і пріоритезації ефекторів; у наземних підрозділах Hyundai Rotem просуває UGV із напівавтономним рухом і модульним озброєнням/РЕБ (радіоелектронною боротьбою) для супроводу взводів і розвідки під час обстрілів, що відображено в профільних оглядах і польових тестах з Армією РК [264; 263].

Нормативно-політична рамка безпеки й "людського контролю" у Республіці Корея має виразний міжнародно-правовий компонент. На відміну від КНДР, яка голосувала "проти", Республіка Корея підтримала першу резолюцію ГА ООН (Генеральної Асамблеї Організації Об'єднаних Націй) щодо LAWS, A/RES/78/241 у грудні 2023 р., і в подальшому подала письмовий внесок до Об'єданого звіту 2024 р., наголошуючи: центральним майданчиком має лишатися Група урядових експертів при КЗЗЗ/ССW, фокус - на ефективній імплементації МГП; РК визнає двошаровий підхід, заборони + регулювання, та необхідність "людського судження" у взаємодії "людина-машина" по всьому життєвому циклу системи, з урахуванням консенсусних формулювань GGE (Group of Governmental Experts, Групи урядових експертів) 2019 р. [270].

Як продовження зовнішньополітичної ролі "чесного брокера", Сеул у вересні 2024 р. прийняв міжнародний саміт із військового ШІ, наступник Гаазького процесу 2023 р., запропонувавши "блакитну книгу" добросовісного застосування, без створення поки юридично зобов'язуючих норм, з участю понад 90 держав і акцентом на запобіганні ухваленню "life-and-death" рішень суто машинами та на верифікації відповідності МГП [271]. За офіційним повідомленням МЗС Республіки Корея, підсумковим документом REAIM Summit 2024 став "Blueprint for Action", а незалежні аналітичні огляди зазначають, що документ підтримали близько 60 держав, що демонструє поступове, але неповне формування консенсусу навколо відповідального військового ШІ.

У ширшому цивільно-технологічному процесі РК у 2024 р. співорганізувала AI Seoul Summit і "Frontier AI Safety Commitments" для компаній; ці ініціативи є частиною комплексної лінії держави на узгодження військових і цивільних застосувань ІІІ з етикою, правом і прозорими процедурами оцінювання ризиків. Причинно-наслідкова логіка корейської моделі полягає у поєднанні кількох чинників. По-перше, демографія та противник з асиметричними засобами форсують розвиток "розумних" сенсорно-ударних ланцюгів і зменшення ризику для особового складу за рахунок UxV (unmanned systems, безпілотних систем різних доменів) і C2-автоматизації. По-друге, густо урбанізований театр бойових дій зумовлює ставку на класифікацію цілей і пріоритезацію ефекторів у реальному часі, зокрема лазери проти роїв БпЛА, низьковисотні крилаті ракети [265; 264]. По-третє, союзницька інтеперабельність зі США потребує системних C-UAS тренувань та обміну ТТХ (тактико-технічними характеристиками) і процедурами тестування алгоритмів у полі [268]. По-четверте, інституційна платформа Міністерства оборони, ADD (Agency for Defense Development, Агентство оборонного розвитку) і DAPA забезпечує перехід від "пілотів" до платформного управління моделями, Runway/Defense Innovation 100, що знімає "бутилкові горлечка" безпеки і ретрейнінгу в закритих мережах і створює основу для масштабування ІІІ в підрозділах [274; 272].

Ключові приклади військового ІІІ Республіки Корея доцільно винести у додатки як окрему таблицю, оскільки вона має систематизаційний, а не основний наративний характер (Таблиця 6) (Додаток 13). У ній мають бути відображені такі напрями: Defense Innovation 4.0, Dronebot Combat Unit, лазерне C-UAS Block-I/LAMD, тактичний БпЛА KUS-FT, UGV-сімейства, AI-платформа Runway, C-UAS інтеперабельність РК-США, охорона ДМЗ через SGR-A1, міжнародна рамка LAWS та Саміт військового ІІІ у Сеулі 2024 р. Такий додаток дозволяє зберегти щільність основного викладу і водночас показати, що корейська військова модель є не декларативною, а предметно прив'язаною до конкретних платформ, програм і міжнародних процедур [261-268; 270-274].

Ключові особи й структури, релевантні ІІІ-курсу Республіки Корея, охоплюють політичну опіку уряду в межах "Defense Innovation 4.0" від Міністерства оборони РК

[261]; промислових інтеграторів, Hanwha, LIG Nex1, Hyundai Rotem, KAI, які працюють із UGV, БпЛА, ППО та С-UAS [263; 264; 267]; інституції R&D (research and development, дослідження і розробки) та стандартизації, ADD і DAPA як замовника і тестовий полігон програм лазерної ППО/SHORAD [266; 264]; підприємницький сегмент III-платформ, MakinaRocks і програму Defense Innovation 100 [274; 272]. На міжнародній арені ключову роль відіграють МЗС (Міністерство закордонних справ) і Міністерство оборони РК, які у 2024 р. виступили хостами "сеульського" процесу щодо військового III, співзвучного з REAIM-процесом 2023 р., підкресливши застосовність МГП і потребу в практичних "запобіжниках" у ланцюзі "сенсор - шутер" [271].

Цивільне застосування III: економіка, бізнес, наука

Південна Корея належить до найбільш цифровізованих держав світу, що забезпечує сприятливий ґрунт для широкого використання III у цивільному секторі. Провідні корпорації, Samsung, LG, Hyundai, інтегрують III у свою продукцію: смартфони з голосовим асистентом Bixby від Samsung, автомобілі з автопілотом у межах платформи Hyundai Motional, побутова електроніка LG з алгоритмами передбачувального керування енергоспоживанням. ІТ-гіганти Naver та Kakao розробили власні великі мовні моделі, зокрема HyperCLOVA 2021 р., оптимізовану для корейської мови, яка використовується в чат-ботах, системах рекомендацій і пошукових сервісах [276].

Стартап-екосистема посідає 4-е місце у світі за кількістю AI-компаній: серед найпомітніших - Upstage, комп'ютерний зір, Vaiv, обробка природної мови, Lunit, AI-діагностика онкології, рішення FDA та CE-marked (маркування відповідності вимогам ЄС). За рейтингом AI 100 2022 р. четверо корейських компаній увійшли до сотні світових лідерів [277]. Це підтверджує інтегрованість корейських рішень у глобальні технологічні ланцюги.

Наукова сфера представлена такими центрами, як Сеульський національний університет, KAIST (Korea Advanced Institute of Science and Technology, Корейський передовий інститут науки і технологій), Університет Йонсей. Вони формують наукові центри світового рівня, отримують великі гранти та співпрацюють із глобальними

гравцями: у Сеулі відкрито лабораторії Google AI і Microsoft Research. Уряд інвестує у створення шести університетських інститутів ШІ та двох національних центрів суперкомп'ютерів. Приклад - проєкт Korea AI Supercomputing, 88,5 PFLOPS, 0,5 трлн вон, у партнерстві з Nebius, що має забезпечити навчання великих моделей і підтримати дослідження у фундаментальній науці [278].

Важливим напрямом є інтеграція ШІ у ключові галузі: медицина, де уряд підтримує платформу Dr. Answer для аналізу МРТ (магнітно-резонансної томографії) і клінічних даних; сільське господарство, де розвиваються смарт-ферми з прогнозуванням урожайності; урбаністика, де Smart City у Пусані та Інчхоні використовують AI-менеджмент трафіку і відеоаналітику безпеки. Окремий елемент - AI Hub, національна платформа з відкритими наборами даних і хмарними обчислювальними ресурсами для стартапів та університетів. Держава і бізнес співпрацюють у держзамовленнях: приклад - участь Naver у національній освітній програмі з персоналізованим навчанням [279]. У 2022 р. Міністерство науки та ІКТ анонсувало спільні інвестиції, 1 млрд вон на кожен з 30 відібраних проєктів, у впровадження ШІ у державні сервіси.

У сфері безпеки поліція використовує AI-CCTV (системи відеоспостереження із ШІ) у Сеулі, що попереджають про підозрілу поведінку. Корейські компанії орієнтуються на глобальний ринок: Seegene експортує AI-рішення для діагностики COVID-19 і онкології. Культура інновацій підтримується через змагання, AI ODA Challenge, та акселераційні програми для стартапів. Таким чином, цивільна модель розвитку ШІ у Південній Кореї базується на симбіозі державних інвестицій, високої цифрової інфраструктури й активного приватного сектору. Вона робить країну одним із центрів світового ШІ-ринку, здатним не лише інтегрувати глобальні розробки, а й пропонувати власні проривні рішення.

Південна Корея стала однією з перших країн Азії, яка почала формувати правові рамки для ШІ на основі демократичних принципів. У 2020 р. Міністерство науки та ІКТ опублікувало "Етичні стандарти для ШІ", що спиралися на принципи OECD (Organisation for Economic Co-operation and Development, Організації економічного

співробітництва та розвитку): людиноцентричність, прозорість, принцип "не нашкодь" та відповідальність. Хоча ці стандарти мали добровільний характер, уряд рекомендував їх до впровадження приватними компаніями [280]. У січні 2021 р. MSIT створило AI Ethics Council, який розробив практичний посібник з етичного дизайну ШІ-систем, включно з недискримінацією, захистом приватності та конфіденційності даних. У 2022 р. до Закону про захист персональних даних внесли поправки, що дозволили використовувати анонімізовані набори для навчання моделей, але водночас посилили відповідальність за витоки інформації [280].

Ключовим кроком стало ухвалення у січні 2025 р. "Основного закону про ШІ" (AI Basic Act), першого в Азії комплексного акту такого рівня [281]. Закон набуде чинності з січня 2026 р. та закріплює державну політику підтримки ШІ-індустрії; обов'язки компаній щодо прозорості, безпеки та відповідальності; ризик-орієнтований підхід через визначення "високоімпактних систем" із суворішою сертифікацією та моніторингом; створення механізму сертифікації довіри для продуктів на базі ШІ. Офіційний переклад закону в корейській правовій базі визначає його як Framework Act on the Development of Artificial Intelligence and the Creation of a Foundation for Trust, тобто рамковий акт про розвиток ШІ та створення основи довіри; переклади й аналітичні джерела підтверджують ухвалення у 2025 р. та набрання чинності у 2026 р.

Важливий нюанс: сфера оборони і безпеки вилучена з дії закону, оскільки регулюється окремими актами [281]. Паралельно уряд заснував Національний комітет з питань ШІ при прем'єр-міністрові для координації між міністерствами, а у 2025 р. запрацювала Міжвідомча консультативна група з безпеки ШІ під егідою спецслужби NIS (National Intelligence Service, Національна розвідувальна служба) та Управління нацбезпеки, що фокусується на загрозах дідфейків і кібератак [281]. Корея активно розвиває етичний вимір ШІ: уряд закріпив принцип "людиноцентричного ШІ" в усіх стратегічних документах [280]. У співпраці з ЮНЕСКО Сеул організовує азійсько-тихоокеанські форуми з етики ШІ. Державні службовці проходять обов'язковий курс AI Literacy, що охоплює питання відповідального застосування ШІ. Судова система теж

реагує: у 2022 р. вперше розглянуто справу про авторське право на AI-згенеровані зображення, де суд виходив із необхідності людського внеску для охорони твору.

Ставлення Республіки Корея до МГП та глобальних принципів має стабільно кооперативний характер. На міжнародній арені Південна Корея позиціонує себе як відповідальна технологічна держава. Вона разом зі США брала участь у розробці принципів OECD з ШІ 2019 р., а також підтримала "Заклик до дій щодо ШІ" Генерального секретаря ООН. У 2024 р. Корея приєдналася до ухвалення резолюції ГА ООН щодо військового ШІ [281]. Як учасник Конвенції про ЗОЗ/ССW, Сеул бере участь у дискусіях про LAWS з 2014 р. і послідовно заявляє: зброя, що діє повністю без контролю людини, є небажаною. Республіка Корея підтримує концепцію "значимого людського контролю" над критичними функціями озброєнь; це положення включене до "Напутніх принципів" CCW 2019 р. [280]. Водночас Сеул обережний щодо негайної юридичної заборони: делегація наполягає, що спершу необхідно виробити спільні визначення, а потім переходити до правових обмежень. У 2023 р. РК, як і США, висловилися за "кодекс поведінки" для військового ШІ як проміжний крок.

Південна Корея дуже активна на міжнародній сцені в темі ШІ. Вона є одним із засновників GPAI і приєдналася до партнерства у 2020 р., ставши одним із небагатьох членів з Азії. У лютому 2023 року Південна Корея разом із Нідерландами співорганізувала перший глобальний саміт REAIM 2023 у Гаазі. На цьому саміті понад 50 країн підтримали "заклик до відповідального використання ШІ військового призначення". Сеул став флагманом цієї ініціативи: корейські представники, МЗС і Міністерство оборони, активно заохочували інші держави приєднуватися до декларації.

У вересні 2024 р. Південна Корея прийняла другий саміт REAIM у Сеулі, розширивши діалог за участю широкого кола держав і підтримавши підсумковий документ "Blueprint for Action" про подальшу роботу над принципами міжнародного регулювання військового ШІ [271]. В ООН Корея відіграла важливу роль у просуванні резолюцій щодо військового ШІ та міжнародної безпеки, працюючи разом із Нідерландами й іншими партнерами. Це Сеул розглядає як дипломатичне підтвердження свого статусу відповідального технологічного актора.

У рамках НАТО Республіка Корея має статус глобального партнера: у 2022 р. вона вперше була запрошена на саміт НАТО, де підписала меморандум про співробітництво в новітніх технологіях. Корейські фахівці беруть участь у деяких робочих групах НАТО зі стандартів "відповідального ШІ", хоча не мають права голосу. У G7 Корея не входить, але у 2023 р. була запрошена на зустріч лідерів G7, де підтримала Хіросімський процес щодо ШІ. Також Сеул є активним членом ОЕСР і одним із перших імплементує OECD AI Principles на національному рівні. В АСЕАН+3 Корея пропонує допомогу у підготовці етичних норм для ШІ, наприклад тренінги для держслужбовців Південно-Східної Азії з політики у сфері ШІ. Загалом, Південна Корея використовує свою "м'яку силу" і технологічний авторитет, щоб мостити правила глобального ШІ, підкреслюючи баланс між інноваціями та безпекою, між розвитком та правами людини.

На державному рівні це, перш за все, Міністерство науки та ІКТ, яке формує і реалізує стратегії, керує національними проєктами через NIA (National Information Society Agency, Національне агентство інформаційного суспільства). При MSIT у 2020 р. створено Бюро з ШІ. Політичними керівниками у різні періоди були міністри науки, зокрема Чхве Гі Йон, який представив Нацстратегію, та Лі Чон Хо, який продовжив курс. Президентський комітет Четвертої промислової революції у 2017-2022 рр. очолював д-р Чан Бьон Гю, засновник SparkLabs, що забезпечило зв'язок з індустрією. З 2022 р. його замінив Комітет з цифрової стратегії при президенті Юні, де також є підкомітет з ШІ. Наукова спільнота, зокрема професори KAIST і Сеульського національного університету, консультує уряд через R&D ради.

У бізнес-секторі лідери Naver та Kakao публічно підтримували державні ініціативи і входили в робочі групи при MSIT. В оборонній сфері DAPA запустила Офіс інновацій, що включає напрям ШІ, а ADD формує технічні завдання на військові AI-системи. Спецслужби, зокрема NIS, відіграють роль у безпековому аспекті ШІ: у 2025 р. вперше NIS очолила міжвідомчу групу з AI Security, що свідчить про перехід від загальної цифрової політики до спеціалізованої політики протидії дідфейкам, кібератакам, маніпуляціям і безпековим ризикам моделей. Політику ШІ також

підтримують місцеві органи: наприклад, уряд Сеула має власну програму "Seoul AI", що включає запуск міського AI-хабу та регуляторної пісочниці.

Південна Корея демонструє модель "малої технологічної держави", яка робить ставку на ІІІ як на драйвер економіки та інструмент геополітичної ваги. Її акценти: розвиток людського капіталу, масштабна підготовка кадрів, підтримка інноваційного бізнесу, фонди, дерегуляція, та побудова довіри, етичні стандарти, правові рамки. Інструменти: національна стратегія з конкретними KPI (key performance indicators, ключовими показниками ефективності), значні бюджетні вкладення, активна дипломатія на міжнародних майданчиках. Підходи: Корея прагне балансу, вона стимулює ІІІ-стартапи для економічного ривка і водночас запроваджує правила для їх безпеки; впроваджує ІІІ в армії, але паралельно очолює заклики до відповідального використання ІІІ у війні. У порівнянні з Китаєм, корейська модель більш відкрита та людиноцентрична: держава діє у партнерстві з приватним сектором та громадськістю, базуючись на демократичних цінностях і міжнародній координації. Південна Корея фактично стала регіональним лідером у нормативному врядуванні ІІІ: її AI Basic Act 2025 р. є одним із перших подібних законів у світі, а участь у глобальних ініціативах REAIM і GPAI підтверджує репутацію "відповідального інноватора". Завдяки високій технологічній базі, 5G-інфраструктурі, електронному урядуванню і згуртованості суспільства навколо ідеї інновацій, Корея має шанси реалізувати амбітну мету - увійти до провідних світових хабів ІІІ до 2030 року.

У зіставленні КНР та Республіки Корея простежується головна відмінність далекосхідних моделей. Китайська модель є централізованою, сувереністською і безпеково орієнтованою: ІІІ включено до державної стратегії, оборонної модернізації, контролю даних і міжнародного просування стандартів. Корейська модель є кооперативною, експортно-технологічною і нормативно відкритою: ІІІ розглядається як економічний драйвер, елемент оборонної модернізації та інструмент міжнародної дипломатії відповідального використання. У міжнародно-правовому вимірі обидві держави визнають застосовність МГП до військового ІІІ, але роблять це з різними акцентами: КНР підтримує обмежений і поетапний підхід, який залишає простір для

власного технологічного розвитку, тоді як Республіка Корея намагається поєднати розвиток військового ШІ з публічною підтримкою принципів людського контролю, прозорості та міжнародної координації. Саме тому далекосхідна модель не є однорідною: вона поєднує китайський варіант керованої технологічної автономії та корейський варіант відповідального інноваційного лідерства.

2.4. Концептуальні підходи НАТО до міжнародно-правового регулювання використання штучного інтелекту у військовій сфері

НАТО (Організація Північноатлантичного договору) сформувало один з найпослідовніших у демократичному світі підходів до врядування військового ШІ (штучного інтелекту), поєднавши політичні зобов'язання, принципи "відповідального використання" та інституційну архітектуру для трансферу цих норм у практику оборонного планування. Відправною точкою стала "Стратегія НАТО у сфері ШІ" 2021 р., що закріпила роль ШІ як "технології загального призначення" для оборони та визначила рамку впровадження на рівні Альянсу й держав-членів [206]. Перша стратегія НАТО у сфері ШІ була оприлюднена 22 жовтня 2021 р. і прямо пов'язала принципи відповідального використання ШІ з цінностями, нормами та міжнародним правом Альянсу. Ключовим інструментом імплементації цієї рамки НАТО ухвалило "Принципи відповідального використання ШІ в обороні", lawfulness, responsibility and accountability, explainability and traceability, reliability, governability, bias mitigation, тобто законність, відповідальність і підзвітність, пояснюваність і відстежуваність, надійність, керованість та зниження упередженості. Вони мають застосовуватися на всіх стадіях життєвого циклу військових систем, від проектування та тестування до розгортання і виведення з експлуатації [207]. Узагальнюючи взаємозв'язок стратегії та принципів, Забара показує, що 2021-2024 рр. стали періодом інституційної кристалізації "натівського стандарту" військового ШІ: політичні документи було підсилено створенням інструментів інновацій та експертизи, а також приєднанням

НАТО до ширших міжнародних ініціатив, спрямованих на утвердження людського контролю й підзвітності алгоритмів у сфері безпеки [101].

Цей "натівський стандарт" лежить у площині сумісності з міжнародним правом і глобальними процесами в ООН (Організації Об'єднаних Націй). Принципи НАТО прямо спираються на вимогу законності та дотримання МГП (міжнародного гуманітарного права), а також на ідею значущого людського контролю, *meaningful human control*, тобто норматив, який розвивається в рамках Групи урядових експертів КЗЗЗ (Конвенції про заборону або обмеження застосування конкретних видів звичайної зброї, CCW, *Convention on Certain Conventional Weapons*) щодо LAWS (*lethal autonomous weapon systems*, летальних автономних систем озброєння) і який Альянс інтегрує у власні підходи до проєктування та застосування систем з автономними функціями [207; 217]. Дипломатичне тло цьому створила резолюція ГА ООН (Генеральної Асамблеї Організації Об'єднаних Націй) "Artificial intelligence in the military domain and its implications for international peace and security" A/RES/79/239, ухвалена 24 грудня 2024 р., що зафіксувала тематику військового ШІ в порядку денному міжнародного миру та безпеки й підштовхнула регіональні блоки, включно з НАТО, до конвергенції норм на базі МГП і людського контролю [114]. Забара констатує, що для НАТО така конвергенція проявляється двома шляхами: через власну систему принципів і настанов, які задають мінімальні пороги безпеки та підзвітності для усіх союзників; через підтримку політичних декларацій поза НАТО, як-от Декларації про відповідальне військове використання ШІ та автономії, REAIM-процес (*Responsible AI in the Military Domain*, відповідальний ШІ у військовій сфері), що окреслює "спільний знаменник" для широкої коаліції держав і сумісний із натівською рамкою [101; 210; 211].

Для того, щоб норми не лишалися "паперовими", НАТО вибудувало інституційний контур, здатний масштабувати перевірку, сертифікацію та інтеграцію ШІ-рішень у єдиний оперативний простір. Центральним елементом стала мережа DIANA (*Defence Innovation Accelerator for the North Atlantic*, Оборонний інноваційний акселератор для Північної Атлантики), тобто розподілена інфраструктура тест-центрів та акселераторів, що працює з подвійними технологіями, включно з компонентами ШІ,

і дозволяє випробовувати алгоритми, сенсори та автономні платформи під сценарії міждоперабельності НАТО [208]. Фінансову "артерію" забезпечує NATO Innovation Fund, NIF (Фонд інновацій НАТО), спеціальний інвестиційний механізм, який спрямовує капітал у критичні технологічні напрями, пов'язані з обороною, серед яких засоби штучного інтелекту, аналітика даних, автономні системи та edge-AI (обробка ШІ на периферійних пристроях) [209]. Ця пара інструментів, DIANA + NIF, забезпечує, за висновком Забари, з'єднання нормотворення з практикою: принципи відповідального ШІ проходять "через воронку" випробувань, перевірок на надійність і керованість і лише тоді піднімаються на рівень спільних спроможностей Альянсу [101; 206-209]. Показово, що перші інвестиції NIF були спрямовані саме в deep tech (глибокі технології), зокрема робототехніку, космічні технології та обчислювальні компоненти, що підтверджує практичну орієнтацію фонду на критичні технології подвійного призначення.

НАТО свідомо синхронізує свою рамку з позанатовськими політичними процесами, щоби мінімізувати регуляторні розриви між союзниками та партнерами. По-перше, союзники підтримали "Політичну декларацію щодо відповідального військового використання ШІ та автономії", запущену у 2023 р. під егідою США, яка кодифікує практики людського контролю, верифікованості та тестування і корелює з "Принципами відповідального використання" НАТО [210; 207]. По-друге, REAIM-процес, Гаага 2023 р. та Сеул 2024 р., став майданчиком, де виробляється ширший консенсус щодо етичних "запобіжників" у військовому ШІ; участь союзників у цих самітах посилила легітимність натівської рамки в очах інших регіонів [211]. За підсумками Сеульського саміту 2024 р. близько 60 держав підтримали "Blueprint for Action" щодо відповідального військового ШІ, що підтвердило зростання значення неформальних політичних документів у цій сфері. По-третє, Велика Британія як держава-союзник просунула глобальну дискусію про безпечні frontier-моделі, тобто передові моделі ШІ, Bletchley Park 2023 р., де було погоджено механізми доступу урядів до оцінювання ризиків найпотужніших систем; це опосередковано важливо і для військового виміру ШІ, з огляду на ланцюги постачання моделей і компонентів [212].

У ЄС (Європейському Союзі), зі свого боку, остаточний текст AI Act (Акту ЄС про штучний інтелект) закріпив чіткі виключення для сфер оборони та національної безпеки, що дозволяє уникати конфлікту юрисдикцій між правом Союзу і зобов'язаннями в межах НАТО, водночас залишаючи простір для добровільного вирівнювання процедур оцінки ризиків і систем управління якістю, наприклад у закупівлях подвійного призначення [213]. У сумі це створює "шов" між глобальними, європейськими та натівськими процесами, який мінімізує нормативні прогалини в критично чутливій військовій сфері [206-207; 210-213].

Внутрішня логіка натівського врядування військового ШІ є ризик-орієнтованою і життєво-цикловою. Принцип "керованості людиною", *governability*, вимагає наявності контурів аварійного вимкнення або перехоплення, *fail-safe/fail-secure*, спроможностей аудиту та відтворюваності рішень, а принцип "надійності", *reliability*, передбачає систематичні випробування у репрезентативних умовах, включно з міжвідомчими й багатонаціональними вправами [207]. Саме тому випробувальні режими DIANA, а також традиційні мережеві події на кшталт CWIX (Coalition Warrior Interoperability eXploration, коаліційне дослідження міжоперабельності бойових систем), концептуально важливі: вони дозволяють уніфікувати метрики пояснюваності, стійкості до помилок та взаємодії людина-машина до того, як здатності підуть у серійне застосування. Забара підкреслює, що "натівський" підхід робить акцент не стільки на заборонах, скільки на керованій інтеграції через політичні принципи, технічні стандарти випробувань і фінансово-інституційні механізми, які приводять ці стандарти у відповідність з оперативними потребами [101; 206-209].

Суміжний вимір становить узгодженість із правовими рамками союзників. Національні стратегії та директиви міністерств оборони, як-от підхід "Ambitious, Safe, Responsible" у Великій Британії та технічна директива JSP-936 (Joint Service Publication 936) щодо *dependable AI*, тобто надійного ШІ в обороні, фактично виступають імплементаційними "адаптерами" натівських принципів на національному рівні, забезпечуючи спільну термінологію ризиків, ролі людини, верифікації, сертифікації та *after-action* аудиту, тобто оцінювання після застосування [214; 158-160]. Така

вертикальна узгодженість "НАТО - національні політики/процедури" скорочує час від політичних декларацій до практичних протоколів застосування боездатностей, що особливо важливо в доменах ППО/ПРО (протиповітряної / протиракетної оборони), C2 (Command and Control, командування і управління) та MUM-T (Manned-Unmanned Teaming, взаємодія пілотованих і безпілотних систем), де ітеративні оновлення моделей або програмного забезпечення мають проходити під відповідним контролем і документуванням [206-207; 214].

Нарешті, натівська рамка свідомо вбудовується у ширшу "екосистему довіри". У цивільному контексті діють принципи ОЕСР (Організації економічного співробітництва та розвитку) про людиноцентричний ШІ, які багато союзників імплементували в національні політики, а на рівні G7 (Group of Seven, Групи семи) діють Hiroshima AI Process і подальші кроки до координації оцінювання frontier-ризиків. Ці сюжети не замінюють, але підживлюють військову частину, задаючи загальні ціннісні й методологічні орієнтири для розробників і регуляторів [15; 16; 212]. У підсумку, як резюмує Забара, приклад НАТО демонструє "модель відповідального озброєння ШІ": політичні норми і людський контроль, спираючись на МГП і узгоджені багатосторонні декларації, підкріплюються практичними інструментами випробувань, фінансування й інтероперабельності, що дозволяє транслювати етико-правові вимоги у реальні технічні й процедурні стандарти застосування [101; 206-211; 214-215].

Натівський підхід до військового ШІ побудований як послідовний ланцюг "принципи - процеси - інструменти - спроможності", де політичні зобов'язання трансформуються в перевірювані процедури життєвого циклу й стандарти випробувань. Базу становлять "Стратегія НАТО у сфері ШІ", яка визначає ШІ як ключовий технологічний вектор оборонної переваги та міжоперабельності, і "Принципи відповідального використання ШІ в обороні": законність; відповідальність та підзвітність; пояснюваність і відстежуваність; надійність; керованість людиною; зниження упередженості [206; 207]. У логіці цих документів саме процеси, керування ризиками, верифікація/валідація, V&V (verification and validation, верифікація і валідація), аудити та after-action оцінювання, стають "мостом" між нормами МГП і

практикою застосування автономних функцій у C2, ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance, розвідка, спостереження, виявлення цілей і рекогносцировка), ППО/ПРО, MUM-T та інших доменах [206; 207]. Узагальнюючи 2021-2024 рр., Забара показує, що Альянс окреслив інституційний контур, який дозволяє цим принципам "проходити" через випробування, інвестиції та міждержавну координацію, зменшуючи розрив між етико-правовими вимогами і бойовою доцільністю [101].

Щоб норми не лишались декларативними, НАТО поставило у центр дієві інструменти. По-перше, DIANA є мережею випробувальних центрів і акселераторів для подвійних технологій, які охоплюють алгоритми сприйняття, навігації, злиття даних і edge-AI; DIANA дає можливість перевіряти на практиці надійність, відтворюваність, explainability/traceability, тобто пояснюваність і відстежуваність, та режими "людина-в-контурі" і "людина-над-контуром" перед масштабуванням до спільних спроможностей [208; 207]. По-друге, NATO Innovation Fund забезпечує капіталізацію критичних напрямів, аналітика даних, автономні системи, засоби ШІ, закриваючи "долину смерті" між прототипом та серійним застосуванням і водночас уніфікуючи вимоги з безпеки та керованості, які впливають з натівських принципів [209; 207]. У цій комбінації, підкреслює Забара, технічні треки, V&V, T&E (testing and evaluation, випробування та оцінювання), безпека моделей, стають продовженням правових і політичних зобов'язань Альянсу, а не окремими "лабораторними" практиками [101; 206-209].

Критичним елементом є інтеграція натівських підходів у ширші багатосторонні процеси, які задають "зовнішні контури" для нормотворення. Політична декларація щодо відповідального військового використання ШІ та автономії, під егідою США, деталізує практики людського контролю, тестування і верифікації, що корелюють з "Принципами відповідального використання" НАТО. Це дає країнам-партнерам спільну мову вимог навіть поза членством в Альянсі [210; 207]. Лінія REAIM, Гаага 2023 р. і Сеул 2024 р., консолідувала міжрегіональний консенсус щодо "запобіжників" у сенсор-шутер ланцюгах і підсвітила необхідність прозорих процедур оцінювання відповідності МГП для систем із автономними функціями [211]. На рівні

універсального міжнародного права тематику військового ШІ закріплено у резолюції ГА ООН A/RES/79/239 2024 р., яка підкреслила значення людського контролю та відповідності МГП; це створює для НАТО "опорний" правовий фон, на який Альянс спирається в легітимації своїх політик [114; 206-207]. Забара акцентує: натівська рамка не прагне "перекрити" ООН-процеси за LAWS у межах CCW GGE, а навпаки імпортує вироблені там підходи щодо *meaningful human control* у свої настанови і тестові режими [101; 217]. Позиція МКЧХ (Міжнародного Комітету Червоного Хреста), що закликає зберігати ефективний людський контроль над застосуванням сили, додатково підсилює саме ті принципи, які НАТО вже формалізувало, *governability, responsibility, lawfulness*, тобто керованість, відповідальність і законність [4; 207].

Окремий блок становить правова "вбудованість" у національні структури союзників, що слугують імплементаційними "адаптерами" натівських норм. У Великій Британії стратегія "Ambitious, Safe, Responsible" розгортає вимоги щодо керованості людиною, управління ризиками і незалежного тестування для всіх *sarability lines*, тобто напрямів спроможностей, а DAIC (Defence Artificial Intelligence Centre, Оборонний центр штучного інтелекту) виступає як вузол компетенцій і практик випробувань та впровадження *across Defence*, тобто в масштабі всього оборонного відомства [158; 160; 181; 193]. Технічна директива JSP-936, "Dependable AI in Defence", кодифікує процесні вимоги, від даних і MLOps (Machine Learning Operations, операційне управління моделями машинного навчання) до V&V, експлуатаційного моніторингу, журналювання та процедур *kill-switch/abort*, тобто аварійного припинення або переривання дії системи. Тим самим *explainability, traceability, reliability* і *governability*, тобто пояснюваність, відстежуваність, надійність і керованість, стають не просто принципами, а контрактними і проєктними вимогами [159; 207]. У Франції політика "Artificial Intelligence in Support of Defence" і створення AMIAD (Agence ministérielle de l'intelligence artificielle de défense, Міністерське агентство з питань штучного інтелекту в обороні) формують "one-stop" контур для оборонного ШІ: пріоритезація задач, власність на критичні алгоритми, оцінювання безпеки та етики з обов'язковим

людським контролем; Комітет оборонної етики випускає операційні висновки щодо застосовності ІІІ у бойових сценаріях [145; 153; 186; 187; 189; 154].

На рівні ЄС "AI Act" фіксує винятки для оборони та національної безпеки, уникаючи колізії з обов'язками в межах НАТО, але водночас дозволяє країнам узгоджувати процесні практики ризик-менеджменту і систем якості в суміжних проєктах подвійного призначення [213]. Поза-натівське, але взаємодоповнювальне джерело технічних орієнтирів - "Trusted AI in Defence" від EDA (European Defence Agency, Європейського оборонного агентства): документ деталізує вимоги до trustworthiness, тобто надійності й довіреності, зокрема робастність, безпека, кіберстійкість, управління даними та життєвими циклами моделей, які легко "зчіплюються" з натівськими принципами [156; 207]. У підсумку формується вертикальна узгодженість "НАТО - національні політики - проєктні/закупівельні вимоги", яка зменшує час між політичними деклараціями та бойовою готовністю [101; 206-207; 156; 158-160; 213-215].

Міжоперабельність ІІІ-можливостей НАТО спирається і на "економіку інновацій": перевірка технологій у DIANA та їх подальший рух через NATO Innovation Fund створюють єдину "воронку" для подвійних рішень, від обробки багатоспектральних даних і цільової класифікації до автономних носіїв і edge-fusion (периферійного злиття даних) у ППО/ПРО. Це важливо не лише фінансово: інноваційна інфраструктура вбудовує процесні вимоги explainability, traceability, reliability, governability у pipeline розробника і постачальника, включно з журналюванням, валідацією даних, вбудованими circuit-breakers, тобто запобіжними механізмами зупину або обмеження дії системи, ще до потрапляння продукту у процедури закупівель союзників [208-209; 207]. Такий підхід зменшує ризики "чорної скриньки" у спільних операціях і полегшує юридичні рев'ю на відповідність МГП, у тому числі національні процедури за статтею 36 ДП І (Додаткового протоколу І до Женевських конвенцій) у доречних випадках, про важливість яких системно нагадують гуманітарні актори [62; 4; 207].

Нарешті, НАТО цілеспрямовано уникає регуляторної фрагментації з цивільними рамками довіри. Принципи ОЕСР щодо людиноцентричного ІІІ задають загальну "методологічну гравітацію" для союзників, від управління ризиками і якості даних до підзвітності, і тим полегшують зближення оборонних і цивільних підходів там, де це не суперечить виняткам для безпеки та оборони [15; 213]. Додаткову синергію з військовим виміром створює Bletchley-процес, зокрема загальний доступ урядів до оцінювання ризиків frontier-моделей і розвиток інтероперабельних підходів до red teaming/eval (стрес-тестування моделей та оцінювання їхніх ризиків), який союзники інтегрують у власні контури безпеки моделей і ланцюгів постачання ІІІ-компонентів [212; 190-192]. У сукупності це підтверджує тезу Забари: модель НАТО - це не "регуляція заради регуляції", а керований цикл практик і інститутів, які перетворюють вимоги МГП та людського контролю на вимірювані метрики якості, безпеки та підзвітності у бойових системах, узгоджені між державами Альянсу [101; 206-211; 214-215].

Операційні виклики, прогалини та напрями вдосконалення міжнародно-правових механізмів НАТО у сфері штучного інтелекту

Проблематика впровадження принципів і процедур НАТО у сфері військового ІІІ у реальний операційний контекст виявляє низку системних викликів. По-перше, ключовою проблемою залишається забезпечення прозорості алгоритмів і пояснюваності їхніх рішень у високодинамічному середовищі сучасних бойових дій. Навіть за наявності директиви JSP-936 у Великій Британії чи програмної діяльності AMIAD у Франції, складність багатомодальних систем, C2, ISTAR, ППО/ПРО, створює ризики "чорної скриньки" в ухваленні рішень, що може підірвати як правові гарантії відповідності МГП, так і довіру союзників у багатонаціональних операціях [159; 153; 101]. У цьому сенсі, як наголошує Забара, НАТО змушене поєднувати технічні практики, red teaming, adversarial testing, audit trails, тобто командне стрес-тестування, тестування на ворожі впливи та аудиторські сліди, з правовими зобов'язаннями, намагаючись уніфікувати вимірювані критерії "meaningful human control" [101; 206-207; 217].

По-друге, серйозною прогалиною залишається питання управління даними. Стандарти НАТО та національні інструкції союзників окреслюють вимоги до якості, безпеки та відстежуваності наборів даних, однак відсутня повна гармонізація процедур анонімізації, захисту персональних даних і кіберстійкості у спільних дата-центрах чи edge-середовищах. Це породжує ризики як правового характеру, наприклад конфлікт між національними положеннями щодо захисту даних та спільними операційними вимогами Альянсу, так і безпекового, у випадку зламу або маніпуляції даними противником [213; 156; 62]. НАТО намагається компенсувати ці ризики шляхом впровадження trustworthiness-критеріїв на рівні EDA "Trusted AI in Defence" і узгодженням підходів з цивільними рамками, ОЕСР, AI Act, однак відсутність єдиного міжнародно-правового інструменту ускладнює створення суцільного "ланцюга довіри" [15; 213; 156].

По-третє, викликом стає відповідальність і підзвітність у багатонаціональних операціях. У випадках, коли алгоритми ухвалюють критичні рішення, ідентифікація цілі, пріоритезація ефекторів у ППО, розподіл ресурсів у MUM-T, постає питання: хто є суб'єктом відповідальності, держава, що надала систему, чи багатонаціональне командування, що нею користувалося. МГП і прецеденти міжнародного права, зокрема імператив статті 36 ДП І щодо оцінки нових видів озброєнь, лише частково закривають цю лакуну. Як зазначає Crootoof, автономні функції створюють нову категорію "war torts", де відшкодування шкоди і притягнення до відповідальності набувають нових вимірів [7]. НАТО намагається вирішити це питання через інституційні механізми колективного аудиту та lessons learned (узагальнення вивчених уроків), але без чіткої міжнародно-правової кодифікації розподіл відповідальності залишається фрагментованим [101; 206; 62].

По-четверте, проблемним є питання адаптивності та ретренінгу моделей у закритих оборонних мережах. Приклади південнокорейської платформи Runway AI чи британських edge-тестів засвідчують: без регулярного оновлення моделей існує ризик деградації точності й підвищення вразливості до атак противника [272; 273; 159]. Проте процедури retraining, тобто повторного навчання моделей, у військовому контексті

пов'язані з ризиками втрати контролю над новими версіями, що може підірвати гарантії МГП. Тому постає потреба у формуванні стандартизованих механізмів MLOps/LLMOps (Machine Learning Operations / Large Language Model Operations, операційного управління моделями машинного навчання / операційного управління великими мовними моделями) з міжнародним наглядом. Саме на цьому акцентує Забара, наголошуючи на переході НАТО від пілотних проєктів до платформного управління моделями [101; 206-207].

Окремо слід зупинитися на взаємодії натівських підходів з глобальними ініціативами. REAIM, Гаага 2023 р. і Сеул 2024 р., та політичні декларації США і партнерів формують основу для глобального кодифікованого "кодексу поведінки" у сфері військового ШІ [210; 211]. НАТО фактично тестує ці принципи у своїй інноваційній екосистемі, створюючи прецеденти практичної імплементації. Водночас резолюція ГА ООН A/RES/79/239 2024 р. зафіксувала очікування світової спільноти щодо людського контролю та дотримання МГП у військових застосуваннях ШІ [114]. Це підкреслює ключову тезу Забари: Альянс розглядає власні принципи та DIANA/Innovation Fund як лабораторію для відпрацювання міжнародних норм, які у перспективі можуть стати основою нового правового режиму [101].

Таким чином, натівська архітектура військового ШІ - це не лише декларація принципів, а й жива система правових, технічних і організаційних інструментів. Водночас вона стикається з низкою прогалин: уніфікація управління даними, розподіл відповідальності, контроль retraining-процесів і формування глобального правового режиму. Вирішення цих викликів потребує тіснішої інтеграції між національними практиками, натівськими процедурами і універсальними рамками, зокрема ООН та МКЧХ. Перспективно саме взаємодія НАТО з ООН-процесами, CCW GGE, та глобальними ініціативами, REAIM, Bletchley, OECD AI Principles, може створити фундамент для міжнародного договору щодо автономних систем, у якому досвід і напрацювання Альянсу стануть практичним каркасом для юридичного врегулювання [101; 206-207; 214-217].

Висновки до 2-го розділу

У другому розділі здійснено порівняльно-правовий аналіз регіональних, національних і союзницьких моделей регулювання військового використання штучного інтелекту. На відміну від підходів, у яких окремо розглядаються політики США, Європи, Китаю, Республіки Корея або НАТО, у роботі ці напрями систематизовано як різні моделі правового оформлення військового ІІІ. Встановлено, що американська модель орієнтована на технологічне лідерство, відомче регулювання і практичну інтеграцію ІІІ в оборонні спроможності; європейська модель поєднує технологічний суверенітет, етичну кодифікацію, інститути тестування і ризик-орієнтований контроль; далекосхідна модель демонструє розходження між централізованим китайським підходом і кооперативною корейською моделлю відповідального інноватора; натівська модель формує союзницький стандарт відповідального військового ІІІ через принципи законності, підзвітності, керованості, надійності та інтероперабельності.

Наукове значення розділу полягає у тому, що військовий ІІІ досліджено не як сукупність розрізнених національних стратегій, а як систему регіональних правових конструкцій, які поступово наближаються до спільного нормативного ядра. Доведено, що незалежно від політичної природи держав і відмінностей їхніх правових систем у сфері військового ІІІ повторюються однакові регуляторні елементи: людський контроль, правова експертиза, верифікація, валідація, аудит, простежуваність рішень, управління даними, оцінка ризиків і відповідальність протягом життєвого циклу системи. Саме це дає підстави розглядати другий розділ як аналітичну основу для подальшого переходу від регіональних моделей до універсального міжнародно-правового рівня.

РОЗДІЛ 3. РОЗВИТОК ВІЙСЬКОВОЇ СФЕРИ ІНСТИТУТУ ШТУЧНОГО ІНТЕЛЕКТУ В РАМКАХ МІЖНАРОДНИХ КОНФЕРЕНЦІЙ І ІНСТИТУЦІЙ

3.1. REAIM: визначення засад використання штучного інтелекту у військовій сфері

Формування міжнародно-правових засад використання штучного інтелекту у військовій сфері не може бути зведене лише до діяльності окремих військово-політичних союзів, національних оборонних стратегій або дискусій щодо летальних автономних систем озброєнь. На сучасному етапі воно відбувається у складнішій площині, де одночасно взаємодіють держави, міжнародні організації, оборонна промисловість, наукові установи, технологічні компанії, експертні платформи та гуманітарні організації. Саме у цьому контексті особливого значення набуває REAIM (Responsible Artificial Intelligence in the Military Domain, відповідальний штучний інтелект у військовій сфері), який після 2023 р. перетворився на один із центральних багатосторонніх майданчиків для визначення засад відповідального використання ШІ у військовій сфері [210; 211].

На відміну від НАТО (Організації Північноатлантичного договору), яка виробляє стандарти відповідального військового ШІ в межах союзницької оборонної архітектури, REAIM має іншу правову та політичну природу. Це не організація з установчим договором, не система колективної оборони і не спеціалізований орган ООН (Організації Об'єднаних Націй). REAIM слід розглядати як глобальний політико-правовий процес, спрямований на вироблення спільного розуміння ризиків, можливостей, процедурних гарантій і майбутніх напрямів регулювання військового застосування ШІ. Його значення полягає не у створенні юридично обов'язкових норм, а у формуванні первинного консенсусу держав щодо того, що військовий ШІ вже не може залишатися поза міжнародним контролем, а його розроблення, розгортання і використання повинні оцінюватися крізь призму міжнародного права, міжнародної безпеки, гуманітарних наслідків і відповідальності людини [210; 211; 114].

Перший саміт REAIM відбувся у Гаазі 15-16 лютого 2023 р. Його організаторами виступили Нідерланди та Республіка Корея. Саміт мав принципове значення, оскільки

вперше на глобальному рівні зібрав державних представників, міжнародні організації, наукові кола, громадянське суспільство та приватний сектор для обговорення саме відповідального використання ШІ у військовому домені, а не лише вузького питання автономних систем озброєнь. Офіційний документ REAIM 2023 Call to Action був ухвалений 16 лютого 2023 р. і визначив основні напрями подальшого міжнародного діалогу щодо відповідального розроблення, розгортання та використання ШІ у військовій сфері. Уряд Нідерландів прямо зазначив, що представники урядів на саміті погодили спільний заклик до дій щодо відповідальної розробки, розгортання і використання ШІ у військовому домені [210]. Офіційна сторінка уряду Нідерландів підтверджує, що Call to Action був опублікований 16 лютого 2023 р. і стосувався саме responsible development, deployment and use of AI in the military domain.

У роботах І. М. Забари REAIM розглядається не як ізольована конференційна подія, а як елемент ширшого процесу становлення міжнародно-правових і доктринальних підходів до військового ШІ. У статті про концептуальні підходи НАТО автор наголошує, що Стратегія НАТО щодо ШІ враховувала результати REAIM 2023 і певним чином вплинула на результати REAIM 2024, оскільки обидва процеси були пов'язані із виробленням стандартів відповідального застосування технологій ШІ відповідно до принципів і норм міжнародного права та цінностей безпеки [101]. У статті про ООН І. М. Забара вказує, що міжнародні саміти REAIM 2023 і REAIM 2024 разом із іншими конференціями та брифінгами стали частиною практичних передумов, які вплинули на позицію ООН під час формування резолюції ГА ООН (Генеральної Асамблеї Організації Об'єднаних Націй) A/RES/79/239 щодо ШІ у військовій сфері [282]. Такий підхід є важливим для цього дослідження, оскільки дозволяє розглядати REAIM не лише як дипломатичний форум, а як проміжну ланку між національними стратегіями, союзницькими стандартами НАТО та універсальним рівнем ООН [101; 114; 282].

Правова природа документів REAIM є м'якою. Call to Action 2023 не створює міжнародно-договірних зобов'язань, не встановлює процедур відповідальності і не передбачає механізму примусу. Однак саме в цьому полягає його функціональна

цінність. На етапі, коли між державами ще немає згоди щодо обсягу майбутнього договору, статусу автономних систем, меж human oversight (людського нагляду), стандартів аудиту алгоритмів і відповідальності за наслідки роботи ІІІ, soft law виконує роль попереднього юридичного орієнтира. Воно дозволяє державам узгодити спільну мову, визначити зони ризику, встановити мінімальні принципи поведінки і перевірити політичну готовність до подальшої юридизації. У цьому сенсі REAIM є типовим прикладом сучасного формування міжнародного права через поступове накопичення політичних зобов'язань, експертних стандартів, декларативних формул і практик імплементації [210; 211; 282].

REAIM 2023 виходив з визнання того, що ІІІ істотно вплине на майбутнє військових операцій. У Call to Action зазначено, що військові структури дедалі активніше використовують ІІІ у різних застосуваннях і контекстах, а сама технологія відкриває значний потенціал для роботи з великими обсягами даних та поліпшення процесів прийняття рішень [210]. Одночасно документ фіксує низку ризиків: ненадійність систем ІІІ, питання людської участі, неясність відповідальності, непередбачувані наслідки та ризик ненавмисної ескалації у спектрі застосування збройної сили [210]. Отже, вихідна логіка REAIM полягає у балансі між визнанням військово-технологічної корисності ІІІ та усвідомленням його правових, гуманітарних і безпекових небезпек.

Першою засадою REAIM можна визначити застосовність міжнародного права до військового ІІІ. У Call to Action 2023 наголошено на першочерговому значенні відповідального використання ІІІ у військовому домені в повній відповідності до міжнародно-правових зобов'язань і у спосіб, що не підриває міжнародну безпеку, стабільність і підзвітність [210]. Це положення має фундаментальне значення. Воно відкидає підхід, за яким новизна технології може створювати правовий вакуум. Навпаки, REAIM виходить із того, що військовий ІІІ повинен розглядатися в межах чинного міжнародного права. Це стосується Статуту ООН, норм про заборону сили та загрозу силою, МГП (міжнародного гуманітарного права), МППЛ (міжнародного права

прав людини), норм міжнародної відповідальності держав, а також спеціальних режимів контролю над озброєннями, роззброєння і нерозповсюдження [114; 210; 282].

Другою засадою є збереження людської відповідальності. REAIM 2023 прямо визнав, що ІІІ може впливати на процес прийняття рішень, але держави мають працювати над тим, щоб люди залишалися відповідальними і підзвітними за рішення при використанні ІІІ у військовому домені [210]. Це положення має прямий зв'язок із проблемою правосуб'єктності та відповідальності у міжнародному праві. ІІІ не є суб'єктом міжнародного права і не може самостійно нести міжнародно-правову відповідальність. Тому будь-яка модель регулювання військового ІІІ повинна виходити з того, що відповідальність за його розроблення, впровадження, контроль і застосування залишаються за державами, військовими командуваннями, операторами, розробниками та іншими людськими або організаційними суб'єктами. У протилежному випадку виникла б небезпечна зона безвідповідальності, у якій технічна складність системи перетворювалася б на аргумент проти притягнення до відповідальності [210; 282].

Третьою засадою REAIM є ризик-орієнтований підхід. У документі 2023 р. зазначено необхідність оцінювати ризики, пов'язані з різними типами нинішніх і майбутніх застосувань ІІІ у військовому домені, а також із різними військовими контекстами, у яких ці системи застосовуються [210]. Це положення є особливо важливим, оскільки військовий ІІІ не є однорідним явищем. Він може використовуватися для логістики, прогнозування технічного обслуговування, розвідки, аналізу супутникових даних, кібероборони, управління безпілотними системами, підтримки командних рішень, наведення озброєнь, інформаційних операцій або ядерного командування. Очевидно, що рівень правового ризику в цих випадках різний. Тому ефективне регулювання повинно бути не формальним, а контекстуальним. Воно має враховувати функцію системи, ступінь автономності, близькість до застосування сили, можливість впливу на цивільних осіб, якість даних, передбачуваність результату та наявність людини у контурі прийняття рішення [210; 4; 67].

Четвертою засадою є обережність щодо швидкості впровадження. REAIM 2023 містить важливу формулу: несвоєчасне впровадження ІІІ може призвести до військової переваги противника, але передчасне впровадження без достатніх досліджень, тестування і гарантування безпеки може спричинити ненавмисну шкоду [210]. Ця формула точно відображає ключову дилему сучасної оборонної політики. Держави не можуть повністю відмовитися від військового ІІІ, оскільки це означало б технологічне відставання і втрату оборонних можливостей. Водночас вони не можуть впроваджувати його без належних правових і технічних запобіжників, оскільки це підвищує ризик помилкових рішень, порушення міжнародного гуманітарного права, ескалації конфлікту або втрати контролю над системами. Отже, REAIM формує модель обережної інновації, у якій швидкість впровадження має бути обмежена тестуванням, оцінкою ризиків, людським контролем і правовою перевіркою [210; 211].

П'ятою засадою є управління даними. Call to Action 2023 визначає, що дані для систем ІІІ мають збиратися, використовуватися, поширюватися, архівуватися і видалятися відповідно до міжнародного права, національних, регіональних та міжнародних правових рамок і стандартів даних [210]. Документ також наголошує на потребі механізмів захисту даних та управління якістю даних із ранньої фази проєктування, включно з отриманням і використанням навчальних даних [210]. У військовій сфері це положення має особливе значення. Дані можуть містити розвідувальну інформацію, персональні дані, біометричні параметри, геолокаційні відомості, дані про об'єкти цивільної інфраструктури, переміщення населення або поведінкові патерни. Помилки у таких даних можуть призвести до помилкової класифікації цілі, дискримінаційних наслідків або неправомірного застосування сили. Тому відповідальний військовий ІІІ починається не з моменту бойового застосування, а з моменту збору, маркування, перевірки і використання даних [210; 282].

Шостою засадою є охоплення всього життєвого циклу системи. REAIM 2023 підкреслює, що через розподілений характер військового прийняття рішень і складність систем ІІІ необхідно приділяти увагу всім стадіям розроблення, розгортання і використання ІІІ у військовому домені [210]. Це положення відрізняє

REAIM від вузьких моделей регулювання, які зосереджуються лише на моменті застосування зброї. Насправді ризики військового ШІ виникають значно раніше: під час формування технічного завдання, вибору постачальника, створення наборів даних, навчання моделі, тестування, закупівлі, інтеграції у командні системи, підготовки операторів, оновлення алгоритмів, експлуатації та виведення системи з використання. Якщо хоча б один із цих етапів не регулюється, виникає слабка ланка, через яку може бути зруйнована вся система відповідальності [210; 282].

Сьомою засадою є людський нагляд. REAIM 2023 підтверджує важливість належних запобіжників і human oversight за використанням систем ШІ з урахуванням людських обмежень щодо часу і спроможностей [210]. Це положення є тоншим, ніж проста вимога залишити людину в контурі. Воно визнає, що формальна присутність людини ще не гарантує реального контролю. Якщо система працює надто швидко, оператор не розуміє її логіки, не має достатнього часу на оцінку або психологічно схильний довіряти машинному висновку, людський контроль може стати фіктивним. Тому REAIM фактично підводить до потреби оцінювати якість людської участі: чи має людина достатню інформацію, час, повноваження, підготовку і технічну можливість змінити або зупинити дію системи [210; 4; 217].

Восьмою засадою є підготовка військового персоналу. REAIM 2023 визнає, що військові, які використовують ШІ, повинні достатньо розуміти характеристики систем, потенційні наслідки їх використання, обмеження, зокрема упередження у даних, а також потребують досліджень, освіти і тренування щодо взаємодії з системами ШІ [210]. Це положення має юридичне значення, оскільки якість підготовки оператора прямо впливає на можливість дотримання міжнародного гуманітарного права. Якщо військовий персонал не розуміє меж системи, він не може належно оцінити її рекомендацію, не може виявити помилку і не може реалізувати відповідальний контроль. Отже, належна підготовка є не лише технічною вимогою, а елементом правомірного використання ШІ [210; 282].

Дев'ятою засадою є багатосторонність і багатосуб'єктність. REAIM 2023 прямо наголошує на необхідності цілісного, інклюзивного і комплексного підходу за участю

держав, приватного сектору, громадянського суспільства та академічних кіл [210]. Причина цього полягає в тому, що значна частина технологій ШІ розробляється не військовими структурами, а приватними компаніями та науково-технічними центрами. Держава залишається головним суб'єктом міжнародного права і відповідальною стороною у військовому застосуванні технологій, але вона вже не контролює весь технологічний ланцюг одноосібно. Це створює нову регуляторну реальність, у якій приватні актори не є класичними суб'єктами міжнародного публічного права, однак фактично впливають на формування воєнних можливостей держав. Тому майбутня система регулювання військового ШІ повинна включати стандарти належної обачності для компаній, механізми перевірки постачальників, правила використання цивільних моделей у військовому контексті та процедури обміну передовими практиками [210; 211].

Десятою засадою є подолання розриву між державами. REAIM 2023 визнав, що імплементація ШІ у військовому домені відрізняється від держави до держави, а відповідальне використання потребує міжнародного та багатостороннього обміну, щоб усі держави, особливо держави, що розвиваються, могли отримувати користь від можливостей і реагувати на ризики [210]. У статті І. М. Забари про ООН цей аспект отримує подальший розвиток через аналіз резолюції ГА ООН A/RES/79/239, у якій окремо порушується необхідність подолання розривів між державами у сфері відповідального використання ШІ у військовій сфері через добровільну співпрацю, допомогу, передачу знань, обмін інформацією та передовим досвідом [282]. Це важливий елемент, оскільки без урахування нерівності технологічних можливостей міжнародне регулювання ризикує стати формальним: одні держави матимуть високотехнологічні військові системи і власні процедури контролю, а інші залишатимуться залежними від імпорту технологій без належної експертизи й можливості перевірки [210; 282].

Базові засади REAIM 2023 щодо відповідального використання ШІ у військовій сфері доцільно винести у додатки як узагальнену таблицю, оскільки її функція є систематизаційною, а не основною наративною (Таблиця 7) (Додаток 14). У ній мають

бути відображені застосовність міжнародного права, людська відповідальність, оцінка ризиків, обережна інновація, управління даними, життєвий цикл системи, людський нагляд, підготовка персоналу, багатосуб'єктність і подолання розривів між державами. Такий додаток дозволяє не перевантажувати основний текст, але зберегти логіку переходу від політичної декларації до міжнародно-правового значення відповідних засад [210; 282].

Другий саміт REAIM відбувся у Сеулі 9-10 вересня 2024 р. Його організували Міністерство закордонних справ і Міністерство національної оборони Республіки Корея. За офіційним повідомленням МЗС Республіки Корея, саміт зібрав представників понад 90 держав, які обговорили загальні підходи та пріоритети, занепокоєння і виклики, а також перспективи міжнародної співпраці [211]. У структурі саміту було три пленарні напрями: розуміння наслідків ІІІ для міжнародного миру і безпеки, імплементація відповідального застосування ІІІ у військовому домені та бачення майбутнього врядування ІІІ у військовій сфері [211]. На відміну від Гаазького саміту, який переважно формував спільне розуміння проблеми, Сеульський саміт зробив акцент на переході від принципів до практичних заходів. Офіційні матеріали МЗС Республіки Корея підтверджують, що підсумковим документом REAIM 2024 став *Blueprint for Action*, підтриманий 61 державою.

Головним результатом REAIM 2024 став *Blueprint for Action*. Цей документ був офіційно схвалений як підсумковий документ саміту. МЗС Республіки Корея повідомило, що його підтримала 61 держава, а сам документ окреслює дорожню карту встановлення норм ІІІ у військовому домені [211]. Він підкреслює, що відповідальне використання передбачає дотримання міжнародного права, збереження людської відповідальності і підзвітності, забезпечення надійності й довіри до ІІІ, підтримання належної людської участі та поліпшення пояснюваності ІІІ [211]. Це свідчить про еволюцію REAIM від декларативного заклику до більш структурованої рамки майбутнього управління військовим ІІІ. Reuters також повідомляв, що документ підтримали близько 60 держав, а Китай не приєднався до його підтримки, що додатково

засвідчує політичну вагу і водночас неповний характер консенсусу щодо військового ІІІ.

Порівняння REAIM 2023 і REAIM 2024 дозволяє визначити важливу динаміку. У 2023 р. головним завданням було зафіксувати наявність проблеми, визнати ризики, закликати до інклюзивного діалогу і визначити мінімальні принципи відповідального використання. У 2024 р. фокус змістився до розроблення дорожньої карти, перетворення принципів на практичні заходи, конкретизації людського контролю, пояснюваності, надійності, міжнародної співпраці та майбутнього врядування. Тому REAIM можна розглядати як процес, що рухається від політичного усвідомлення до операційної нормативності. Він ще не створює юридично обов'язкової системи, але поступово формує елементи, без яких така система не зможе виникнути [210; 211; 282].

Еволюцію REAIM від Гааги 2023 р. до Сеула 2024 р. доцільно відобразити в окремій таблиці, винесеній у додатки (Таблиця 8) (Додаток 15). У ній необхідно зіставити дати, організаторів, основні документи, ключовий акцент, правову природу, суб'єктний підхід, розуміння людського контролю, роль даних, зв'язок із міжнародним правом і перспективу подальшої юридизації. Така таблиця показує, що REAIM є не одноразовою конференцією, а послідовним процесом формування засад відповідального військового ІІІ [210; 211; 282].

REAIM 2024 також засвідчив, що питання військового ІІІ вже не обмежується проблемою автономного летального ураження. У порядку денному саміту були наслідки ІІІ для міжнародного миру і безпеки, поширення зброї масового знищення, відповідальне застосування, технічні підходи до імплементації політики, а також демонстрація практичних військових застосувань ІІІ [211]. Отже, REAIM охоплює широкий військовий домен: від аналітичних систем і decision-support systems (систем підтримки прийняття рішень) до автономії, кібербезпеки, контролю над озброєннями, інформаційних операцій і можливих впливів на стратегічну стабільність. Це є принциповою відмінністю від дискусій у межах К333/CCW, які здебільшого фокусуються на летальних автономних системах озброєнь. REAIM не замінює ці дискусії, але розширює їхній горизонт [67; 210; 211].

У межах дослідження REAIM варто розглядати як один із механізмів подолання "білих плям" міжнародно-правового регулювання військового ІІІ. Міжнародне право перебуває на етапі формування концептуальних рамок регулювання ІІІ у військових цілях, а заповнення прогалів можливе через багаторівневу систему: узгодження визначень, створення динамічних процедур перевірки, встановлення відповідальності та запровадження міжнародних механізмів прозорості [282]. REAIM саме й виконує цю підготовчу функцію. Він не вирішує всі питання, але створює простір, у якому держави можуть поступово домовлятися про зміст відповідального використання, межі людського контролю, вимоги до даних, процедурну підзвітність і форми міжнародної співпраці [210; 211; 282].

Особливе значення REAIM полягає у зв'язку з резолюцією Генеральної Асамблеї ООН A/RES/79/239 від 24 грудня 2024 р. У статті І. М. Забари про ООН ця резолюція розглядається як стартовий акт, що закладає підвалини розвитку міжнародно-правового регулювання відносин у сфері використання технологій ІІІ у військовій сфері [282]. Автор наголошує, що резолюція акумулювала загальні підходи до можливостей, ризиків і наслідків, які були обговорені на міжнародних самітах і конференціях, серед яких прямо згадуються REAIM 2023 і REAIM 2024 [282]. Зміст резолюції підтверджує цю логіку: у ній визнається потреба спільного розуміння впливу ІІІ у військовому домені, необхідність обміну знаннями, багатостороннього діалогу, участі міжнародних і регіональних організацій, МКЧХ (Міжнародного Комітету Червоного Хреста), академічних кіл, громадянського суспільства, технічної спільноти і приватного сектору [114; 282]. UNODA підтверджує, що A/RES/79/239 стала першою резолюцією Генеральної Асамблеї ООН щодо ІІІ у військовій сфері та його наслідків для міжнародного миру і безпеки.

Резолюція A/RES/79/239 має ключове значення для оцінки REAIM, оскільки вона переводить напрацювання таких майданчиків у рамку універсального обговорення в ООН. У резолюції прямо підтверджено, що міжнародне право, включно зі Статутом ООН, міжнародним гуманітарним правом і міжнародним правом прав людини, застосовується до питань, що виникають на всіх стадіях життєвого циклу ІІІ у

військовому домені [114]. Це положення фактично закріплює на універсальному рівні ту ідею, яка була сформульована у REAIM 2023: військовий ІІІ не перебуває поза правом. Більше того, резолюція заохочує держави продовжувати оцінку наслідків військового ІІІ для міжнародного миру і безпеки, проводити багатосторонній діалог, обмінюватися передовими практиками і подолати розриви між країнами у сфері відповідального військового ІІІ [114; 282].

Еволюцію REAIM як процесу формування засад відповідального військового ІІІ доцільно подати через авторську схему, винесену в додатки (Рис. 8) (Додаток 16). Її логіка має показати послідовний рух від REAIM 2023 Call to Action до REAIM 2024 Blueprint for Action і подальшого універсального закріплення проблематики у резолюції ГА ООН A/RES/79/239. Така схема не створює новий зміст, а лише візуально узагальнює вже розкритий у тексті процес переходу від *soft law* до ширшої міжнародно-правової рамки [210; 211; 114; 282].

Зміст REAIM також потрібно оцінювати крізь призму міжнародного гуманітарного права. Хоча документи REAIM не замінюють Женевські конвенції та звичаєве МГП, вони конкретизують питання, які виникають при застосуванні ІІІ у збройному конфлікті. Передусім це стосується принципів розрізнення, пропорційності та запобіжних заходів. Якщо система ІІІ використовується для ідентифікації цілей, аналізу поведінки, прогнозування ризику або підтримки рішення про ураження, вона повинна працювати так, щоб командир або оператор міг здійснити реальну правову оцінку. Наявність алгоритмічної рекомендації не звільняє людину від обов'язку перевірити характер цілі, очікувану побічну шкоду, військову перевагу і можливість альтернативних способів дії. У цьому аспекті REAIM підсилює не нові норми, а застосування чинних норм до нових технологічних умов [4; 62; 210; 282].

Водночас REAIM не вирішує питання про обов'язковість *meaningful human control* (значущого людського контролю). Документи 2023 і 2024 рр. говорять про людський нагляд, людську відповідальність, належну людську участь і підзвітність, але не встановлюють єдиної юридичної дефініції людського контролю [210; 211]. Це одна з головних меж процесу. Для одних держав достатнім може бути загальний командний

контроль на стадії розгортання системи. Для інших необхідним є безпосереднє людське схвалення кожного рішення щодо застосування сили. Треті держави можуть просувати модель контекстного контролю, де рівень людської участі залежить від типу системи, середовища, часу реагування і ризику для цивільних осіб. REAIM не усуває цю розбіжність, але створює спільну рамку, в якій сама необхідність людської участі вже визнається як засадничий елемент відповідального військового ІІІ [210; 211; 217].

Не менш складним є питання пояснюваності. REAIM 2024 прямо пов'язує відповідальне використання із поліпшенням пояснюваності ІІІ [211]. У військовому контексті пояснюваність не може тлумачитися так само, як у цивільних адміністративних процедурах. Частина систем буде секретною, частина функціонуватиме у реальному часі, частина використовуватиме складні моделі, які не можуть бути повністю пояснені оператору у момент бойової дії. Однак з міжнародно-правової точки зору мінімальний рівень пояснюваності має бути забезпечений. Він повинен дозволяти встановити, які дані використовувала система, які межі її застосування були визначені, хто мав повноваження прийняти або відхилити її рекомендацію, які процедури тестування були проведені і чи могла система функціонувати в умовах, у яких її фактично застосували. Без цього неможливі ні аудит, ні відповідальність, ні подальше розслідування можливого порушення МГП [211; 282].

REAIM також є важливим для осмислення взаємодії військового ІІІ та контролю над озброєннями. У документах і порядку денному саміту 2024 р. окремо згадувалися наслідки для міжнародної безпеки, динаміки конфліктів і поширення зброї масового знищення [211]. Це означає, що військовий ІІІ сприймається не лише як тактичний інструмент на полі бою, а як технологія, здатна впливати на стратегічну стабільність. Застосування ІІІ у системах раннього попередження, ядерному командуванні, кіберопераціях, протиракетній обороні або автоматизованому аналізі розвідувальних даних може скоротити час прийняття рішень і підвищити ризик помилкової ескалації. Саме тому відповідальне використання ІІІ у військовій сфері має включати не лише гуманітарний, а й стратегічно-безпековий вимір [211; 114].

Важливою особливістю REAIM є участь середніх держав у формуванні глобального порядку денного. Нідерланди і Республіка Корея виступили не лише організаторами першого саміту, а й модераторами ширшого процесу. Для Республіки Корея цей напрям має особливе значення. У попередньому аналізі було зазначено, що Південна Корея разом із Нідерландами співорганізувала REAIM 2023, а у вересні 2024 р. прийняла другий саміт REAIM у Сеулі, розширивши діалог за участю великої кількості держав і просуваючи подальшу роботу над принципами міжнародного регулювання військового ІІІ [211]. Це показує, що регулювання військового ІІІ не є виключною сферою великих військових держав. Навпаки, саме середні держави можуть відігравати роль посередників, які здатні поєднувати інтереси високотехнологічних держав, держав, що розвиваються, міжнародних організацій і громадянського суспільства [210; 211].

У практичному вимірі REAIM виконує кілька функцій. Перша функція полягає у нормалізації самого питання військового ІІІ як предмета міжнародного обговорення. До 2023 р. значна частина дискусії була зосереджена навколо LAWS. REAIM розширив предмет до всього військового домену. Друга функція полягає у формуванні спільної мови: відповідальність, людський нагляд, дані, ризики, тестування, пояснюваність, багатосторонність. Третя функція полягає у зв'язуванні різних рівнів регулювання: національного, регіонального, союзницького і універсального. Четверта функція полягає у підготовці ґрунту для майбутніх юридично обов'язкових норм. П'ята функція полягає у залученні приватного сектору, без якого військовий ІІІ неможливо ефективно регулювати [210; 211; 282].

Разом з тим REAIM має низку обмежень. Перше обмеження полягає у необов'язковій природі його документів. Держави можуть підтримувати декларації, але не змінювати внутрішні практики. Друге обмеження полягає у відсутності єдиного механізму моніторингу. Немає органу, який перевіряв би, чи виконують держави проголошені принципи. Третє обмеження полягає у розбіжностях між державами щодо автономності, контролю і майбутніх заборон. Четверте обмеження пов'язане з приватним сектором: технологічні компанії можуть бути залучені до діалогу, але їхня

поведінка не завжди прямо контролюється міжнародним публічним правом. П'яте обмеження стосується нерівності технологічних можливостей: держави мають різний рівень доступу до інфраструктури, даних, моделей, експертизи і засобів перевірки. Саме тому REAIM поки що не є завершеною системою регулювання, а радше процесом формування майбутньої системи [210; 211; 282].

Функціональну модель REAIM у системі становлення міжнародно-правового регулювання військового ІІІ доцільно винести у додатки як авторську схему (Рис. 9) (Додаток 17). У ній REAIM має бути показаний як проміжна ланка між національними оборонними стратегіями, союзницькими підходами НАТО, універсальним рівнем ООН, позицією МКЧХ та участю приватного сектору. Така схема дозволяє відобразити його не як окрему конференцію, а як функціональний механізм накопичення *soft law*, експертних стандартів і політичних очікувань щодо відповідального військового ІІІ [101; 210; 211; 282].

З урахуванням викладеного REAIM доцільно визначити як багатосторонній процес формування засад відповідального використання ІІІ у військовій сфері, що поєднує політичні декларації, експертну взаємодію, міжнародно-правові орієнтири, технічні підходи до управління ризиками та багатосуб'єктну співпрацю. Його сутність полягає не в тому, щоб одразу створити новий міжнародний договір, а в тому, щоб сформувати мінімальний консенсус щодо того, які вимоги повинні передувати будь-якій подальшій юридизації. Такими вимогами виступають відповідність міжнародному праву, людська відповідальність, належний *human oversight*, управління даними, оцінка ризиків, пояснюваність, підготовка персоналу, інклюзивність, обмін передовими практиками та подолання технологічних розривів [210; 211; 282].

REAIM не слід розглядати лише як дипломатичний формат обговорення нової технології. Його значення є ширшим, оскільки він поступово виконує функцію проміжного нормативного середовища між політичними деклараціями, доктринальними напрацюваннями і майбутніми міжнародно-правовими механізмами. У сфері військового ІІІ саме такий проміжний рівень є особливо важливим, оскільки

класична договірна нормотворчість рухається повільніше, ніж технологічні зміни, а ризики вже мають практичний характер [210; 211; 282].

REAIM фактично зміщує фокус міжнародної дискусії з питання, чи можна використовувати ІІІ у військовій сфері, на питання, як саме його можна використовувати відповідально, правомірно і підконтрольно. Це означає, що процес не виходить із повної заборонної логіки. Він визнає військову реальність, у якій ІІІ вже використовується або готується до використання в системах аналізу даних, розвідки, логістики, захисту від кібератак, управління безпілотними платформами, ситуаційної обізнаності та підтримки прийняття рішень. Водночас REAIM не легітимує будь-яке застосування ІІІ автоматично. Навпаки, він ставить таке застосування у залежність від міжнародного права, людської відповідальності, оцінки ризиків, управління даними, тестування, пояснюваності та недопущення неконтрольованої шкоди [210; 211].

Окремо потрібно наголосити на тому, що REAIM є відповіддю не лише на проблему автономних систем озброєнь. У цьому полягає одна з його головних відмінностей від багаторічних дискусій у межах КЗЗЗ. Дискусія щодо LAWS зосереджується переважно на системах, здатних самостійно обирати та уражати цілі. REAIM охоплює значно ширший військовий домен. У документах REAIM 2023 увага звертається на відповідальне використання ІІІ загалом у військовому домені, включаючи ризики ненадійності систем, людської участі, відповідальності, непередбачуваних наслідків і ненавмисної ескалації [210]. Тому REAIM розширює предмет міжнародного регулювання від автономної зброї до всієї системи військового використання ІІІ. Це має принципове значення для становлення міжнародного права штучного інтелекту, оскільки найближчі ризики можуть походити не лише від повністю автономних бойових роботів, а й від менш помітних, але практично впливових систем.

До таких систем належать системи підтримки прийняття рішень командуванням; алгоритмічні системи аналізу розвідувальних даних; системи розпізнавання образів і об'єктів; системи прогнозування переміщення військ або цивільного населення; моделі оцінки ризику ураження; засоби захисту від кібератак, захисту та здійснення кібероперацій з елементами автоматизації; генеративні моделі для інформаційних

операцій або контрінформаційної діяльності; системи управління безпілотними платформами; системи логістичної оптимізації; інструменти оцінки бойової обстановки у режимі реального часу [210; 211; 282].

Кожен із цих напрямів породжує власну юридичну проблему. Наприклад, система підтримки командного рішення не застосовує силу безпосередньо, але може суттєво вплинути на людське рішення про ураження. Система розпізнавання цілей може помилитися через якість даних або невідповідність навчального набору реальним умовам збройного конфлікту. Генеративний ШІ може бути використаний для створення маніпулятивного контенту, дезінформації або психологічного впливу. Алгоритмічна система кібероборони може автоматично реагувати на атаку та кібератаку, але при цьому створити ризик ескалації, якщо реакція буде помилково сприйнята як наступальна дія. У зв'язку з цим REAIM доцільно розглядати як майданчик, який дозволяє вийти за межі спрощеної формули "автономна зброя дорівнює військовий ШІ". Така формула є недостатньою. Військовий ШІ є ширшим явищем, і саме через це його регулювання не може бути побудоване лише навколо заборони або дозволу автономних летальних систем [210; 211].

З практичного погляду REAIM формує декілька додаткових засад, які доцільно виділити в роботі. Перша додаткова засада полягає у контекстності правової оцінки. Одна й та сама технологія ШІ може мати різний правовий статус залежно від того, де і як вона використовується. Система аналізу даних у тилівій логістиці має один рівень ризику. Та сама або подібна система, інтегрована у процес вибору цілі, має зовсім інший рівень ризику. Тому відповідальне регулювання не повинно оцінювати ШІ абстрактно. Воно має виходити з конкретного військового контексту, ступеня автономності, можливого впливу на застосування сили, наслідків для цивільного населення та рівня людського контролю [210; 211].

Друга додаткова засада полягає у розмежуванні технічної надійності і правової допустимості. Система може бути технічно ефективною, але юридично проблемною. Наприклад, алгоритм може швидко і точно класифікувати об'єкти за формальними ознаками, але якщо ці ознаки не дозволяють відрізнити цивільний об'єкт від

військового, така ефективність не гарантує відповідності міжнародному гуманітарному праву. Отже, тестування військового ІІІ має включати не лише технічні параметри, а й правові сценарії [4; 62; 210].

Третя додаткова засада полягає у недопущенні автоматизаційного ухилю. У військових умовах оператор може надмірно покладатися на висновок системи, особливо якщо рішення потрібно приймати швидко. Це створює ризик формального, а не реального людського контролю. Тому *human oversight* не може зводитися до механічного натискання кнопки людиною. Він повинен включати розуміння системи, можливість поставити її висновок під сумнів, достатній час для оцінки, доступ до альтернативної інформації та реальне повноваження відхилити машинну рекомендацію [210; 217].

Четверта додаткова засада полягає у відповідальності на всіх етапах життєвого циклу. REAIM 2023 прямо звертає увагу на всі стадії розроблення, розгортання і використання ІІІ у військовому домені [210]. Це означає, що відповідальність не починається у момент бойового застосування. Вона виникає вже на стадії формування технічного завдання, вибору даних, навчання моделі, тестування, закупівлі, інтеграції, навчання персоналу і подальшого оновлення системи. П'ята додаткова засада полягає у контролі даних як передумові правомірності. Дані у військовому ІІІ не є нейтральним технічним ресурсом. Вони можуть містити помилки, упередження, неповноту, застарілі відомості або незаконно отриману інформацію. Якщо дані є дефектними, система може генерувати юридично небезпечні результати. Тому вимога REAIM щодо збирання, використання, поширення, архівування і видалення даних відповідно до міжнародного права та стандартів даних є не технічною, а правовою гарантією [210; 282].

Окремий акцент варто зробити на співвідношенні REAIM із позицією МКЧХ щодо автономних систем озброєнь. МКЧХ визначає автономні системи озброєнь як такі, що після активації людиною самостійно обирають і застосовують силу до цілей на підставі інформації з навколишнього середовища та узагальненого профілю цілі [4]. У такій ситуації користувач не обирає конкретну ціль і не знає точного часу або місця застосування сили. Це формулювання має безпосереднє значення для REAIM, оскільки

показує крайню межу ризику, за якої людський контроль може бути фактично втрачений [4; 217]. Проте REAIM і МКЧХ працюють у різних площинах. МКЧХ просуває більш чіткий гуманітарно-правовий підхід, орієнтований на обмеження або заборону певних автономних систем. REAIM має ширший і гнучкіший характер, оскільки об'єднує різні державні позиції та не формулює обов'язкової заборони. Це не є недоліком у чистому вигляді. Навпаки, REAIM може виконувати роль політичного мосту між державами, які підтримують жорстке регулювання, і державами, які не готові до юридично обов'язкових обмежень [4; 210; 211].

У цій логіці МКЧХ задає гуманітарно-правову межу допустимого; REAIM створює багатосторонній майданчик для погодження мінімальних стандартів відповідального використання; ООН переводить цю дискусію на універсальний рівень через резолюції і доповіді; держави імплементують ці підходи через національні стратегії, оборонні політики, процедури закупівель, тестування і навчання персоналу; приватний сектор впливає на практичну реалізацію через розробку моделей, даних, програмного забезпечення і технічної інфраструктури [4; 114; 210; 211; 282]. Така багаторівнева логіка дозволяє уникнути повторення матеріалу про НАТО і водночас показати REAIM як самостійний елемент становлення міжнародно-правового регулювання.

Особливо важливим є аналіз Blueprint for Action 2024. У ньому підкреслено, що військові застосування ШІ мають розроблятися, розгортатися і використовуватися таким чином, щоб не підривати міжнародний мир, безпеку і стабільність [211]. Документ також визнає потенційні переваги ШІ, зокрема підвищення ситуаційної обізнаності, точності, ефективності, можливостей захисту цивільних, миротворчості, моніторингу та верифікації режимів контролю над озброєннями [211]. Це положення є важливим, оскільки балансує аналіз. Військовий ШІ не може розглядатися виключно як загроза. Науково коректний підхід має визнавати і позитивний потенціал, і ризики. Потенційно ШІ може підвищити точність аналізу оперативної обстановки, пришвидшити обробку великих масивів розвідувальних даних, поліпшити ситуаційну обізнаність командування, зменшити ризик ненавмисного ураження через точніші дані,

підтримати гуманітарні цілі, якщо система допомагає краще ідентифікувати цивільні об'єкти, а також посилити моніторинг режимів контролю над озброєннями і допомагати у миротворчих, стабілізаційних, логістичних, медико-евакуаційних та розмінувальних операціях [211].

Однак цей потенціал може бути реалізований лише за певних умов. Система повинна бути перевіреною і надійною; її межі застосування мають бути визначені заздалегідь; дані мають бути якісними, релевантними і законно використаними; людина повинна зберігати реальний контроль; персонал повинен розуміти можливості та обмеження системи; застосування ШІ має бути інтегроване у правові процедури військового планування; мають існувати механізми аудиту, документування і післяопераційної перевірки [210; 211; 282]. У цьому сенсі REAIM формує не заборонну, а умовно-дозвільну модель. Військовий ШІ не заперечується як такий, але його правомірність залежить від відповідності певним критеріям. Ця модель є реалістичною, оскільки вона враховує фактичний розвиток технологій і водночас не відмовляється від міжнародно-правових обмежень [210; 211].

Окремо треба додати блок про відповідальність і підзвітність. Blueprint for Action 2024 прямо закріплює, що люди залишаються відповідальними і підзвітними за використання та наслідки застосувань ШІ у військовому домені, а відповідальність і підзвітність не можуть бути передані машинам [211]. Це положення варто вважати одним із центральних для міжнародно-правового регулювання. Воно виконує три функції. По-перше, воно зберігає класичну суб'єктну логіку міжнародного права. Відповідальність несуть держави, командири, оператори, розробники і відповідні організації, а не система ШІ. По-друге, воно запобігає появі аргументу технологічної непрозорості як підстави для уникнення відповідальності. По-третє, воно дозволяє інтегрувати військовий ШІ у вже наявні режими міжнародної відповідальності, командної відповідальності та відповідальності за порушення МГП [211; 282].

Якщо система ШІ рекомендує ураження об'єкта, але командир ухвалює рішення про застосування сили, правова оцінка не може зупинитися на рівні алгоритму. Необхідно встановити, чи було рішення командира обґрунтованим, чи мав він достатню

інформацію, чи розумів межі системи, чи були проведені перевірки, чи існували підстави сумніватися у рекомендації, чи була забезпечена можливість незалежної оцінки. Якщо ж система діяла без достатнього людського контролю, питання відповідальності переноситься на рівень тих суб'єктів, які дозволили таку архітектуру застосування [211; 282]. Тому REAIM фактично підводить до потреби в попередній правовій експертизі військової системи ІІІ, документуванні технічних і правових меж її використання, визначенні конкретних посадових осіб, відповідальних за розгортання і контроль, веденні журналів рішень, оновлень, вхідних даних і результатів, післяопераційному аудиті, процедурі зупинення або обмеження системи у разі виявлення помилок, а також регулярному перегляді відповідності системи новим технологічним і правовим умовам [210; 211; 282].

Окремо варто розширити питання human oversight. У документах REAIM ця категорія використовується як одна з головних гарантій, але сама вона потребує деталізації [210; 211]. Необхідно відрізнити формальний людський нагляд від змістовного людського контролю. Формальний нагляд існує тоді, коли людина лише присутня в процедурі, але не має реальної можливості вплинути на результат. Змістовний контроль існує тоді, коли людина має інформацію, компетентність, час, повноваження і технічні засоби для прийняття самостійного рішення. У межах цієї логіки можна розмежувати стратегічний контроль, що полягає у визначенні політики, меж допустимого застосування, правил розгортання і загальних заборон; оперативний контроль, який здійснюється на рівні планування операції, вибору середовища застосування, оцінки ризиків і встановлення обмежень для системи; тактичний контроль, який стосується конкретного рішення про використання системи у певній ситуації; технічний контроль, який передбачає можливість моніторингу, коригування, деактивації або зупинення системи; післяопераційний контроль, який полягає в аналізі дій системи, перевірці відповідності праву і встановленні відповідальності [210; 211; 217]. Таке розмежування посилює підрозділ, оскільки дозволяє показати, що human oversight не є єдиною простою дією. Це комплекс процедур, які мають супроводжувати військовий ІІІ від проєктування до післяопераційного аналізу.

Важливо також додати, що REAIM пов'язаний із майбутньою юридикацією, але не гарантує її автоматично. Soft law може мати два різні наслідки. У позитивному варіанті воно поступово перетворюється на основу для договору, міжнародного стандарту або звичаєвого правила. У негативному варіанті воно може залишитися декларативним рівнем, який держави використовують для демонстрації відповідальності без реальної зміни практики. Саме тому оцінка REAIM повинна бути збалансованою [210; 211; 282].

Перевага REAIM полягає у тому, що він створює глобальний майданчик за участю різних держав, виводить військовий ІІІ за межі вузької дискусії про LAWS, прямо пов'язує ІІІ з міжнародним правом, визнає людську відповідальність і підзвітність, включає питання даних, тестування, пояснюваності і персоналу, залучає приватний сектор, академічні кола і громадянське суспільство, впливає на подальше обговорення в межах ООН і створює термінологічну та концептуальну базу для майбутніх норм [210; 211; 282]. Водночас його слабкі сторони також очевидні: документи не мають юридично обов'язкової сили, немає механізму перевірки виконання, держави можуть підтримувати загальні формули, але по-різному тлумачити їх зміст, поняття людського контролю залишається недостатньо визначеним, питання відповідальності приватних розробників не вирішене, не встановлено єдиної процедури аудиту військових систем ІІІ, не визначено мінімальних вимог до прозорості в умовах військової секретності, не усунуто нерівність між технологічно розвиненими державами і державами, що залежать від імпорту технологій, а також відсутній чіткий зв'язок між політичними деклараціями і майбутніми санкційними або відповідальнісними механізмами [210; 211; 282].

Додатково можна ввести поняття нормативної щільності. REAIM підвищує нормативну щільність у сфері військового ІІІ, тобто збільшує кількість принципів, процедур, очікувань і політичних стандартів, які держави мають враховувати. Навіть якщо ці стандарти не є юридично обов'язковими, вони поступово формують уявлення про належну поведінку. У майбутньому саме такі стандарти можуть бути використані

для оцінки того, чи діяла держава добросовісно, чи забезпечила належну обачність, чи впровадила мінімальні гарантії безпеки [210; 211; 282].

Це особливо важливо у зв'язку з резолюцією ГА ООН A/RES/79/239. Резолюція підтверджує, що міжнародне право, включно зі Статутом ООН, міжнародним гуманітарним правом і міжнародним правом прав людини, застосовується до питань, які виникають на всіх стадіях життєвого циклу ІІІ у військовому домені [114]. У цьому положенні фактично закріплена ідея, яку REAIM розвивав із 2023 р.: технологічна новизна не скасовує правову відповідальність. Навпаки, що складнішою є технологія, то більшими мають бути вимоги до контролю, пояснюваності і правової перевірки [114; 282].

Для загального контексту роботи REAIM має особливе значення, оскільки демонструє, як міжнародне право ІІІ формується не одномоментно, а через послідовне зближення політичних, технічних і правових стандартів. У цьому процесі *soft law* не є слабким або другорядним явищем. Воно виконує функцію правового передетапу, без якого складно перейти до договору. Спочатку держави мають погодити поняття, ідентифікувати ризики, визначити мінімальні стандарти відповідальності, перевірити механізми співпраці і лише потім можуть переходити до формально обов'язкових норм. Саме таку роль відіграє REAIM у сфері військового ІІІ [210; 211; 282].

Отже, REAIM є одним із ключових механізмів становлення міжнародно-правового регулювання використання ІІІ у військовій сфері. Його значення полягає у тому, що він виводить проблему військового ІІІ за межі вузької дискусії про автономну зброю, формує засади відповідального використання для всього військового домену, поєднує держави і недержавних акторів, створює основу для подальшого обговорення в межах ООН та впливає на зміст універсальних актів м'якого права, зокрема резолюції ГА ООН A/RES/79/239. На цьому етапі REAIM не є завершеним правовим режимом, але саме він формує той мінімальний нормативний каркас, без якого майбутній міжнародно-правовий режим військового ІІІ залишався б фрагментарним, декларативним і технічно відірваним від реальної практики застосування технологій у сфері оборони та безпеки [210; 211; 114; 282].

3.2. ООН: формування універсальних доктринальних основ використання штучного інтелекту у військовій сфері

Формування універсальних доктринальних основ використання штучного інтелекту у військовій сфері в межах Організації Об'єднаних Націй слід розглядати як окремий етап становлення міжнародно-правового регулювання новітніх військових технологій. Його специфіка полягає не у створенні завершеного договірного режиму, а у визначенні загальних правових, гуманітарних, технічних, етичних і безпекових орієнтирів, які мають універсальний характер і можуть бути використані державами для подальшого розвитку національних стратегій, міждержавної співпраці та майбутніх міжнародно-правових інструментів. На відміну від регіональних або союзницьких підходів, позиція ООН спрямована на вироблення мінімально узгодженої рамки для всіх держав, незалежно від рівня їхнього технологічного розвитку, військово-політичної орієнтації або участі в окремих оборонних альянсах [275; 276].

У межах ООН питання військового використання штучного інтелекту було поставлено не як вузькотехнічна проблема оборонної модернізації, а як питання міжнародного миру і безпеки. Саме така постановка є принциповою. Вона означає, що застосування ШІ у військовій сфері потенційно може впливати на стабільність міждержавних відносин, режими контролю над озброєннями, рівень ескалації збройних конфліктів, захист цивільного населення, дотримання міжнародного гуманітарного права, а також на здатність держав забезпечувати підзвітне і правомірне застосування сили. Відповідно, міжнародно-правове регулювання військового ШІ не може бути зведене лише до правил технічного тестування, етичних декларацій або загальних принципів цифрового врядування. Його предметом стає комплекс правовідносин, пов'язаних із розробкою, закупівлею, оцінкою, розгортанням, використанням, передачею, експлуатацією і виведенням з експлуатації систем ШІ у військовій сфері [275; 276].

Підхід ООН до військового ШІ сформувався на тлі ширшого розуміння штучного інтелекту як технології подвійного використання. Така характеристика має правове значення, оскільки одна й та сама технологічна основа може використовуватися як для

цивільних, так і для військових завдань. Системи обробки великих даних, розпізнавання образів, автономної навігації, прогнозової аналітики, генеративного моделювання, кіберзахисту або підтримки прийняття рішень можуть одночасно мати комерційне, адміністративне, гуманітарне і військове значення. Саме тому регулювання військового ШІ не може бути побудоване за принципом повного відмежування військових технологій від цивільних. Правове значення набуває не лише сама технологія, а контекст її використання, суб'єкт застосування, цільове призначення, рівень автономності, можливість впливу на застосування сили та наслідки для міжнародного миру і безпеки [275; 281].

Першим важливим етапом універсалізації цієї проблематики став брифінг Ради Безпеки ООН 18 липня 2023 р. на тему "Artificial Intelligence: Opportunities and Risks for International Peace and Security". Концептуальна записка до цього засідання, поширена як документ S/2023/528 від 17 липня 2023 р., визначала метою обговорення потенційні наслідки ШІ для міжнародного миру і безпеки, а також необхідність сприяти його безпечному та відповідальному використанню [277]. Це мало принципове значення, оскільки питання ШІ було поставлене перед Радою Безпеки не як загальна тема цифрового розвитку, а як потенційний фактор впливу на сферу, що належить до ядра мандату ООН. Саме з цього моменту військовий і безпековий вимір ШІ отримав чітку інституційну прив'язку до компетенції ООН щодо підтримання міжнародного миру і безпеки [275; 277].

Рада Безпеки не створила спеціального правового режиму ШІ. Проте її брифінг заклав важливу доктринальну передумову: штучний інтелект може бути одночасно інструментом підвищення ефективності миротворчості, раннього попередження, гуманітарного реагування і контролю ризиків, а також джерелом нових загроз, зокрема дезінформації, кібератак, автономізації насильства, кібероперацій, алгоритмічної ескалації та непрозорого військового планування спецслужбами. Така двоїстість стала основою подальшого підходу ООН. Вона не дозволяє кваліфікувати ШІ лише як загрозу або лише як корисний інструмент. Натомість формується ризик-орієнтована правова

логіка, за якою значення має спосіб використання, ступінь контролю, відповідність міжнародному праву і наявність належних процедур запобігання шкоді [275; 277; 281].

Наступним етапом стала резолюція Генеральної Асамблеї ООН № 78/241 "Lethal autonomous weapons systems", ухвалена 22 грудня 2023 р. Вона стосувалася смертоносних автономних систем озброєнь і стала важливим актом у площині поступового переходу дискусії про автономну зброю з експертно-технічного рівня до універсального рівня Генеральної Асамблеї [278]. Значення цієї резолюції полягає в тому, що вона підтвердила актуальність питання систем, здатних функціонувати із високим ступенем автономності у зв'язку із застосуванням сили. Водночас її предмет був вузьчим, ніж подальший підхід ООН до військового ШІ загалом. Смертоносні автономні системи озброєнь є лише одним, хоча й найбільш чутливим, сегментом військового ШІ. Саме тому наступна резолюція № 79/239 розширила предмет розгляду від автономної зброї до штучного інтелекту у військовому домені загалом [275; 276; 278].

Такий перехід має правове значення. Якщо увага зосереджується лише на автономних системах озброєнь, поза межами регулювання можуть залишатися системи підтримки прийняття рішень, алгоритмічна розвідка, аналіз супутникових даних, автоматизовані кібероперації, генеративні інформаційні інструменти, системи прогнозування ризиків, військова логістика, системи раннього попередження та інші застосування, які не є зброєю у вузькому сенсі, але можуть прямо або опосередковано впливати на застосування сили. Тому розширення предмета з LAWS до військового ШІ як комплексного домену є необхідним для адекватного міжнародно-правового реагування [275; 276; 278].

Ключовим актом у цьому процесі стала резолюція Генеральної Асамблеї ООН № 79/239 "Artificial intelligence in the military domain and its implications for international peace and security", ухвалена 24 грудня 2024 р. Вона має характер акта м'якого права, але її зміст свідчить про формування універсальної доктринальної рамки для подальшого міжнародно-правового регулювання. У резолюції було підтверджено застосовність міжнародного права, включаючи Статут ООН, міжнародне гуманітарне

право і міжнародне право прав людини, до питань, які виникають на всіх етапах життєвого циклу ІІІ у військовому домені [276]. Це положення є центральним для всього подальшого правового аналізу, оскільки заперечує можливість існування технологічного винятку із чинного міжнародного права [275; 276].

Застосовність міжнародного права до всіх етапів життєвого циклу військового ІІІ означає, що правова оцінка не може обмежуватися моментом безпосереднього використання системи в операції. Вона повинна охоплювати передпроектну оцінку, проектування, розробку, навчання моделі, добір і перевірку даних, тестування, валідацію, закупівлю, передачу, розгортання, експлуатацію, оновлення, аудит і виведення системи з використання. Такий підхід є особливо важливим для ІІІ, оскільки правовий ризик часто виникає ще до моменту застосування системи. Помилки у даних, непрозорість моделі, відсутність тестування у релевантному середовищі, недостатня підготовка операторів або невизначеність командної відповідальності можуть створити незаконні наслідки пізніше, навіть якщо безпосереднє рішення формально ухвалюється людиною [275; 276; 281].

У цьому аспекті резолюція № 79/239 закріплює доктринальний зсув від подієвої до процесуальної моделі правового контролю. Подієва модель концентрується на конкретному акті застосування сили. Процесуальна модель охоплює весь цикл створення і використання військової системи ІІІ. Для міжнародного гуманітарного права це означає, що відповідність принципам розрізнення, пропорційності та запобіжних заходів має забезпечуватися не лише на етапі бойового рішення, а й на етапі конструювання технічної системи, визначення її функцій, меж автономності, способу обробки даних і порядку людського контролю. Без такої попередньої правової інтеграції принципи МГП можуть залишитися формальними [275; 276; 282].

Підхід ООН також відображає необхідність комплексного аналізу військового ІІІ. У резолюції № 79/239 і в доктринальних підходах, що передували її ухваленню, виділяються щонайменше п'ять взаємопов'язаних площин: правова, гуманітарна, технічна, етична і безпекова [275; 276]. Ці площини не можуть бути розглянуті окремо одна від одної. Правова площина визначає застосовні норми та відповідальність.

Гуманітарна площина стосується захисту цивільного населення, недопущення невивіркованої шкоди та збереження людського контролю. Технічна площина охоплює якість даних, тестування, надійність, кіберстійкість і пояснюваність. Етична площина пов'язана з допустимими межами делегування рішень машинним системам. Безпекова площина включає ризики ескалації, гонки озброєнь, нерозповсюдження, кіберзагроз і використання ШІ недержавними суб'єктами [275; 276; 281].

Саме комплексність відрізняє підхід ООН від вузьких моделей регулювання. Військовий ШІ не може бути врегульований лише через технічний стандарт, оскільки навіть надійна система може бути використана неправомірно. Він не може бути врегульований лише через етичну декларацію, оскільки етичні принципи без юридичних процедур не забезпечують підзвітності. Він не може бути врегульований лише через МГП, оскільки частина ризиків виникає до збройного конфлікту або поза безпосереднім застосуванням сили. Тому універсальна доктринальна модель ООН передбачає багаторівневе поєднання правових, технічних, політичних і гуманітарних інструментів [275; 276].

У резолюції № 79/239 особливу увагу приділено питанню наслідків військового ШІ для міжнародного миру і безпеки. Держави заохочуються продовжувати оцінювати такі наслідки, включаючи багатосторонній діалог у відповідних міжнародних форумах [276]. Це положення показує, що ООН не обмежується констатацією існування ризиків. Вона формує обов'язок політико-правової обачності, який, хоча й не має договірної характеру, визначає очікувану поведінку держав. Оцінка наслідків має проводитися не після виникнення шкоди, а до та під час впровадження військових систем ШІ. Інакше міжнародна спільнота реагуватиме лише на вже реалізовані порушення, а не запобігатиме їм [275; 276].

До основних безпекових ризиків військового ШІ належать прискорення гонки озброєнь у сфері автономних і алгоритмічних систем, зниження політичного або військового порогу застосування сили, автоматизована або напівавтоматизована ескалація в умовах кризової невизначеності, поширення військових технологій ШІ серед недержавних суб'єктів, поєднання ШІ з кіберопераціями та кібератаками,

квантовими технологіями, біотехнологіями, хімічними технологіями або ядерними системами, використання генеративного ШІ для дезінформації, маніпуляцій і психологічного впливу, ускладнення атрибуції дій у кіберпросторі та інформаційному середовищі, зростання залежності командування від алгоритмічних рекомендацій, виникнення технічних помилок, які можуть бути помилково інтерпретовані як ворожі дії, а також розширення технологічної нерівності між державами [275; 276; 277; 281; 283].

Наведені ризики мають різну юридичну природу. Частина з них стосується міжнародного гуманітарного права, частина належить до сфери *jus ad bellum*, частина пов'язана з міжнародною відповідальністю держав, частина стосується режимів контролю над озброєннями і нерозповсюдження, а частина має значення для міжнародного права прав людини. Саме тому ООН формує не вузький режим для одного виду зброї, а широку доктринальну основу, здатну охопити різні способи використання ШІ у військовій сфері [275; 276; 281; 283].

Доктринальні блоки підходу ООН до міжнародно-правового регулювання військового ШІ доцільно узагальнити в окремій таблиці, винесеній у додатки (Таблиця 9) (Додаток 18). Передумови формування універсального підходу ООН до військового ШІ доцільно подати через авторську схему (Рис. 10) (Додаток 19).

У межах підходу ООН особливе значення має категорія відповідального застосування ШІ у військовій сфері. Вона включає людиноцентричне, підзвітне, безпечне, надійне і таке, що заслуговує на довіру використання ШІ відповідно до міжнародного права [275; 276]. Це визначення має системний характер. Людиноцентричність означає, що людина не може бути усунута з процесу правового контролю над застосуванням сили. Підзвітність означає збереження можливості встановити відповідальних суб'єктів. Безпечність означає наявність процедур мінімізації технічних і операційних ризиків. Надійність передбачає перевірку системи у релевантних умовах. Довіра означає, що використання ШІ повинно бути не лише ефективним, а й правомірним, контрольованим і передбачуваним [275; 276; 281].

Людиноцентричність у військовому ШІ не може тлумачитися як загальна гуманітарна декларація. У правовому сенсі вона означає, що рішення, пов'язані із застосуванням сили, не повинні бути повністю виведені з-під людського контролю. Це не обов'язково означає однакову форму участі людини у всіх системах. Рівень людського контролю може залежати від характеру системи, її функції, швидкості роботи, середовища застосування, потенційної шкоди і близькості до ураження цілі. Проте мінімальна вимога залишається незмінною: людина повинна мати реальні повноваження, інформацію і можливість впливу на використання системи. Інакше підзвітність стає формальною [275; 276; 282].

Підзвітність у підході ООН пов'язана з недопущенням перенесення відповідальності на алгоритм. ШІ не є суб'єктом міжнародного права, не має власної волі у юридичному сенсі і не може бути носієм міжнародно-правової відповідальності. Відповідальність зберігається за державами, військовими командуваннями, операторами, розробниками, постачальниками і посадовими особами, які визначали архітектуру системи, її межі, порядок використання та процедури контролю. Якщо система ШІ сприяла незаконному результату, правова оцінка має встановити не лише технічну помилку, а й те, чи були виконані обов'язки належної обачності, перевірки, тестування, навчання персоналу та контролю [275; 276].

Безпечність і надійність у військовому ШІ мають не лише технічне, а й юридичне значення. Технічно працездатна система може бути юридично непридатною, якщо вона не здатна функціонувати у складному бойовому середовищі, не враховує присутність цивільних осіб, працює на нерелевантних даних або не дозволяє людині зрозуміти межі її рекомендацій. Тому надійність повинна оцінюватися не лише за показниками точності, швидкості або продуктивності, а й за здатністю системи підтримувати правомірне прийняття рішень. У цьому проявляється важлива особливість військового ШІ: його якість визначається не лише ефективністю, а й відповідністю праву [275; 276; 281].

Категорія довіри також потребує правового уточнення. Довіра до військового ШІ не може ґрунтуватися на загальній вірі в технологічну перевагу. Вона має бути

результатом процедур: тестування, валідації, документування, контролю даних, незалежної оцінки, підготовки персоналу, післяопераційного аналізу і можливості зупинення системи. Довіра без процедур перетворюється на небезпечну технологічну залежність. Саме тому універсальний підхід ООН фактично орієнтує держави на створення не лише принципів, а й інституційних механізмів їх виконання [275; 276; 281].

Окремим елементом резолюції № 79/239 є заклик до обміну знаннями, інформацією, передовим досвідом і засвоєними уроками. ООН заохочує Секретаріат та інші структури системи ООН, за рахунок добровільних внесків, сприяти обміну знаннями і підвищенню обізнаності щодо наслідків військового ІІІ для міжнародного миру і безпеки [276]. Це положення має практичне значення. Військовий ІІІ розвивається нерівномірно. Частина держав має власні дослідницькі центри, військово-промислову базу і процедури тестування. Інші держави можуть отримувати готові технології без повного розуміння їхніх обмежень. Така нерівність створює безпекові ризики, оскільки слабкий контроль у одній державі може мати транскордонні наслідки [275; 276].

Саме тому подолання розривів між державами є не лише питанням цифрової справедливості, а й питанням міжнародної безпеки. Якщо окремі держави не мають експертизи для оцінки військових систем ІІІ, вони можуть використовувати їх без належної правової і технічної перевірки. Якщо держави залежать від зовнішніх постачальників, вони можуть не контролювати дані, оновлення, приховані функції або вразливості системи. Якщо держави не мають доступу до передового досвіду, вони можуть повторювати помилки інших. Тому добровільна допомога, передача знань і обмін інформацією мають розглядатися як елементи превентивного міжнародно-правового механізму [275; 276; 281].

У підході ООН також простежується важлива відмінність між цивільним і військовим використанням ІІІ. Універсальні документи щодо цифрового розвитку і цивільного ІІІ орієнтовані на сталий розвиток, інклюзивність, права людини, подолання цифрового розриву і відповідальне управління технологіями. Глобальний

цифровий договір, ухвалений як додаток до Пакту в ім'я майбутнього, прямо визначає, що він стосується немілітарного домену, але водночас створює загальні підходи до цифрової співпраці, інклюзивного управління даними та відповідального технологічного розвитку [280]. Військовий ШІ потребує окремого розгляду, оскільки його наслідки прямо пов'язані із застосуванням сили, збройними конфліктами, стабільністю, контролем над озброєннями і захистом цивільного населення [275; 276; 280].

Таке розмежування не означає повної ізоляції цивільного і військового регулювання. Навпаки, між ними існує постійний перетин через подвійне використання технологій. Цивільні моделі можуть бути адаптовані для військових цілей. Військові технології можуть впливати на цивільну інфраструктуру. Дані, зібрані у цивільному середовищі, можуть використовуватися для військової аналітики. Генеративні моделі можуть застосовуватися як для освіти або комунікації, так і для інформаційних операцій. Тому ООН фактично формує двоконтурний підхід: загальна рамка цифрового врядування і спеціальний військово-безпековий контур для ШІ у військовій сфері [275; 276; 280].

Для подальшого розвитку міжнародно-правового регулювання це означає, що майбутні норми щодо військового ШІ повинні будуть враховувати щонайменше три рівні. Загальний рівень міжнародного права включає Статут ООН, принцип суверенної рівності держав, заборону сили, міжнародне право прав людини, міжнародне гуманітарне право і міжнародну відповідальність. Спеціальний військово-технічний рівень стосується систем озброєнь, автономності, тестування, людського контролю, управління даними, кіберстійкості і процедур застосування. Інституційно-коопераційний рівень включає обмін знаннями, участь міжнародних організацій, наукових кіл, технічної спільноти, приватного сектору і громадянського суспільства [275; 276; 281].

На цьому етапі ООН ще не створила повного правового режиму військового ШІ. Проте резолюція № 79/239 уже закріпила універсальну доктринальну основу, на якій такий режим може розвиватися. Її значення полягає в тому, що вона визначила межі

допустимої дискусії: військовий ШІ не є правовим вакуумом; він повинен оцінюватися протягом усього життєвого циклу; його використання має бути відповідальним; його наслідки повинні оцінюватися через міжнародний мир і безпеку; держави мають співпрацювати для подолання технологічних розривів [275; 276].

Універсальну доктринальну модель ООН щодо військового ШІ доцільно винести в додатки як узагальнювальну схему (Рис. 11) (Додаток 20).

Універсальний підхід ООН до військового використання штучного інтелекту не обмежується констатацією того, що міжнародне право застосовується до нових технологій. Його значення полягає у поступовому перенесенні правового контролю на весь життєвий цикл системи ШІ. Саме це дозволяє говорити про становлення не лише політичної, а й доктринальної основи майбутнього міжнародно-правового режиму. Якщо автономна зброя або інша система військового ШІ оцінюється лише в момент фактичного застосування сили, значна частина правових ризиків залишається поза аналізом. Такі ризики можуть виникнути ще на стадії формування технічного завдання, добору даних, навчання моделі, визначення меж автономності, закупівлі, інтеграції до військової інфраструктури, оновлення програмного забезпечення або підготовки персоналу. Тому резолюція ГА ООН № 79/239 принципово закріплює підхід, за яким міжнародне право застосовується до всіх питань, що виникають на всіх етапах життєвого циклу засобів ШІ у військовій сфері [276]. Саме в цьому положенні зосереджена одна з головних новацій універсального підходу ООН [275; 276].

Життєвий цикл військового ШІ охоплює не тільки розробку і використання, а значно ширший комплекс дій: передпроектну оцінку, проектування, програмну розробку, навчання моделі, добір навчальних даних, оцінювання, тестування, валідацію, продаж, закупівлю, передачу, розгортання, експлуатацію, оновлення, аудит і виведення з експлуатації [275; 276; 281]. Такий підхід фактично змінює юридичну логіку контролю над військовими технологіями. У класичному розумінні питання правомірності зброї часто пов'язувалося з її характеристиками і способом застосування. У випадку ШІ цього недостатньо. Алгоритмічна система може не мати сталої, заздалегідь повністю передбачуваної поведінки, оскільки її результати залежать

від даних, середовища, оновлень, налаштувань, режиму автономності та взаємодії з оператором. Відповідно, правова перевірка повинна бути не одноразовою, а повторюваною і процесуально закріпленою. Це означає, що міжнародно-правова оцінка має бути інтегрована в інженерний, управлінський і командний цикл [275; 276; 281].

На стадії передпроектної оцінки має визначатися, чи може запланована система ІІІ бути використана у військовій сфері без порушення базових норм міжнародного права. Йдеться не лише про загальне питання допустимості технології, а про функціональну оцінку її призначення. Якщо система створюється для логістики, медичної евакуації або обробки технічних даних, рівень правового ризику буде одним. Якщо система створюється для розпізнавання цілей, підтримки рішення про ураження або автономної навігації бойової платформи, правовий ризик істотно зростає. Саме тому передпроектна стадія повинна містити правову класифікацію призначення системи, можливих сценаріїв її застосування і потенційного впливу на захищені об'єкти та осіб. Без такої оцінки держава може створити систему, яка буде технічно ефективною, але юридично непридатною для безпечного використання у збройному конфлікті [275; 276; 282].

На стадії проектування і розробки особливого значення набувають якість даних, пояснюваність, кіберстійкість, можливість людського втручання і документування технічних рішень. У військовому ІІІ дані не можуть розглядатися як нейтральний ресурс. Вони визначають логіку поведінки системи, її здатність класифікувати об'єкти, розрізняти контексти, оцінювати ризики і формувати рекомендації. Якщо навчальні дані містять помилки, зміщення, застарілу інформацію або нерелевантні бойовому середовищу приклади, система може створювати неправомірні результати. У контексті міжнародного гуманітарного права це може вплинути на здатність відрізнити цивільний об'єкт від військової цілі, оцінити очікувану побічну шкоду або врахувати зміну статусу об'єкта. Тому управління даними стає не технічною, а юридично значущою умовою правомірного використання ІІІ [276; 281; 282].

На стадії тестування і валідації повинна перевірятися не лише технічна продуктивність системи. З погляду ООН, військовий ІШ має оцінюватися комплексно, тобто з урахуванням гуманітарної, правової, технічної, етичної і безпекової складових [275; 276]. Це означає, що тестування повинно включати сценарії, у яких перевіряється поведінка системи за умов невизначеності, неповних даних, змішаного цивільно-військового середовища, спроб ворожого втручання, помилкових сигналів, швидкої зміни обстановки і нестандартних цілей. Якщо система демонструє високу точність у контрольованих умовах, але не проходить перевірку в реалістичному військовому середовищі, її впровадження створює правовий ризик. Відповідно, тестування має бути орієнтоване не лише на ефективність, а на відповідність праву [275; 276; 281].

На стадії закупівлі і передачі системи виникає окрема проблема відповідальності держави. Універсальний підхід ООН дозволяє поставити питання про належну обачність при придбанні військових систем ІШ. Держава не може обмежитися прийняттям технології від постачальника без перевірки її функцій, обмежень, режиму оновлення, кіберзахисту, джерел даних і можливих прихованих вразливостей. Якщо держава використовує систему, походження, логіка і межі якої їй недостатньо зрозумілі, це створює ризик неконтрольованого делегування військової функції. Особливо складною є ситуація, коли система створена приватним розробником, навчається на комерційних або змішаних наборах даних, має закриту архітектуру і постійно оновлюється без повного контролю користувача. У такому разі закупівля має супроводжуватися процедурою юридико-технічної експертизи [275; 276; 281].

На стадії розгортання і використання центральним стає питання людського контролю. Резолюція № 79/239 звертає увагу на гарантії, які включають заходи щодо прийняття рішень і забезпечення контролю з боку людини у питанні застосування сили відповідно до міжнародно-правових зобов'язань держав [276]. Це положення має особливе значення для систем, які здатні підтримувати або впливати на рішення щодо цілей. Людський контроль не може бути формальним. Сам факт присутності оператора у процесі не гарантує правомірності, якщо оператор не має достатнього часу, інформації, технічного розуміння, повноважень і реальної можливості зупинити або

змінити дію системи. Тому змістовний людський контроль повинен мати як мінімум чотири елементи: розуміння функцій системи, можливість критичної оцінки її висновків, право втручання та документовану відповідальність за рішення [275; 276; 282].

Зв'язок підходу ООН із проблематикою смертоносних автономних систем озброєнь залишається принциповим, але не вичерпним. Резолюція № 78/241 щодо LAWS і резолюція № 79/239 щодо ШІ у військовому домені разом формують дві взаємопов'язані площини. Перша стосується найбільш небезпечного сегмента автономізації, тобто систем, здатних самостійно обирати і уражати цілі. Друга охоплює ширший військовий домен ШІ, включаючи системи, які не є зброєю у вузькому значенні, але можуть впливати на планування, аналіз, командування, логістику, кібердії і застосування сили [276; 278]. Такий поділ є виправданим. Він дозволяє не розчиняти проблему автономної зброї у загальному регулюванні ШІ, але водночас не залишати поза увагою інші військові застосування, які можуть мати істотні правові наслідки [275; 276; 278].

Діяльність Групи урядових експертів у межах Конвенції про конкретні види звичайної зброї має окреме значення для формування доктринальних основ ООН. Саме в межах цього процесу тривалий час обговорюються питання контролю з боку людини, рівня автономності, термінології, неприйнятності систем, що функціонують без належного людського контролю, а також співвідношення автономності з вимогами міжнародного гуманітарного права [275; 278; 279]. Проблема полягає в тому, що держави не мають єдиного підходу до базових категорій. Не існує повністю погодженого визначення автономної системи озброєнь, значущого людського контролю, прийнятного рівня автономності або мінімального набору заборонених функцій. Саме тому універсальна доктринальна роль ООН полягає не лише в прийнятті резолюцій, а й у створенні простору для поступового узгодження понять [275; 279].

Позиція МКЧХ посилює гуманітарно-правовий вимір цього процесу. МКЧХ визначає автономні системи озброєнь як такі, що після активації або запуску людиною самостійно ініціюють або запускають застосування сили у відповідь на інформацію із

середовища на основі узагальненого профілю цілі. Це означає, що користувач не обирає конкретну ціль і може не знати точного часу та місця застосування сили [282]. МКЧХ з 2015 р. закликає держави встановити міжнародно погоджені межі для автономних систем озброєнь, щоб забезпечити захист цивільного населення, дотримання міжнародного гуманітарного права та етичну прийнятність [282]. Ця позиція співвідноситься з підходом ООН у тому, що питання людського контролю визнається не допоміжною технічною деталлю, а центральною правовою гарантією [275; 282].

Водночас підхід ООН є ширшим за підхід МКЧХ. МКЧХ акцентує увагу передусім на автономних системах озброєнь і гуманітарних наслідках втрати людського контролю. ООН включає цю проблематику до ширшого безпекового поля, де військовий ШІ впливає також на контроль над озброєннями, нерозповсюдження, ядерну стабільність, кібербезпеку, інформаційні операції, технологічну нерівність і стратегічну конкуренцію [275; 276; 277; 281; 283]. Така різниця не є суперечністю. Вона демонструє багаторівневість майбутнього регулювання. Гуманітарно-правовий рівень встановлює межі захисту людини в умовах збройного конфлікту. Безпековий рівень оцінює вплив технологій на міжнародну стабільність. Доктринальний рівень ООН поєднує ці площини в єдину універсальну рамку [275; 276].

У межах міжнародного гуманітарного права найважливішими залишаються принципи розрізнення, пропорційності та запобіжних заходів. Військовий ШІ може підтримувати виконання цих принципів, якщо він підвищує точність аналізу, допомагає виявляти цивільні об'єкти, зменшує помилки людини або покращує ситуаційну обізнаність. Проте він може також ускладнювати їх виконання, якщо система працює непрозоро, класифікує об'єкти за недостатньо зрозумілими ознаками, не враховує зміну контексту або створює надмірну довіру з боку оператора. Тому питання полягає не в тому, чи ШІ як такий відповідає або не відповідає МГП. Правова оцінка має стосуватися конкретної системи, конкретної функції, конкретного середовища і конкретного режиму людського контролю [275; 276; 282].

Особливої уваги потребує принцип розрізнення. Якщо система ШІ використовується для ідентифікації цілей, вона повинна дозволяти людині оцінити, чи

є об'єкт військовою ціллю за нормами міжнародного гуманітарного права. Алгоритмічна класифікація не може замінити правову оцінку. Наприклад, об'єкт може мати ознаки, які модель пов'язує з військовою діяльністю, але в конкретному контексті бути цивільним або втратити військове значення. Так само особа може поводитися у спосіб, який система помилково класифікує як загрозу. Тому застосування ІІІ у таргетингу повинно супроводжуватися додатковими процедурами перевірки, особливо у змішаному середовищі, де військові та цивільні об'єкти перебувають поруч [275; 276; 282].

Принцип пропорційності також ускладнюється в умовах алгоритмічної підтримки. Пропорційність не є суто математичним співвідношенням між очікуваною військовою перевагою і побічною шкодою. Вона потребує контекстної людської оцінки, яка враховує невизначеність, характер об'єкта, наявність цивільних осіб, час операції, альтернативні засоби і можливість відкласти або змінити дію. Система ІІІ може допомогти оцінити деякі параметри, але не може самостійно нести юридичну відповідальність за пропорційність. Тому командир або інший уповноважений суб'єкт повинен мати можливість зрозуміти межі алгоритмічної рекомендації і не сприймати її як автоматично правомірну [275; 276; 282].

Принцип запобіжних заходів передбачає, що сторони конфлікту повинні вживати всіх практично можливих заходів для уникнення або мінімізації шкоди цивільним особам і цивільним об'єктам. У випадку військового ІІІ це означає необхідність попереднього тестування, обмеження середовища застосування, визначення часових і просторових меж роботи системи, встановлення процедур переривання дії, підготовки персоналу і післяопераційного аналізу. Якщо система використовується без таких процедур, важко стверджувати, що держава забезпечила належні запобіжні заходи. Саме тому життєвий цикл військового ІІІ має прямий зв'язок із виконанням норм МГП [275; 276; 282].

Окремий блок становить питання міжнародної відповідальності. Універсальний підхід ООН не змінює класичної структури міжнародної відповідальності держав, але створює підстави для її застосування до нових технологічних ситуацій. Якщо система

III, що перебуває під контролем держави, спричиняє порушення міжнародного зобов'язання, виникає питання про атрибуцію поведінки, порушення обов'язку належної обачності, недотримання МГП або неправомірне застосування сили. Складність алгоритму не може сама по собі виключати відповідальність. Навпаки, держава, яка впроваджує складну систему у військовий домен, повинна забезпечити вищий рівень перевірки і контролю [275; 276; 281].

При цьому відповідальність може виникати на кількох рівнях. На рівні держави йдеться про міжнародно-протиправне діяння, порушення МГП, неправомірне застосування сили або недотримання обов'язків контролю. На рівні військового командування може постати питання командної відповідальності, якщо особи знали або повинні були знати про ризики системи, але не забезпечили належних заходів. На рівні оператора може оцінюватися, чи була можливість зрозуміти і зупинити неправомірну дію. На рівні розробника або постачальника, хоча міжнародне публічне право не завжди прямо встановлює їхню відповідальність, може виникати питання внутрішньодержавної, контрактної, експортної або корпоративної відповідальності. Тому військовий III потребує багаторівневої моделі підзвітності [275; 276; 281].

Роль недержавних акторів у цьому контексті є однією з найскладніших. ООН у резолюції № 79/239 визнає значення міжнародних і регіональних організацій, МКЧХ, наукових і технічних кіл, громадянського суспільства та приватного сектору для обміну знаннями, інформацією і передовим досвідом [276]. Це відображає фактичну структуру сучасного технологічного розвитку. Значна частина III створюється не державними військовими лабораторіями, а приватними компаніями, університетами, дослідницькими центрами і змішаними консорціумами. Тому класична модель, за якою держава повністю контролює створення і використання військової технології, вже не відповідає реальності [275; 276; 281].

Водночас залучення приватного сектору не означає перенесення міжнародно-правової відповідальності з держави. Держава залишається головним носієм міжнародних зобов'язань. Якщо вона закупає, адаптує або використовує систему приватного походження у військовій сфері, саме вона повинна забезпечити її

відповідність міжнародному праву. Приватний сектор може бути залучений до стандартів належної обачності, прозорості, технічної документації, кібербезпеки, оцінки ризиків і запобігання зловживанням. Проте міжнародно-правовий обов'язок забезпечити правомірне військове використання залишається за державою. Такий підхід дозволяє уникнути розмивання відповідальності між розробником, постачальником, військовим відомством і оператором [275; 276; 281].

Універсальна доктринальна основа ООН також повинна враховувати ризик поширення військового ІІІ серед недержавних суб'єктів. Це питання має безпосередній зв'язок із міжнародною безпекою. На відміну від складних традиційних систем озброєнь, окремі елементи ІІІ можуть бути дешевшими, доступнішими і швидше адаптованими. Моделі розпізнавання, навігації, автономного керування, генерації контенту або кібернетичного аналізу можуть бути використані не лише державами, а й приватними військовими компаніями, незаконними збройними формуваннями, терористичними групами або кримінальними мережами. Це створює новий виклик для режимів експортного контролю, нерозповсюдження і кібербезпеки [275; 276; 281; 283].

Особливо небезпечним є поєднання ІІІ з кіберопераціями. Системи ІІІ можуть використовуватися для автоматизованого пошуку вразливостей, генерації фішингових кампаній, обходу захисту, створення шкідливого коду або прискорення аналізу великих масивів викрадених даних. У військовому контексті такі дії можуть впливати на критичну інфраструктуру, командні системи, зв'язок, супутникові мережі або системи раннього попередження. Правова проблема полягає в тому, що атрибуція таких дій у кіберпросторі вже є складною, а використання ІІІ може додатково ускладнити встановлення джерела, наміру і рівня контролю держави. Тому питання військового ІІІ неминуче перетинається з міжнародно-правовими дискусіями щодо відповідальної поведінки держав у кіберпросторі [275; 276; 281; 283].

Окремо слід враховувати генеративний ІІІ. Його військове значення не обмежується створенням текстів або зображень. Генеративні моделі можуть використовуватися для інформаційно-психологічних операцій, створення синтетичних

доказів, імітації командних повідомлень, маніпуляції суспільними настроями, деморалізації населення або військ, а також для автоматизованого створення пропагандистських матеріалів. У контексті міжнародного права це піднімає питання втручання у внутрішні справи держав, поваги до прав людини, захисту цивільного населення від інформаційного впливу під час збройного конфлікту і відповідальності за дезінформаційні операції. Саме тому безпековий вимір ІІІ у підході ООН є ширшим за питання фізичного ураження [275; 276; 281].

Питання ядерної стабільності є ще одним перспективним і водночас небезпечним напрямом. Поєднання ІІІ з системами раннього попередження, аналізом ракетних пусків, командно-контрольними системами або оцінкою стратегічних сигналів може скоротити час прийняття рішень і підвищити ризик помилкової ескалації. Навіть якщо ІІІ не приймає рішення про застосування ядерної зброї, його рекомендації або автоматизована оцінка можуть вплинути на сприйняття загрози. У кризовій ситуації помилка алгоритму або неправильно інтерпретований сигнал може мати катастрофічні наслідки. Саме тому ООН розглядає військовий ІІІ у зв'язку з контролем над озброєннями, роззброєнням і нерозповсюдженням [275; 276; 283].

У контексті біотехнологій і хімічних технологій ризик полягає у прискоренні досліджень, моделюванні речовин, аналізі біологічних процесів або оптимізації виробничих схем. ІІІ може використовуватися для корисних медичних, захисних і дослідницьких цілей, але також може підвищувати ризик зловживань. Саме подвійне використання тут проявляється особливо гостро. Технологія, яка допомагає розробляти ліки або засоби захисту, теоретично може бути використана для небезпечного моделювання у військових або терористичних цілях. Тому універсальний підхід ООН до військового ІІІ повинен бути пов'язаний з режимами нерозповсюдження, біобезпеки, хімічної безпеки і міжнародного контролю чутливих технологій [275; 276; 283].

Значення резолюції № 79/239 полягає також у формуванні мови майбутнього регулювання. Документ закріплює такі базові категорії, як військовий домен ІІІ, життєвий цикл, відповідальне застосування, міжнародний мир і безпека, комплексний

підхід, обмін знаннями, передовий досвід, подолання розривів, *human control in the use of force* [276]. Ці категорії поступово можуть перетворитися на елементи майбутнього правового режиму. Поки що вони не мають повної договірної конкретизації, але саме через них держави починають однаково описувати проблему. Для міжнародного права це важливо, оскільки правова норма не може ефективно сформуватися без спільної термінології [275; 276].

Перехід від *soft law* до юридично зобов'язуючих норм може відбуватися кількома шляхами. Перший шлях полягає у поступовому розвитку спеціального договору щодо найбільш ризикових автономних систем озброєнь. Такий договір міг би встановити заборону систем, які не дозволяють забезпечити змістовний людський контроль, а також обмеження для інших автономних систем. Другий шлях передбачає прийняття політико-правових стандартів або керівних принципів для всього військового ШІ, які згодом можуть бути імplementовані у національне законодавство. Третій шлях полягає у розвитку секторальних режимів, наприклад для кібероперацій, ядерної стабільності, контролю експорту, біобезпеки або військових закупівель. Четвертий шлях пов'язаний із формуванням звичаєвих очікувань щодо належної обачності держав при використанні військового ШІ [275; 276; 281].

Найбільш реалістичною на сучасному етапі є змішана модель. Вона передбачає поєднання універсальних резолюцій ООН, роботи CCW щодо автономних систем, позицій МКЧХ, національних стратегій, регіональних стандартів, технічних процедур, добровільних декларацій і практик відповідального використання. Така модель не є ідеальною, оскільки вона фрагментарна і повільна. Проте вона відповідає реальній структурі міжнародного права у сфері нових технологій. Спочатку формується м'яке право, потім виникають повторювані практики, далі уточнюються поняття, після цього з'являються секторальні або рамкові зобов'язання. Саме в цій логіці резолюція № 79/239 може розглядатися як початковий універсальний елемент майбутнього правового режиму [275; 276; 278; 282].

Водночас необхідно чітко визначити межі резолюції № 79/239. Вона не вирішує питання юридичної відповідальності за шкоду, завдану військовим ШІ. Вона не

встановлює єдиного визначення автономної системи озброєнь. Вона не визначає мінімальний стандарт людського контролю. Вона не створює процедуру обов'язкового аудиту або міжнародної сертифікації. Вона не встановлює спеціального режиму контролю експорту військових систем III. Вона не забороняє конкретні застосування. Тому її не можна перебільшено тлумачити як завершене регулювання. Її значення полягає в іншому: вона фіксує мінімальну універсальну згоду щодо того, що військовий III є предметом міжнародного права, має оцінюватися через мир і безпеку, потребує відповідального застосування і не може розвиватися без багатостороннього діалогу [275; 276].

У перспективі подальша роль ООН може розвиватися в кількох напрямках. По-перше, може бути посилено звітність Генерального секретаря щодо наслідків військового III. По-друге, можуть розвиватися спеціальні експертні формати для узгодження термінології, стандартів життєвого циклу і процедур оцінки ризиків. По-третє, ООН може координувати обмін інформацією між державами щодо національних підходів, уроків використання і передових практик. По-четверте, може бути розширена робота з подолання технологічного розриву між державами. По-п'яте, може бути встановлено зв'язок між військовим III та чинними режимами контролю над озброєннями, кібербезпеки, нерозповсюдження і прав людини [275; 276; 281; 283].

Підсумково універсальний підхід ООН до військового III можна охарактеризувати як доктринальне закріплення чотирьох базових положень. Перше положення полягає в тому, що військовий III не перебуває поза міжнародним правом. Друге положення полягає в тому, що правова оцінка повинна охоплювати весь життєвий цикл системи. Третє положення полягає в тому, що військовий III має оцінюватися з урахуванням наслідків для міжнародного миру і безпеки, а не лише через технічну ефективність. Четверте положення полягає в тому, що відповідальне застосування потребує людиноцентричності, підзвітності, безпечності, надійності, довіри, людського контролю і міжнародної співпраці [275; 276; 281].

Таким чином, ООН не створила заведеної системи правового регулювання військового III, але сформувала універсальну доктринальну основу для її подальшого

становлення. Ця основа має особливе значення саме тому, що вона універсальна. Вона не належить окремому альянсу, регіону або групі технологічно розвинених держав. Вона фіксує мінімальну позицію міжнародного співтовариства щодо того, що військовий ІІІ має бути предметом правового контролю, оцінки ризиків, людської відповідальності і багатосторонньої співпраці. У подальшому саме ця основа може бути використана для розроблення спеціальних міжнародно-правових норм, модельних стандартів, національних процедур, технічних протоколів і механізмів запобігання шкоді [275; 276].

Для загальної логіки дослідження це означає, що ООН виступає універсальним рівнем становлення міжнародного права штучного інтелекту у військовій сфері. REAIM забезпечує багатосторонню політико-експертну розробку принципів. НАТО формує союзницьку оборонну модель імплементації. МКЧХ задає гуманітарно-правову межу щодо автономної зброї. ООН узагальнює ці процеси і переводить їх у площину універсального міжнародного порядку. Саме тому підрозділ про ООН має розглядатися як центральний для розуміння того, як фрагментарні ініціативи поступово набувають форми загальної доктринальної рамки міжнародно-правового регулювання військового ІІІ [275; 276; 282].

Висновки до 3-го розділу

У третьому розділі досліджено перехід від регіональних і союзницьких підходів до перших універсальних доктринальних закріплень у сфері військового ІІІ. У роботі показано, що REAIM і ООН не є ізольованими міжнародними майданчиками, а формують послідовний механізм становлення майбутнього міжнародно-правового режиму. REAIM виконує функцію політико-експертного простору, у якому виробляються первинні засади відповідального використання ІІІ у військовій сфері, тоді як ООН переводить ці підходи на універсальний рівень міжнародного миру і безпеки. Вперше у межах дослідження REAIM розглянуто не лише як конференційний формат, а як проміжне нормативне середовище, що розширило предмет регулювання від летальних автономних систем озброєнь до всього військового домену ІІІ.

Фахова новизна розділу полягає у тому, що резолюцію Генеральної Асамблеї ООН № 79/239 розглянуто як перше універсальне доктринальне закріплення підходу до військового ІІІ, а не як звичайний політичний акт. Доведено, що її значення полягає у фіксації трьох ключових положень: військовий ІІІ не перебуває поза міжнародним правом; правова оцінка має охоплювати весь життєвий цикл системи; відповідальне використання потребує людського контролю, підзвітності, надійності, управління ризиками і міжнародної співпраці. У цьому аспекті розділ доводить центральну тезу роботи: міжнародно-правове регулювання військового ІІІ формується не через одномоментне прийняття договору, а через поступове поєднання політичних декларацій, м'якого права, гуманітарно-правових меж, союзницьких стандартів і універсальних доктринальних актів.

ВИСНОВКИ

Досліджено Становлення міжнародно-правового регулювання використання штучного інтелекту у військових цілях як складного міжгалузевого процесу, що формується на перетині міжнародного гуманітарного права, міжнародного права прав людини, права міжнародної безпеки, режимів контролю над озброєннями, кібербезпеки, технічної стандартизації та практики міжнародних організацій. Встановлено, що військовий ШІ не може розглядатися лише як новий різновид технології або окрема категорія озброєння, оскільки його правове значення полягає у здатності впливати на весь цикл прийняття рішень у сфері застосування сили. Саме тому його регулювання потребує не ізольованого технічного підходу, а комплексної міжнародно-правової моделі, яка враховує гуманітарні, безпекові, етичні, процедурні та відповідальнісні аспекти.

Проаналізовано етап становлення міжнародно-правового регулювання інституту штучного інтелекту у 2017-2026 рр. і встановлено, що на універсальному рівні досі не сформовано єдиного конвенційного визначення ні штучного інтелекту загалом, ні військового штучного інтелекту зокрема. Це зумовлює множинність підходів, за яких міжнародні та регіональні організації, зокрема ООН, ЮНЕСКО, Європейський Союз, Рада Європи, Організація економічного співробітництва та розвитку, НАТО, G7 і REAİM, використовують власні робочі визначення відповідно до своїх статутних завдань, тематичних актів, політичних декларацій або підсумкових документів. Такий стан свідчить не про відсутність регулювання, а про його поступове формування через поєднання *soft law*, політичних стандартів, регіональних актів, технічних вимог і доктринальних підходів.

Визначено, що інститут штучного інтелекту, розглянутий з позицій міжнародного права, має виразний міждисциплінарний і міжгалузевий характер. У міжнародно-правовому вимірі він формує новий комплексний об'єкт регулювання, який виходить за межі традиційних галузевих класифікацій і одночасно належить до сфери прав людини, міжнародного гуманітарного права, міжнародного економічного права, права

міжнародної безпеки, кібербезпеки, міжнародної відповідальності та права міжнародних організацій. З огляду на це, розвиток інституту ШІ не може бути зведений лише до етичних декларацій або технічної стандартизації, оскільки він безпосередньо стосується змісту міжнародно-правових обов'язків держав, меж допустимого використання новітніх технологій та процедур забезпечення контролю за їх застосуванням.

Обґрунтовано, що основна проблема міжнародно-правового регулювання військового ШІ полягає не у відсутності права як такого, а у недостатній пристосованості чинних норм до алгоритмічної, автономної та багаторівневої природи нових військових систем. Норми міжнародного гуманітарного права, міжнародного права прав людини, міжнародної відповідальності, контролю над озброєннями та міжнародної безпеки зберігають застосовність до військового ШІ, однак їх реалізація ускладнюється автономністю систем, непрозорістю алгоритмів, складністю встановлення причинного зв'язку, розподілом відповідальності між державами, розробниками, операторами і командуванням, а також швидкістю прийняття рішень у цифровому середовищі. Тому подальший розвиток регулювання має бути спрямований не на заміну чинного міжнародного права, а на створення нових процедурних форм його застосування.

Доведено, що розвиток інституту штучного інтелекту, включаючи військовий штучний інтелект, доцільно розглядати не як окремий етап науково-технічного прогресу, а як черговий етап розвитку інформаційно-комунікаційних технологій, зумовлений формуванням глобального інформаційного суспільства. У цьому контексті штучний інтелект є результатом поглиблення діджиталізації, цифрової конвергенції, масштабування транскордонних потоків даних, доступності обчислювальних ресурсів і взаємопроникнення цивільних, безпекових та військових технологій. Така природа ШІ обумовлює потребу в особливому міжнародно-правовому режимі, здатному враховувати не лише окремі ризики застосування технології, а й системні наслідки її інтеграції у глобальні правові, економічні, військові та інформаційні процеси.

Встановлено тісний взаємозв'язок між цивільними та військовими аспектами розвитку інституту штучного інтелекту. Технології подвійного призначення утворюють перетин правових режимів, оскільки інновації у сфері цивільного застосування, зокрема в медицині, транспорті, освіті, цифрових сервісах, управлінні даними та автоматизованому прийнятті рішень, одночасно можуть формувати потенціал для їхнього військового використання. Це вимагає спеціального міжнародно-правового підходу, який має поєднувати елементи міжнародного гуманітарного права, міжнародного права прав людини, права міжнародної безпеки, кібербезпеки, експортного контролю та процедурної оцінки ризиків протягом усього життєвого циклу систем ШІ.

Проаналізовано американський, європейський і далекосхідний підходи до формування базових міжнародно-правових засад використання військового штучного інтелекту. Встановлено, що ці моделі, попри відмінності у політичних, правових і технологічних акцентах, характеризуються поєднанням ідеї технологічного лідерства з категорією відповідального використання військового ШІ. Американський підхід більшою мірою зосереджений на оборонних інноваціях, інституційній адаптації та збереженні стратегічної переваги; європейський підхід акцентує увагу на правах людини, ризик-орієнтованому регулюванні, етичних стандартах і правових гарантіях; далекосхідний підхід поєднує технологічну модернізацію, державне стратегічне планування, безпекові пріоритети та інституційний контроль. У сукупності ці моделі формують емпіричну основу для подальшого становлення міжнародних стандартів військового ШІ.

Виявлено найбільш актуальні проблеми майбутнього міжнародно-правового регулювання використання технологій штучного інтелекту у військових цілях. До таких проблем належать питання летальних автономних систем озброєнь у межах Конвенції про конкретні види звичайних озброєнь, відсутність чіткої категоризації систем ШІ за рівнем автономності та ризику, неврегульованість питань відповідальності за шкоду, завдану автономними системами, складність визначення значущого людського контролю, алгоритмічна непрозорість, недостатня конкретизація механізмів

міжнародного нагляду та ризик використання ШІ у збройних конфліктах без належних гуманітарно-правових гарантій. Дослідження показало, що держави наразі не готові до укладення універсального договору про повну заборону летальних автономних систем озброєнь, однак поступово визнають необхідність значущого людського контролю як мінімального стандарту відповідального військового ШІ.

Досліджено концептуальні підходи НАТО до міжнародно-правового регулювання використання штучного інтелекту у військовій сфері. Встановлено, що модель НАТО має не договірний, а інституційно-стандартизаційний характер. Її сутність полягає у формуванні підходу відповідального військового ШІ через поєднання правових принципів, політичних зобов'язань, внутрішніх процедур оцінки, технологічної інфраструктури, інтероперабельності, тестування, інноваційної екосистеми та партнерської взаємодії. Така модель не замінює універсальне міжнародне право, але конкретизує його вимоги для оборонного середовища. Водночас визначено об'єктивні межі натівського підходу: він не має універсальної обов'язкової сили для всіх держав, значною мірою спирається на акти м'якого права і політичні стандарти, а питання відповідальності за помилки ШІ, алгоритмічну непрозорість, транскордонні наслідки та співвідношення зі майбутніми універсальними нормами залишаються недостатньо врегульованими.

Встановлено, що розвиток військової сфери інституту штучного інтелекту в межах міжнародних конференцій має особливе значення для поступового формування спільного політико-правового простору. На відміну від НАТО, яка виробляє стандарти відповідального військового ШІ в межах союзницької оборонної архітектури, REAIM слід розглядати як глобальний політико-правовий процес, спрямований на вироблення спільного розуміння ризиків, можливостей, процедурних гарантій і напрямів подальшого регулювання військового застосування технологій ШІ. Значення REAIM полягає не у створенні юридично обов'язкових норм, а у формуванні первинного широкого консенсусу держав щодо того, що військовий ШІ не може залишатися поза міжнародним контролем, а його розроблення, розгортання і використання повинні

оцінюватися через призму міжнародного права, міжнародної безпеки, гуманітарних наслідків і відповідальності людини.

Обґрунтовано, що формування універсальних доктринальних основ використання штучного інтелекту у військовій сфері в межах Організації Об'єднаних Націй є окремим етапом становлення міжнародно-правового регулювання новітніх військових технологій. Його специфіка полягає не у створенні завершеного договірного режиму, а у визначенні загальних правових, гуманітарних, технічних, етичних і безпекових орієнтирів, які мають універсальний характер і можуть бути використані державами для розвитку національних стратегій, міждержавної співпраці та майбутніх міжнародно-правових інструментів. На відміну від регіональних або союзницьких підходів, позиція ООН спрямована на вироблення мінімально узгодженої основи для всіх держав незалежно від рівня їхнього технологічного розвитку, військово-політичної орієнтації або участі в окремих оборонних альянсах.

Сформульовано авторську концепцію перспективного розвитку міжнародного права у сфері штучного інтелекту. Вона передбачає закріплення універсальних базових принципів, зокрема людиноцентричності, значущого людського контролю, відповідальності, пропорційності, прозорості та підзвітності; створення спеціалізованих міжнародних механізмів контролю; розроблення окремих міжнародно-правових підходів для цивільної і військової сфер з урахуванням їхнього перетину як технологій подвійного використання; забезпечення інтеграції міжнародного права з національними правовими системами з метою уникнення нормативної фрагментації. Такий підхід дозволяє розглядати військовий ШІ не фрагментарно, а як цілісний об'єкт міжнародно-правового регулювання.

Визначено теоретичне і практичне значення одержаних результатів. Теоретичне значення полягає у формуванні доктринальної основи для розуміння військового ШІ як нового комплексного напрямку міжнародно-правового регулювання, у межах якого класичні норми міжнародного права не відкидаються, а набувають нових процедурних форм реалізації. Практичне значення полягає у можливості використання сформованих у роботі висновків для подальшого аналізу національних стратегій, розроблення

модельних стандартів правової експертизи систем III, оцінки відповідності військових технологій міжнародному гуманітарному праву, а також підготовки позицій держав у межах ООН, REAIM, CCW, НАТО та інших міжнародних форматів.

Узагальнено, що становлення міжнародно-правового регулювання використання III у військовій сфері відбувається поступово і багаторівнево. На першому рівні формуються національні та регіональні моделі, які випробовують різні способи поєднання технологічних інновацій і правового контролю. На другому рівні союзницькі структури, зокрема НАТО, переводять етичні й правові принципи у процедури інтероперабельності, тестування і впровадження. На третьому рівні REAIM створює політико-експертний простір для вироблення спільної мови відповідального військового III. На четвертому рівні ООН надає цим процесам універсального доктринального значення. Саме поєднання цих рівнів дає підстави стверджувати, що міжнародне право поступово переходить від загального визнання ризиків військового III до формування майбутнього режиму його відповідального, підконтрольного і правомірного використання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Міністерство освіти і науки України; Маріупольський державний гуманітарний університет; Представництво Європейської організації публічного права в Україні. Баймуратов М. О. Міжнародне публічне право: підручник. Харків: Одиссей, 2008. ББК 67.9 Б22.
2. Chesterman S. Weapons of Mass Disruption: Artificial Intelligence and International Law. *Cambridge International Law Journal*. 2021. Vol. 10. P. 181–203.
3. United Nations. Secretary-General's remarks to the Security Council on Artificial Intelligence. New York, 18 July 2023.
4. International Committee of the Red Cross. Preserving Human Control over the Use of Force: A Call to Regulate Lethal Autonomous Weapon Systems under International Law (Statement). Geneva, 12 May 2025.
5. Deeks A. Introduction to the Symposium: How Will Artificial Intelligence Affect International Law? *AJIL Unbound*. 2020. Vol. 114. P. 138–140.
6. Deeks A. High-Tech International Law. *The George Washington Law Review*. 2020. Vol. 88. P. 574–634.
7. Crootoof R. War Torts: Accountability for Autonomous Weapons. *University of Pennsylvania Law Review*. 2016. Vol. 164, № 6. P. 1347–1402.
8. Crootoof R. Autonomous Weapon Systems and the Limits of Analogy. *Harvard National Security Journal*. 2018. Vol. 9. P. 51–83.
9. Crawford J. *Brownlie's Principles of Public International Law*. 8th ed. Oxford: Oxford University Press, 2012. P. 115–126.
10. European Parliament. Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). P. 59(f).
11. Solum L. B. Legal Personhood for Artificial Intelligences. *North Carolina Law Review*. 1992. Vol. 70. P. 1231–1287.
12. Bryson J. J., Diamantis M. E., Grant T. D. Of, for, and by the people: the legal lacuna of synthetic persons. *Artificial Intelligence and Law*. 2017. Vol. 25. P. 273–291.

13. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO, 2021.
14. Council of Europe. Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). Strasbourg, 2024.
15. OECD. Recommendation of the Council on Artificial Intelligence. Paris, 2019.
16. G7 Leaders. G7 Leaders' Statement on the Hiroshima AI Process. 30 Oct. 2023. The White House.
17. Деркач О. О. Діджиталізації та розвиток штучного інтелекту: міжнародно-правові стандарти: стаття (рукопис). Київ, б.р.
18. Деркач О. О. Міжнародний захист прав людини в умовах діджиталізації та розвитку штучного інтелекту: міжнародно-правові стандарти. Наук. публікація. 2024. № 4. DOI: 10.32782/2663-5666.2024.4.15.
19. Деркач О. О. Американський науковий підхід до міжнародно-правового регулювання штучного інтелекту: тези доповіді. Київ: ІМВ КНУ ім. Т. Шевченка, б.р.
20. Derkach O. Artificial intelligence — analysis of the legal framework in the parallel civilian and military spheres: conference theses. Uzhhorod, б.р.
21. Деркач О. О. Стаття: «Аналіз виникнення ІІ та аналіз правової бази»: рукопис (робочі матеріали). Київ, б.р.
22. Деркач О. О. Формування міжнародно-правових стандартів захисту прав людини в умовах діджиталізації та використання штучного інтелекту: стаття (рукопис). Київ, б.р.
23. Hárs Á. Artificial Intelligence and International Law: Between Realism and Hype. Hungarian Journal of Legal Studies. 2021. Vol. 62(4). P. 320–344.
24. Lemnitzer J. M. Back to the Roots: The Laws of Neutrality and the Future of Due Diligence in Cyberspace. European Journal of International Law. 2022. Vol. 33(3). P. 789–819.
25. World Intellectual Property Organization. The WIPO Conversation on Intellectual Property and Artificial Intelligence. WIPO.

26. International Maritime Organization. Autonomous ships: regulatory scoping exercise completed (MSC 103). IMO.
27. Council of Europe. Convention on Cybercrime (Budapest Convention). 2001.
28. UNFCCC. Paris Agreement. 2015.
29. Altman S. Written Testimony before the U.S. Senate Judiciary Subcommittee on Privacy, Technology, & the Law. 16 May 2023.
30. U.S. Congress. Oversight of A.I.: Rules for Artificial Intelligence — hearing transcript. 16 May 2023.
31. United Nations. Interim Report of the High-Level Advisory Body on Artificial Intelligence. 2023.
32. GAO. Autonomous Ships and Efforts to Regulate Them (GAO-24-107059). Washington, DC, 2024.
33. Orzechowski S. C. Regulatory scoping exercise for the future adoption of MASS Code. *Journal of Shipping and Trade*. 2024.
34. WIPO. Revised Issues Paper on IP Policy and AI (WIPO/IP/AI/2/GE/20/1 REV.). 2020.
35. WIPO. Generative AI: Navigating Intellectual Property (Factsheet). 2024.
36. Dias T., Coco A. *Cyber Due Diligence in International Law*. ELAC, University of Oxford, 2021.
37. Schmitt M. N. (ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: CUP, 2017.
38. Jensen E. T. The Tallinn Manual 2.0: Highlights and Insights. *Georgetown Journal of International Law*. 2018. Vol. 48(3).
39. UNOOSA. Liability Convention — reference page. UNOOSA.
40. U.S. Dept. of State. *Convention on International Liability for Damage Caused by Space Objects*. 2017.
41. Kulińska-Kępa Z. *The Convention on International Liability for Damage Caused by Space Objects: Selected Issues*. 2023.

42. van Maanen G. AI Ethics, Ethics Washing, and the Need to Politicize Data Ethics. AI and Ethics. 2022.
43. Rudschies C. Value Pluralism in the AI Ethics Debate. International Review of Information Ethics. 2020.
44. Bietti E. From Ethics Washing to Ethics Bashing. FAT'20 Adjunct. ACM, 2020.
45. Future of Life Institute. Asilomar AI Principles. 2017.
46. Wyckoff A. W. A new institution for governing AI? Lessons from GPAI. Brookings, 2024.
47. OECD AI Policy Observatory. Background – GPAI joins forces with OECD. OECD, July 2024.
48. Reuters. UN chief backs idea of global AI watchdog like nuclear agency. 12 June 2023.
49. UK Government. The Bletchley Declaration. 1–2 Nov. 2023.
50. EUR-Lex. Regulation (EU) 2024/1689 — Artificial Intelligence Act. OJ L, 12 July 2024.
51. OECD. GPAI and OECD unite to advance coordinated international efforts for trustworthy AI. Press release, 3 July 2024.
52. OECD.AI. About the Global Partnership on Artificial Intelligence (GPAI). OECD.
53. Montréal International. The Global Partnership on Artificial Intelligence officially launched. 15 June 2020.
54. OECD.AI Policy Observatory. Integrated Partnership Between OECD and GPAI. Updated 2025.
55. GPAI Data Governance Working Group. Report 2023. GPAI.
56. OECD.AI / GPAI. Responsible AI Working Group — projects. OECD.
57. UK Government. Frontier AI Safety Commitments — AI Seoul Summit 2024. GOV.UK.
58. Encyclopaedia Britannica. MYCIN: рання медична експертна система (1972). Encyclopaedia Britannica.

59. Boulanin V., Verbruggen M. Mapping the Development of Autonomy in Weapon Systems. SIPRI Report, 2017.
60. Israel Aerospace Industries. HARPY — Fire-and-Forget autonomous loitering munition. IAI, офіц. сторінка.
61. U.S. Department of Defense. DoD Directive 3000.09: Autonomy in Weapon Systems. Updated 25 Jan. 2023. Washington, DC: DoD.
62. International Committee of the Red Cross. A Guide to the Legal Review of New Weapons, Means and Methods of Warfare (ст. 36 ДП I). Geneva: ICRC, 2020.
63. PAX; Stop Killer Robots. Slippery Slope: The arms industry and increasingly autonomous weapons. 2021.
64. Council of Europe. Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes. 13 Feb. 2019. Strasbourg: CoE.
65. Council of Europe. Committee of Ministers. Recommendation CM/Rec(2020)1 to member States on the human rights impacts of algorithmic systems. 8 Apr. 2020. Strasbourg: CoE.
66. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO, 2021.
67. United Nations Office for Disarmament Affairs (UNODA). Lethal Autonomous Weapon Systems (LAWS) in the CCW — background and timeline. 2018–2024. New York: UNODA.
68. U.S. Department of State. Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy. Launched at REAIM 2023. 2023. Washington, DC.
69. Government of the Netherlands. REAIM 2023 — Endorsing Countries and Territories / Political Declaration on the Responsible Use of AI in the Military Domain. 16 Feb. 2023. The Hague: Netherlands Government.
70. ISO/IEC JTC 1/SC 42. Artificial Intelligence — committee scope and catalogue. Geneva: ISO, 2023–2025.

71. International Telecommunication Union (ITU). AI/ML pre-standardization; Focus Group on AI for Autonomous and Assisted Driving (AI4AD). 2020–2024. Geneva: ITU.
72. RAND Corporation. Moscow's Lessons from the 1982 Lebanon Air War. Santa Monica: RAND, 1982.
73. RAND Corporation. Background on the Israeli Air Campaign. Research Brief. Santa Monica: RAND, 1982.
74. Smithsonian Air & Space. The Predator, a Drone That Transformed Military Combat. Washington, DC: Smithsonian, 2015.
75. The Atlantic. The Story of America's First Drone Strike in Afghanistan. 2002.
76. New America. America's Counterterrorism Wars: The War in Yemen. Washington, DC: New America Foundation, 2002.
77. United Nations Human Rights Council (UN HRC). Philip Alston. Report on Targeted Killings. 2010. UN Digital Library.
78. United Nations Human Rights Council (UN HRC). Christof Heyns. Report on Lethal Autonomous Robotics. 2013. UN Docs.
79. Office of the High Commissioner for Human Rights (OHCHR). Call for a Moratorium on Lethal Autonomous Robots. 2013. Geneva: OHCHR.
80. Peshawar High Court. Foundation for Fundamental Rights v. Federation of Pakistan. 2013. ICRC Casebook.
81. International Committee of the Red Cross. Casebook. North Rhine-Westphalia Higher Administrative Court (Ramstein). 2013. ICRC.
82. Beinlich L. Germany and its Role in the US Drone Programme. SSRN Papers, 2014.
83. UK Court of Appeal. Noor Khan v. Secretary of State for Foreign and Commonwealth Affairs. 2014. Just Security.
84. Courts and Tribunals Judiciary (UK). Khan v SSFCA. High Court judgment, 2012.

85. Center for Strategic and International Studies (CSIS). Why Ukraine Is Establishing Unmanned Forces. 2024.
86. Reuters. Ukraine sees ‘priceless’ digital battlefield data. 2025.
87. The Wall Street Journal. AI-Powered Drone Swarms Have Now Entered the Battlefield. 2025.
88. The Kyiv Independent. Ukraine unites Unmanned Systems Forces with top ‘Drone Line’. 2025.
89. CSIS. Understanding the Military AI Ecosystem of Ukraine. 2024.
90. NATO Allied Command Transformation (ACT). Delta System at CWIX: interoperability and real-time exchange. 2024.
91. Center for European Policy Analysis (CEPA). Adaptation Under Fire: Russia’s Kill Chain in Ukraine. 2025.
92. NAKO (Independent Anti-Corruption Committee on Defense). Ukrainian Unmanned Systems Forces — new structure. 2024.
93. Euromaidan Press. DELTA battlefield management system. 2025.
94. CSIS Event. Russia-Ukraine Drone War: Innovation. 2025.
95. Financial Times. How Russia is jamming GPS around Europe. 2025.
96. Army-Technology. Lancet Loitering Munition System. 2024.
97. Institute for the Study of War (ISW). Status of Current Russian and Ukrainian AI Drone Efforts. 2025.
98. Royal United Services Institute (RUSI). Methodology for Degrading the Arms of the Russian Federation. 2024.
99. CSIS; NATO. Analysis of Delta and CJADC2 interoperability and C2 algorithms. 2024–2025.
100. Забара І. М. Штучний інтелект у військовій сфері: становлення доктринальних основ міжнародно-правового регулювання в рамках ООН. 2025.
101. Забара І. М. Стратегія НАТО в області штучного інтелекту: становлення і розвиток концептуальних міжнародно-правових засад (2021–2024). 2025.
102. United Nations. Pact for the Future — Summit of the Future. 22 Sept. 2024.

103. United Nations. Global Digital Compact — Summit of the Future. 22 Sept. 2024.
104. UN General Assembly. A/RES/79/1 Pact for the Future. 22 Sept. 2024.
105. UNODA. Yearbook 2024. Ch. 5: згадування Пакту та Глобального цифрового компакту.
106. OECD. Digital transformation — policy issue page. Paris: OECD, 2024.
107. Liu S. та ін. Is Generative AI a General-Purpose Technology? OECD AI Papers No. 40. 17 June 2025. Paris: OECD.
108. ISO. ISO/IEC 42001:2023. Artificial intelligence — Management system requirements. Geneva: ISO, 2023.
109. Council of Europe. Declaration on the manipulative capabilities of algorithmic processes. Strasbourg: CoE, 2019.
110. ITU. WSIS+20 High-Level Event 2025 — information page. 7–11 July 2025. Geneva: ITU.
111. ITU. WSIS+20 High-Level Event 2025 — Highlights & Outcomes. 11 July 2025. Geneva: ITU.
112. International Monetary Fund (IMF). Gopinath G. та ін. Changing Global Linkages: A New Cold War? WP/24/076. April 2024.
113. World Trade Organization (WTO). Global Trade Outlook and Statistics 2024. WTO, 2024.
114. UN General Assembly. A/RES/79/239 Artificial intelligence in the military domain and its implications for international peace and security. 24–31 Dec. 2024. UNIDIR.
115. United Nations — Office for Digital and Emerging Technologies. Global Digital Compact (policy hub). New York: UN, 2024.
116. OECD. Risks and Resilience in Global Trade. Dec. 2024. OECD.
117. Giddens A. The Consequences of Modernity. Cambridge: Polity Press, 1990.
118. Held D., McGrew A., Goldblatt D., Perraton J. Global Transformations: Politics, Economics and Culture. Cambridge: Polity, 1999.
119. Sassen S. The Global City: Introducing a Concept. Brown Journal of World Affairs. 2005.

120. Castells M. The Rise of the Network Society. Oxford: Blackwell, 1996.
121. Castells M., Cardoso G. (eds.). The Network Society: From Knowledge to Policy. Washington, DC: Johns Hopkins Center for Transatlantic Relations, 2005.
122. Baldwin R. The Great Convergence: Information Technology and the New Globalization. Cambridge, MA: Harvard University Press, 2016.
123. Rodrik D. The Globalization Paradox: Democracy and the Future of the World Economy. New York: W. W. Norton, 2011.
124. International Monetary Fund (IMF). Annual Report 2024: Sustaining the Recovery. Washington, DC: IMF, 2024.
125. World Trade Organization (WTO). Global Trade Outlook and Statistics 2024–2025. Geneva: WTO, 2024.
126. Okonjo-Iweala N. (WTO). Statements and Interviews on Trade Challenges. Geneva: WTO, 2025.
127. Manyika J. et al. Digital Globalization: The New Era of Global Flows. McKinsey Global Institute, 2016.
128. McCarthy J., Minsky M., Rochester N., Shannon C. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. 1955. Stanford University.
129. ResearchGate. Огляд становлення американської школи III та хвилі глибинного навчання. 2018.
130. Defense Advanced Research Projects Agency (DARPA). The DARPA Grand Challenge: Ten Years Later. Arlington, VA: DARPA, 2014.
131. Roland A. Strategic Computing. Cambridge, MA: MIT Press; ACM Digital Library, 2002/2015.
132. Gomez-Uribe C. A., Hunt N. The Netflix Recommender System: Algorithms, Business Value, and Innovation. ACM Transactions on Management Information Systems, 2016.
133. Covington P., Adams J., Sargin E. Deep Neural Networks for YouTube Recommendations. RecSys Conference, 2016.

134. Food and Drug Administration (FDA). ID_x-DR (DEN180001) Decision Summary. Washington, DC: FDA, 2018.
135. ProPublica. Machine Bias: Investigating the COMPAS Algorithm. 2016.
136. National Highway Traffic Safety Administration (NHTSA). Recall 23V-838 and EA22002 Investigation Memo. Washington, DC: NHTSA, 2023–2024.
137. U.S. Congress. National Artificial Intelligence Initiative Act of 2020. Washington, DC: Congress.gov.
138. White House, Office of Science and Technology Policy (OSTP). Blueprint for an AI Bill of Rights. Washington, DC: OSTP, 2022.
139. White House, OSTP. What is the Blueprint for an AI Bill of Rights? Washington, DC: OSTP, 2022.
140. Federal Register. Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (EO 14110). 1 Nov. 2023. Washington, DC.
141. White House. Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI. 30 Oct. 2023. Washington, DC.
142. National Institute of Standards and Technology (NIST). AI Risk Management Framework 1.0. Washington, DC: NIST, 2023.
143. Office of Management and Budget (OMB). Memorandum M-24-10: Advancing Governance, Innovation, and Risk Management for Agency Use of AI. Washington, DC: OMB, 28 Mar. 2024.
144. White House. Removing Barriers to American Leadership in Artificial Intelligence. Washington, DC: White House, 23 Jan. 2025.
145. The Verge. Donald Trump rescinds Biden-era executive order on AI safety. 21 Jan. 2025.
146. Food and Drug Administration (FDA). Artificial Intelligence and Machine Learning in Software as a Medical Device: Guidance Portal. Updated 25 Mar. 2025.
147. FDA. Final Guidance: Marketing Submission Recommendations for a Predetermined Change Control Plan for AI-Enabled Device Software Functions. 11 Dec. 2024; updates 2025.

148. U.S. Equal Employment Opportunity Commission (EEOC); DOJ; CFPB; FTC. Joint Statement on Enforcement Efforts against Discrimination and Bias in Automated Systems. 25 Apr. 2023.
149. EEOC. Technical Assistance: Assessing Adverse Impact under Title VII in AI and Other Software. 18 May 2023.
150. Mayer Brown. EEOC Issues Title VII Guidance on Employer Use of AI. Client Alert. 6 July 2023.
151. Law & The Workplace. EEOC Releases Technical Document on AI and Title VII. 23 May 2023.
152. Federal Trade Commission (FTC). Press Release: No AI exemption to the laws on the books. 25 Apr. 2023.
153. Consumer Financial Protection Bureau (CFPB). Automated systems not an excuse for lawbreaking behavior. Newsroom. 25 Apr. 2023.
154. U.S. Department of Justice (DOJ), Civil Rights Division. Joint statement on civil rights enforcement and automated systems. Updated 4 Apr. 2024.
155. California Office of the Attorney General (OAG). California Consumer Privacy Act (CCPA). Official Resource. Sacramento, 2023.
156. California Privacy Protection Agency (CPPA). Regulations & Rulemaking under CPRA/CCPA. Sacramento, 2023.
157. New York City Department of Consumer and Worker Protection (DCWP). Automated Employment Decision Tools (Local Law 144/2021). NYC, 2023.
158. Inside Privacy, Covington. NYC AI Rule to Take Effect July 5, 2023. 26 Apr. 2023.
159. National Association of Attorneys General (NAAG). A Deep Dive into Colorado's Artificial Intelligence Act. 26 Oct. 2024.
160. Colorado General Assembly. SB24-205: Consumer Protections for Artificial Intelligence. Denver, 2024.
161. Reuters. New state privacy laws create a patchwork of obligations. 7 June 2024.

162. Brennan Center for Justice. Artificial Intelligence Legislation Tracker (118th Congress). New York, 2024.
163. National Conference of State Legislatures (NCSL). Artificial Intelligence 2024 Legislation. Washington, DC: NCSL, 2024.
164. White & Case. AI Watch: Global regulatory tracker — United States. White & Case LLP, 2024.
165. National Institute of Standards and Technology (NIST). Artificial Intelligence Safety Institute Consortium (AISIC). Washington, DC: NIST, 2024.
166. NIST. U.S. AI Safety Institute signs agreements with Anthropic & OpenAI. Washington, DC: NIST, 2024.
167. The Future Society. Launch and founding members of GPAI. June 2020.
168. UK Government. The Bletchley Declaration. AI Safety Summit, Nov. 2023. London: GOV.UK.
169. UK Government. Frontier AI Safety Commitments, AI Seoul Summit 2024. GOV.UK, 2024.
170. U.S. Department of State. Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy. Washington, DC, 2023.
171. U.S. Mission Geneva. U.S. Statements on Human Judgment/Control in LAWS Discussions. Geneva, 2016–2023.
172. Congressional Research Service (CRS). In Focus IF11150. U.S. Policy on Lethal Autonomous Weapons Systems. Updated 2 Jan. 2025. Washington, DC: CRS.
173. UNODA. Background & GGE meetings on LAWS. New York: UNODA, 2024.
174. Reuters. Nations meet at UN for 'killer robot' talks as regulation lags. 12 May 2025.
175. U.S. Senate Judiciary Subcommittee. Oversight of A.I.: Rules for Artificial Intelligence. Hearing, 16 May 2023. Washington, DC.
176. Axios. OpenAI CEO Sam Altman calls for regulation before AI gets out of hand. 16 May 2023.

177. Future of Life Institute. Pause Giant AI Experiments: An Open Letter. Mar.–May 2023.
178. Reuters. Elon Musk launches AI firm xAI. 12 July 2023.
179. White House. Readout of Meeting with CEOs on AI. 4 May 2023.
180. White House. Voluntary Commitments from Leading AI Companies. 21 July 2023.
181. UK Ministry of Defence. Defence Artificial Intelligence Strategy. 15 June 2022. London: GOV.UK.
182. UK Ministry of Defence. The Defence AI Playbook. London: MOD, 2024. GOV.UK (PDF).
183. Government Communications Headquarters (GCHQ). Artificial Intelligence at GCHQ. Official explainer page. London: GCHQ, 2023.
184. Reuters. UK's GCHQ head says AI is critical to national security. 2021.
185. Reuters. Macron sets out France's AI ambitions; funding and strategy announcements. 2018; follow-ups 2025.
186. Ministère des Armées (France). Comprendre l'IA de défense: політика, часові рамки та створення AMIAD. Paris: defense.gouv.fr, 1 May 2024.
187. Ministère des Armées (France). La Donnée et l'IA: огляд інституцій і програм; підтвердження запуску AMIAD. Paris: defense.gouv.fr, 5 May 2024.
188. DefenseNews. France reallocates €2B for military AI; new supercomputing for defence. 18 June 2024.
189. European Parliament. Defence and Artificial Intelligence – Key issues and recent developments. Briefing, 25 Feb. 2025. Brussels: European Parliament.
190. UK Government. AI Safety Summit 2023 (Bletchley Park). Офіційна сторінка події; матеріали та «Bletchley Declaration». London: GOV.UK, 2023.
191. UK Government. Prime Minister's speech at the AI Safety Summit. 2 Nov. 2023. London: GOV.UK.
192. UK Government / Cabinet Office. Chair's Summary of the AI Safety Summit 2023. 1 Nov. 2023. London: GOV.UK.

193. UK Defence Digital. The Defence AI Centre: harnessing AI across Defence. 10 Mar. 2023. Defence Equipment & Support.
194. UK Parliament, Defence Committee. Developing AI capacity and expertise in UK Defence (HC 590). 10 Jan. 2025. London: Parliament.uk.
195. UK Government. Response to HC 590. 4 Apr. 2025. London: GOV.UK.
196. U.S. Department of Defense. DoD Directive 3000.09: Autonomy in Weapon Systems. Washington, DC: DoD, updated 25 Jan. 2023.
197. AeroVironment. Switchblade 300 Loitering Munition Systems. Product documentation.
198. AeroVironment. Switchblade 600 Loitering Munition Systems. Product documentation.
199. U.S. Department of State. Political Declaration on Responsible Military Use of AI and Autonomy. Washington, DC: DoS, 2023.
200. WIRED. Material on Project Maven and Google protests. 29 May 2018.
201. U.S. Department of Defense. Responsible AI Strategy & Implementation Pathway. Washington, DC: DoD, June 2022.
202. U.S. Department of Defense. Compliance Plan (OMV/OMB requirements, EO 14110). Washington, DC: DoD, 19 Sept. 2024.
203. Reuters. Global military AI market growth and lessons from Ukraine, Gaza. 2025.
204. Wall Street Journal. U.S. Army contract for edge-AI deployment (TurbineOne). 2025.
205. Zabara I. M. Artificial Intelligence in the Military Sphere: Doctrinal Foundations of International Legal Regulation in the UN Framework. 2025.
206. NATO. NATO's Artificial Intelligence Strategy. Brussels: NATO, 2021.
207. NATO. Principles of Responsible Use of AI in Defence. Brussels: NATO, 2021–2025.
208. NATO DIANA. Defence Innovation Accelerator for the North Atlantic — overview/test centres network. Brussels: NATO, 2023.

209. NATO Innovation Fund. About and investment scope. Brussels: NATO, 2023.
210. U.S. Department of State. Political Declaration on Responsible Military Use of AI and Autonomy. 2023. docs.un.org.
211. REAIM. Responsible AI in the Military Domain (The Hague 2023 / Seoul 2024). Wikipedia, 2024.
212. Tencent. Tencent Miying's AI Electronic Colposcopy-Aided Screening; Value for Users, Tech for Good. Beijing, 22 May 2019; 11 Nov. 2019.
213. iFLYTEK. About / Create a Better World with AI. Hefei: iFlytek Co., 1999–2025 (оновл.).
214. DJI. Newsroom: засновник Frank Wang; підтвердження заснування та роль CEO. Shenzhen: DJI, 21 Dec. 2015; 22 Sept. 2016.
215. Megvii. Founders & Corporate Background. Пекін: Megvii, 21 June 2020; 26 June 2023.
216. YITU Technology. About Us / Our Team. Shanghai: YITU Tech, 2012–2025.
217. SenseTime. Corporate Governance / Leadership. Beijing: SenseTime, 2023–2025.
218. Ministry of Science and Technology of the PRC. Governance Principles for a New Generation of Artificial Intelligence: Develop Responsible AI. Beijing, 2019. Stanford DigiChina.
219. National Governance Committee for New Generation Artificial Intelligence. Ethical Norms for the New Generation AI. Beijing, 2021. Georgetown CSET (пер. DigiChina).
220. Human Rights Watch. China: Positions on Lethal Autonomous Weapons. Killer Robots Campaign Reports. New York: HRW, 2021.
221. United Nations General Assembly. A/RES/79/239: Artificial intelligence in the military domain and its implications for international peace and security. New York: UN, 24–31 Dec. 2024.
222. Republic of Korea. Intelligent Robots Development and Distribution Promotion Act. Seoul: Government of Korea, 2008.

223. Gibney E. Google AI algorithm masters ancient game of Go. Nature News, 15 Mar. 2016. P. 150–151.
224. Presidential Committee on the Fourth Industrial Revolution (PCFIR). Mid-to-Long-Term Master Plan for the Intelligent Information Society. Seoul, 2018.
225. Ministry of Science and ICT (Republic of Korea). National Strategy for Artificial Intelligence. Seoul, Oct. 2019.
226. National Assembly of Korea. Draft AI Basic Act. Seoul, Jan. 2023.
227. Government of the Republic of Korea. National Artificial Intelligence Strategy. Seoul: Ministry of Science and ICT, Oct. 2019.
228. HolonIQ. South Korea AI R&D investment overview. HolonIQ Insights, 2021.
229. Ministry of Science and ICT (MSIT). Data Infrastructure Budget Report 2021. Seoul: MSIT, 2021.
230. MSIT. Press release on private sector AI investment commitments. Seoul: Government of Korea, 2021.
231. Invest Korea. K-Network 2030 Strategy. Seoul: Ministry of Trade, Industry and Energy, Feb. 2023.
232. Ministry of National Defense (Republic of Korea). Defense Innovation 4.0: A strong military based on science and technology. Seoul: MND, 11 Aug. 2022.
233. The Korea Herald. Army expands Dronebot unit's roles to demining, logistics. Seoul, 13 Apr. 2021.
234. Asian Military Review. Venugopal K. UGVs in the Republic of Korea. 20 Jan. 2022.
235. Janes. South Korea's laser air-defence system to enter service in 2024. Dec. 2023.
236. Armada International. South Korea's First Laser Weapon System. 2024.
237. Korea Bizwire. S. Korea Deploys First Laser Weapon System for Drones. 24 June 2023.
238. Korean Air (Aerospace). KUS-FT Tactical UAV. Офіційна продуктова сторінка. Seoul: Korean Air Aerospace, б. д.

239. U.S. Army (Eighth Army). Counter-UAS exercise strengthens ROK-US readiness. 11 May 2023.
240. Guizzo E. Robotic Sentry for Korea's Demilitarized Zone. IEEE Spectrum, 2007.
241. United Nations — UNODA. The Republic of Korea's contribution on LAWS (A/79/88). UN Documents, 2024.
242. Reuters. South Korea summit to target blueprint for using AI in the military. 9–10 Sept. 2024.
243. MakinaRocks. Runway: AI Platform for Automated Retraining in Defense Networks. Seoul, 2025.
244. BusinessKorea. MakinaRocks to establish AI platform in National Defense. 20 Aug. 2025.
245. Venturesquare. MakinaRocks unveils defense AI innovation tech (Defense Innovation 100). July 2025.
246. UK Government. AI Safety Summit (Bletchley Park, 2023): Bletchley Declaration. London: GOV.UK, 2023.
247. Council of the EU. Regulation (EU) 2024/1689 — Artificial Intelligence Act. Brussels: Council of the EU, 2024.
248. UK Ministry of Defence. Ambitious, Safe, Responsible. London: NATO.int, 2022.
249. Ministère des Armées (France). Stratégie ministérielle sur l'IA. Paris: DefenseScoop, 2024.
250. Comité d'éthique de la défense (France). Principes/Guides éthiques pour l'emploi de l'IA. Paris: IISS, 2023–2024.
251. United Nations — CCW. Group of Governmental Experts on LAWS. Official materials. New York: UN, 2024.
252. Webster G., Creemers R., Kania E., Triolo P. Translation: China's New Generation Artificial Intelligence Development Plan (2017). Stanford: DigiChina, 2017.

253. Center for Security and Emerging Technology (CSET). *Made in China 2025: Translation and Analysis*. Washington, DC: Georgetown University, 2022.
254. Triolo P., Webster G., Kania E. *Translation: Three-Year Action Plan for Promoting the Development of a New Generation AI Industry (2018–2020)*. Stanford: DigiChina, 2018.
255. Ministry of Science and Technology of China (MOST). *Guidelines for AI Innovation & Development Pilot Zones*. Beijing, 2019. DigiChina.
256. Shanghai Municipal Government. *Measures to Promote AI Innovation (2019–2021)*. Shanghai, 2019.
257. National People’s Congress of China. *Data Security Law (DSL)*. Beijing, 2021.
258. National People’s Congress of China. *Personal Information Protection Law (PIPL)*. Beijing, 2021.
259. Cyberspace Administration of China (CAC). *Provisions on Algorithmic Recommendation Services*. Beijing, 2022.
260. Cyberspace Administration of China (CAC). *Provisions on Deep Synthesis Internet Information Services*. Beijing, 2023.
261. CAC. *Interim Measures for the Management of Generative AI Services*. Beijing, 2023.
262. Ding J., Cheung T.-M. *Techno-Industrial Policy for New Infrastructure: China’s AI as a General-Purpose Technology*. UC San Diego: IGCC, 2022.
263. State Council Information Office of the PRC. *China’s National Defense in the New Era*. Beijing: SCIO, 2019.
264. Ziyen UAV. *Blowfish A2 UAV Brochure*. Zhuhai Airshow, 2020.
265. Global Times. *China develops AI-powered tanks and robotic combat systems*. 2021.
266. Kania E. *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China’s Future Military Power*. Washington, DC: CNAS, 2017.
267. Allen G., Chan T. *Artificial Intelligence and National Security*. Cambridge, MA: Harvard Belfer Center, 2017.

268. Lin L., Singer P. W. China's Wing Loong Drones and the Proliferation of Armed UAVs. Washington, DC: Brookings, 2020.
269. Human Rights Watch. Losing Humanity: The Case against Killer Robots. 2012; updated 2021.
270. Liu Guozhi. Keynote Speech at National Science and Technology Commission. Beijing, 2017. Cited in: Kania E. CNAS Report, 2019.
271. Webster G., Creemers R., Kania E., Triolo P. Drafting China's National AI Team for Governance. Stanford: DigiChina, 18 Nov. 2019.
272. SenseTime. National Open Innovation Platform for Next-Generation AI (Intelligent Vision). Press release. 20 Sept. 2018.
273. Alibaba Cloud. How ET City Brain Is Transforming the Way We Live. Blog. 11 June 2018.
274. Baidu. Apollo — Intelligent Vehicle / Open Platform. Beijing, 2024–2025.
275. Забара І. М. Штучний інтелект у військовій сфері: становлення доктринальних основ міжнародно-правового регулювання в рамках Організації Об'єднаних Націй. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 90. Ч. 5. С. 138-144.
276. Artificial intelligence in the military domain and its implications for international peace and security: Resolution adopted by the General Assembly on 24 December 2024. A/RES/79/239. New York: United Nations, 2024.
277. Artificial intelligence: opportunities and risks for international peace and security: Letter dated 17 July 2023 from the Permanent Representative of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the Secretary-General. S/2023/528. New York: United Nations Security Council, 2023.
278. Lethal autonomous weapons systems: Resolution adopted by the General Assembly on 22 December 2023. A/RES/78/241. New York: United Nations, 2023.
279. Lethal autonomous weapons systems: Report of the Secretary-General. A/79/88. New York: United Nations, 2024.

280. Pact for the Future, Global Digital Compact and Declaration on Future Generations: Summit of the Future Outcome Documents. New York: United Nations, 2024.

281. United Nations Institute for Disarmament Research. AI in the Military Domain: A briefing note for States. Geneva: UNIDIR, 2025.

282. International Committee of the Red Cross. ICRC position on autonomous weapon systems. Geneva: ICRC, 12 May 2021.

ДОДАТКИ

Додаток 1.

Таблиця 1.

Інститути ІІІ в міжнародному праві

Рівень/підсистема	Зміст / фокус	Ключові міжнародні джерела	Приклади механізмів реалізації	Статус
Загальносистемні рамки	Людиноцентричність, недискримінація, прозорість, підзвітність, людський нагляд протягом життєвого циклу ІІІ	Рекомендація ЮНЕСКО (2021) [13]; Рамкова конвенція РЄ про ІІІ (2024) [14]	Оцінка впливу/ризиків, аудит алгоритмів, наглядові органи	(РЄ) + <i>soft law</i> (ЮНЕСКО)
Міжурядові керівні принципи	Узгоджені принципи довірчого ІІІ; координація політики	Принципи ОЕСР (2019) [15]; G7 «Хіросіма щодо ІІІ» (2023) [16]	Добровільний кодекс для розробників; робочі групи	<i>Soft law</i> / політичні зобов'язання
Права людини і ІІІ	Приватність, недискримінація, ефективні засоби юридичного захисту; застосування регіональних/універсальних договорів до алгоритмічних рішень	РЄ-конвенція про ІІІ [14]; матеріали ООН з прав людини і ІІІ [13; 15]	DPIA/HRIA для ІІІ; доступ до оскарження рішень, що базуються на ІІІ	Наявні договори + рамкові настанови
МГП та автономні системи озброєнь (LAWS)	«Значущий людський контроль», заборони/обмеження для певних категорій систем	Позиція МКЧХ [4]; платформа К333/CCW (обговорення LAWS) [14]	Юридично зобов'язуючі обмеження; правила таргетингу	Норми МГП + очікувані нові інструменти
Кібербезпека і криміналізація зловживань	Узгодження стандартів кіберзахисту та	Рекомендації міжнародних організацій; стандарти	Спільні протоколи реагування;	Напрацьовується в межах

	співпраці проти зловживань ІІІ	NIST/ISO (у твоїх матеріалах) [6]	обмін даними/доказами	чинних режимів
Економічні режими (експортний контроль, торгівля)	Запобігання небажаному поширенню критичних ІІІ-технологій; комплаєнс із санкційними режимами	Підходи ОЕСР/«Групи Васенаар» (у доктрині; згадки в твоїх тезах) [6; 14]	Ліцензування, перелік чутливих товарів/ПО, due diligence	Механізми діють; деталізація триває
Концепт «електронної особи»	Теоретична дискусія про обмежену електронну правосуб'єктність	Резолюція ЄП 2017 р. - пропозиція «на розгляд» [10]	Моделі відповідальності через аналоги корпорацій/МО	Дискусійна зона (без зобов'язуючих норм)

Джерело: розроблено автором на основі [13; 14; 4; 15; 16; 10; 12].

Додаток 2.



Рис. 1. Траєкторія включення ІІІ до системи міжнародно-правових інститутів

Джерело: розроблено автором на основі [14; 26; 25]

Додаток 3.

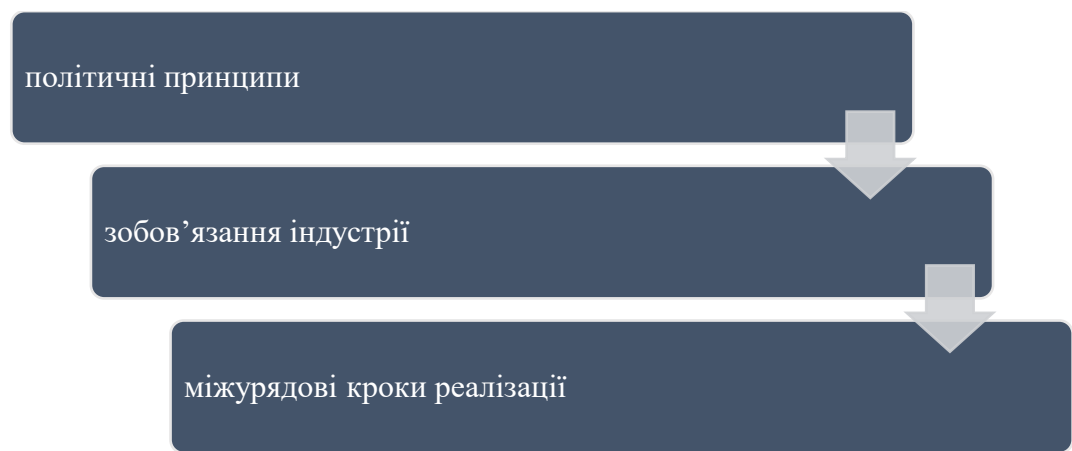


Рис 2. Архітектура процесу реалізації забезпечення правового регулювання ШІ

Джерело: розроблено автором на основі [57]

Додаток 4.

Таблиця 2.

Чотири етапи становлення глобальної архітектури ШІ

Етап / процес	Ключові інструменти	Ініціатори / учасники	Правовий статус	Основні механізми
1. Етична кодифікація	Принципи Азіломар; Принципи ОЕСР щодо ШІ	Науковці/індустрія; ОЕСР + G20	М'які стандарти	Людиноцентричність, прозорість, підзвітність; дорожні карти політик
2. Інституціоналізація співпраці	GPAI (інтеграція з OECD.AI)	Держави G7+ партнери (нині 40+), секретаріат в ОЕСР	Міжурядова координація	Робочі групи, центри в Парижі/Монреалі/Токіо; методики імплементації
3. Рамки безпеки «передових ШІ»	Hiroshima AI Process; Блетчлійська	G7; 28 країн у Блетчлі; уряди + компанії	М'які зобов'язання/політичні комюніке	Принципи, кодекс розробників, допуск

	декларація; AI Seoul Summit (Frontier AI Safety Commitment s)			урядів до тестів, інститути безпеки
4. Юридична обов'язковість	EU AI Act; Конвен т РЄ про III	ЄС; Рада Європи (відкритий для третіх держав)	Обов'язкові норми	Заборони, вимоги до високого ризику, нагляд (AI Office, СЕ-маркування); принципи/ризик- менеджмент, Конференція Сторін

Джерело: розроблено автором на основі [45; 15; 46; 16; 50; 57; 51; 14; 18, с. 1–2; 18, с. 3–4; 18, с. 6–7].

Додаток 5.

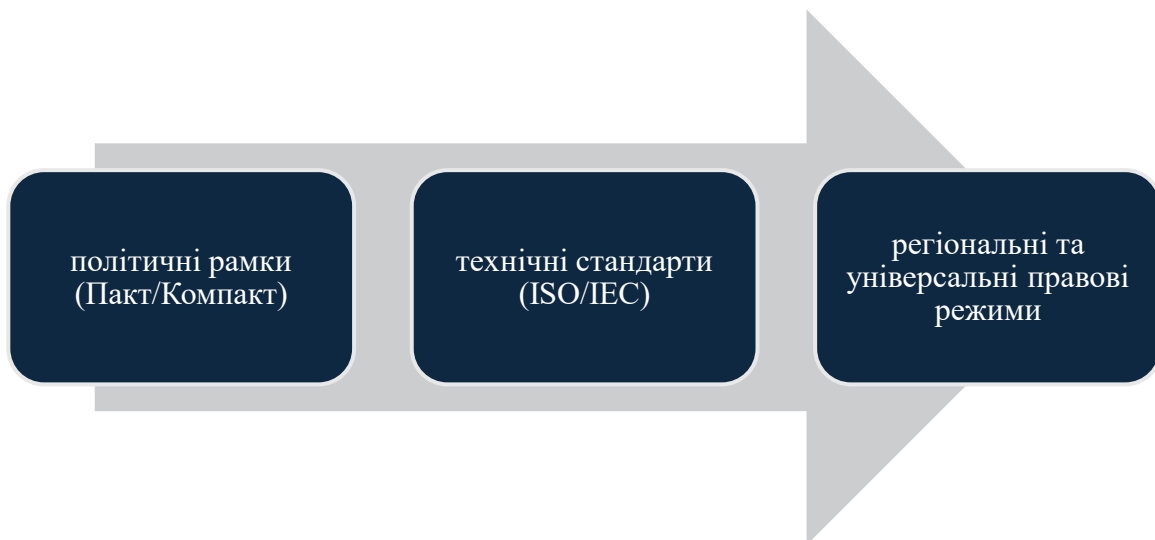


Рис. 3. Багаторівневість правотворення інститутів III

Джерело: розроблено автором на основі [102–105; 108; 109]

Додаток 6.

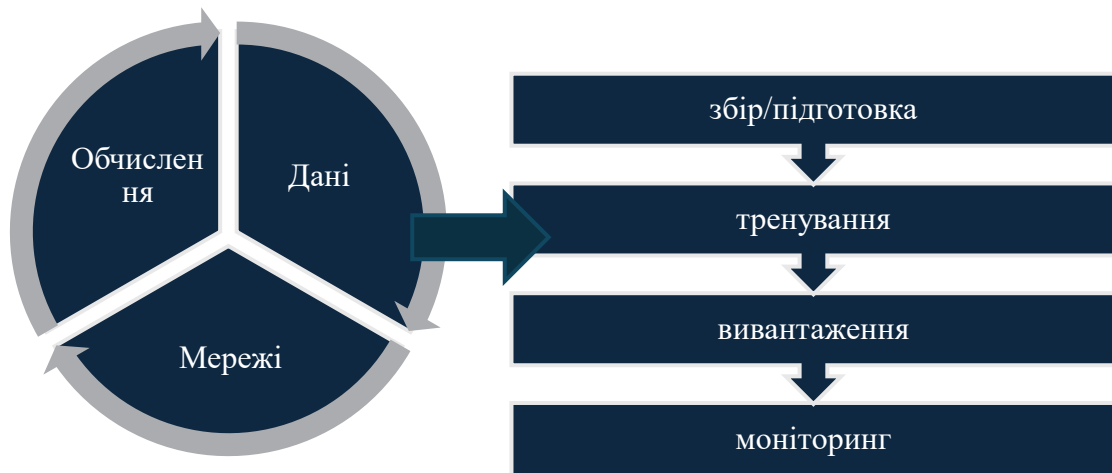


Рис 4. Цифрова конвергенція , що забезпечує життєвий цикл систем ІІІ

Джерело: розроблено автором на основі [100; 101; 109; 108; 110–111]

Додаток 7.

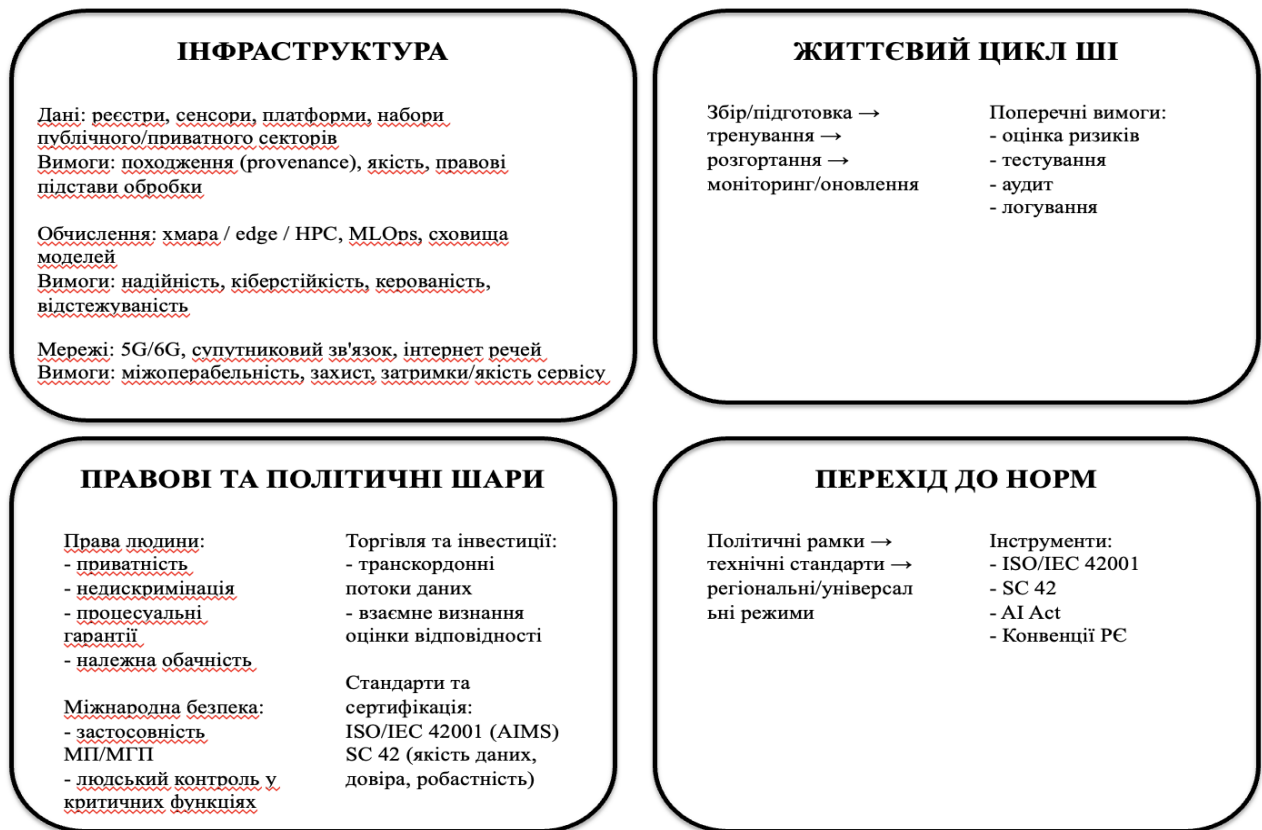


Рис 5. Цифрова конвергенція → інститути для ІІІ

Джерело: розроблено автором на основі [102–105; 108–111]

Додаток 8.

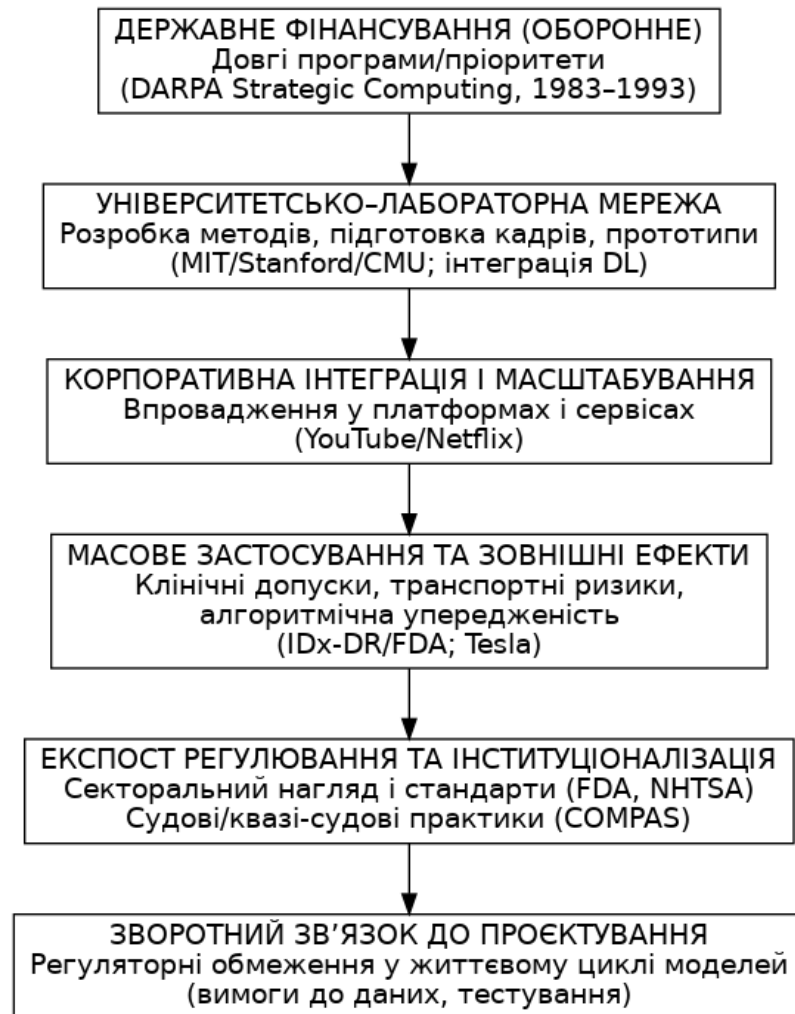


Рис 6. Причинно-наслідковий ланцюг американської моделі

Джерело: розроблено автором на основі [129-131;132-136]

Додаток 9.

Таблиця 3.
Конденсований огляд структурних наслідків (США)

Домен	Інструмент/механізм	Ключовий ефект для права
Охорона здоров'я	Допуск автономної діагностики (IDx-DR), умови застосування	Формалізація вимог до даних, валідації, простежуваності; постмаркетинговий моніторинг
Транспорт і безпека	Програмні відкликання, технічні розслідування NHTSA (Autosteer/Autopilot)	Інкорпорація «поведінкових» вимог і сценаріїв експлуатації; уточнення меж відповідальності
Публічний сектор (правосуддя)	Дискусія довкола COMPAS, доступ до методики і помилок	Вимоги до прозорості, аудитів, процедур оскарження алгоритмічних рішень
Масові платформи	Політики експериментування і контролю даних (Netflix, YouTube)	Узгодження внутрішніх практик із очікуваннями прозорості/підзвітності; підготовка до регуляторної гармонізації

Джерело: розроблено автором на основі [132–136].

Додаток 10.

Таблиця 4.
Стисла порівняльна таблиця (FR/UK)

Вузол	Франція	Велика Британія	Нормативні документи
Стратегія й управління	DGA; політика «AI in Support of Defence»; делегат з озброєнь Емманюель Шіва [153]	Defence AI Strategy; DAIC [155]	Етична опінія Комітету з оборонної етики (FR) [154]; Defence AI Playbook (UK) [171]
Розвідка / JISR	TORNADE (Preligens→Safran); Fortion (Airbus) [163; 162; 167–169; 172–173]	JISR-інтеграція та державні випробування моделей [155]	V&V, простежуваність даних/моделей [153–155; 171]

Повітряний бій / MUM-T	Rafale F5 + UCAV/remote carriers (алгоритмічне підсилення пілота) [171; 168]	Полігонні тести MUM-T (QinetiQ) [170–171]	Людський контроль, пороги автономії [153–155; 171]
Тести «передових моделей»	Відомчі процедури допуску [153–154]	AI Safety Institute (керівник Ієн Гогарт); UK–US/Canada протоколи тестів [174–180]	JSP 936; міжурядові MoU [159; 174–180]
Сенсорика / ППО	Thales Ground Master (AI-класифікація) [166; 165]	Інтеграція в C2 за MOD-вимогами [155]	Аудит даних, кібербезпека ланцюгів [153–155; 171]

Джерело: розроблено автором на основі [153–155; 162; 163; 165–180].

Додаток 11.



Рис. 7. Вбудовування правових гарантій у цикл управління бойовими діями

Джерело: розроблено автором на основі [153–155; 159, 171, 174–180]

Додаток 12.

Таблиця 5.

Основні документи етичного та правового регулювання ІІІ у КНР (2017–2023)

Рік	Документ	Характер	Ключові положення
2017	Закон про кібербезпеку	Закон	Локалізація даних, мережевий захист
2019	Принципи управління ІІІ нового покоління	Етичні принципи	Гармонія, справедливість, безпека, контрольованість
2021	Закон про безпеку даних	Закон	Категорії даних, режими доступу
2021	Закон про захист персональної інформації	Закон	Приватність, транскордонні передачі
2021	Кодекс етичних норм ІІІ	Етичний кодекс	6 принципів + 18 вимог
2022	Правила управління алгоритмічними рекомендаціями	Регламент	Прозорість, відмова користувача
2023 (січ.)	Положення про deep synthesis	Регламент	Маркування deepfake, відповідальність провайдерів
2023 (серп.)	Тимчасові заходи для генеративного ІІІ	Регламент	Реєстрація LLM, цензура, точність

Джерело: розроблено автором на основі [247-250]

Додаток 13.

Таблиця 6.
Ключові приклади військового ІІІ РК (2023–2025)

Напря́м / система	Провідні актори	Статус	Роль ІІІ
Defense Innovation 4.0	МО РК	Діє від 2022	Автономізація, MUM-T, цифрове C2
Dronebot Combat Unit	Армія РК	Підрозділ з 2018; розвідка/логістика	Рої, CV-розвідка
Лазерне C-UAS (Block-I/LAMD)	DAPA; LIG Nex1; Hanwha	Поставки 2023; розгортання 2024–2025	Виявлення/трекінг/класифікація БпЛА
Тактичний БпЛА KUS-FT	Korean Air (KAL-ASD)	Дослідне/серійне застосування	Автономна навігація, ISR
UGV сімейства	Hyundai Rotem; Hanwha	Випробування Армією РК	Напіваавтономний рух, SLAM
AI-платформа Runway	MakinaRocks (Defense Innovation 100)	Контракт 2025 (~₩2 млрд)	MLOps/LLMOps, ретрейнінг у захищених мережах
C-UAS інтероперабельність (ROK–US)	8-ма Армія США + РК	Вправи 2023	Злиття даних, швидка “kill-chain”
ДМЗ охорона (SGR-A1)	МО РК / промисловість	Історичні розгортання	Автоматизоване виявлення/ідентифікація
Міжнар. рамка LAWS	МЗС/МО РК	Внески 2024; підтримка A/RES/78/241	«Людське судження», двошаровий підхід
Саміт військ. ІІІ (Сеул-2024)	Уряд РК	>90 держав	«Блакитна книга» добрососуського застосування

Джерело: розроблено автором на основі [261-268]

Додаток 14.

Таблиця 7.

Базові засади REAIM 2023 щодо відповідального використання ІІІ у військовій сфері

Засада	Зміст у межах REAIM 2023	Міжнародно-правове значення	Практична імплементація
Застосовність міжнародного права	Використання ІІІ має відповідати міжнародно-правовим зобов'язанням	Виключає правовий вакуум щодо військового ІІІ	Юридична експертиза систем, перевірка відповідності МГП і Статуту ООН
Людська відповідальність	Люди залишаються відповідальними і підзвітними за рішення при використанні ІІІ	Недопущення перенесення відповідальності на алгоритм	Визначення операторів, командних ланцюгів, процедур аудиту
Оцінка ризиків	Необхідність оцінювати різні типи застосувань ІІІ в різних військових контекстах	Перехід від абстрактних принципів до контекстної правової оцінки	Risk assessment до розгортання, під час використання та після оновлень
Обережна інновація	Запізніле впровадження створює військовий ризик, передчасне впровадження створює ризик шкоди	Баланс між оборонною необхідністю і правовими гарантіями	Тестування, гарантування безпеки, поетапне впровадження
Управління даними	Дані мають збиратися, використовуватися, архівуватися і видалятися відповідно до права	Дані визнаються джерелом правового ризику	Контроль якості даних, захист даних, перевірка навчальних наборів
Життєвий цикл системи	Увага до розроблення, розгортання і використання систем ІІІ	Регулювання поширюється не лише на момент застосування сили	Контроль на стадіях проектування, закупівлі, навчання, експлуатації
Людський нагляд	Необхідність належних запобіжників і human oversight	Забезпечення реального, а не формального людського контролю	Повноваження оператора, можливість

			втручання, час для оцінки
Підготовка персоналу	Військові користувачі мають розуміти характеристики, обмеження і наслідки ІІІ	Підготовка стає елементом правомірного використання	Навчання операторів, тренування щодо упередженості і помилок
Багатосуб'єктність	Участь держав, приватного сектору, науки, громадянського суспільства	Визнання ролі недержавних акторів у військово-технологічному ланцюгу	Обмін практиками, приватно-публічна взаємодія, експертні платформи
Подолання розривів	Потреба у доступі держав до знань і передових практик	Запобігання нерівності у здатності контролювати військовий ІІІ	Capacity-building, технічна допомога, обмін досвідом

Джерело: розроблено автором на основі [288; 289; 292].

Додаток 15.

Таблиця 8.

Еволюція REAIM від Гааги 2023 до Сеула 2024

Критерій	REAIM 2023, Гаага	REAIM 2024, Сеул	Значення для становлення міжнародного регулювання
Дати	15-16 лютого 2023 р.	9-10 вересня 2024 р.	Формування послідовного процесу, а не одноразової конференції
Організатори	Нідерланди та Республіка Корея	Республіка Корея, за участю співорганізаторів і партнерів	Посилення ролі середніх держав як модераторів глобального діалогу

Основний документ	Call to Action	Blueprint for Action	Перехід від загального заклику до дорожньої карти дій
Ключовий акцент	Спільне розуміння ризиків і можливостей	Імплементация принципів і майбутнє врядування	Поглиблення нормативної конкретизації
Правова природа	Soft law, політичний документ	Soft law, декларативна дорожня карта	Накопичення політичних стандартів без договірної обов'язковості
Суб'єктний підхід	Держави, приватний сектор, академічні кола, громадянське суспільство	Понад 90 держав, експерти, індустрія, міжнародні організації	Формування багатосуб'єктної моделі управління
Людський контроль	Належні запобіжники і human oversight	Належна людська участь, відповідальність і підзвітність	Перехід до уточнення якості людської участі
Дані та технічна надійність	Якість даних, захист даних, тестування, гарантії	Надійність, trustworthy AI, пояснюваність	Посилення техніко-правового блоку
Зв'язок з міжнародним правом	Повна відповідність міжнародно-правовим зобов'язанням	Дотримання міжнародного права як основа відповідальності	Закріплення міжнародного права як межі військового ІІІ
Перспектива	Продовження глобального діалогу	Перетворення принципів на конкретні дії	Підготовка до подальшої юридикації

Джерело: розроблено автором на основі [288; 289; 290; 291; 292].

Додаток 16.

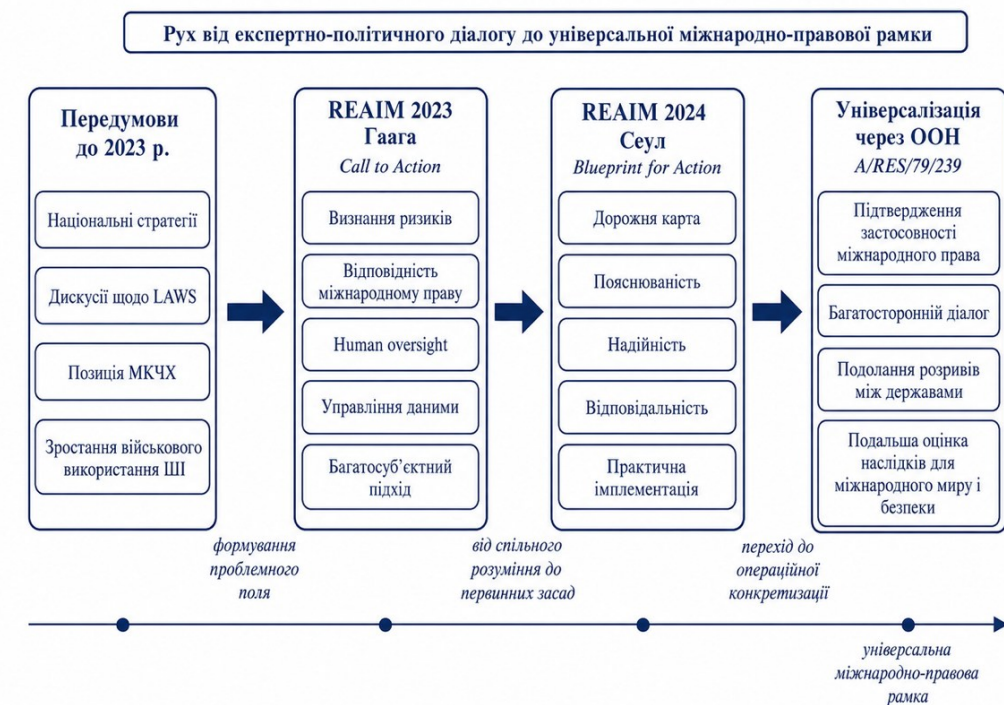


Рис. 8. Еволюція REAIM як процесу формування засад відповідального військового ІІІ

Джерело: розроблено автором на основі [282; 288; 289; 290; 292; 293].

Додаток 17.

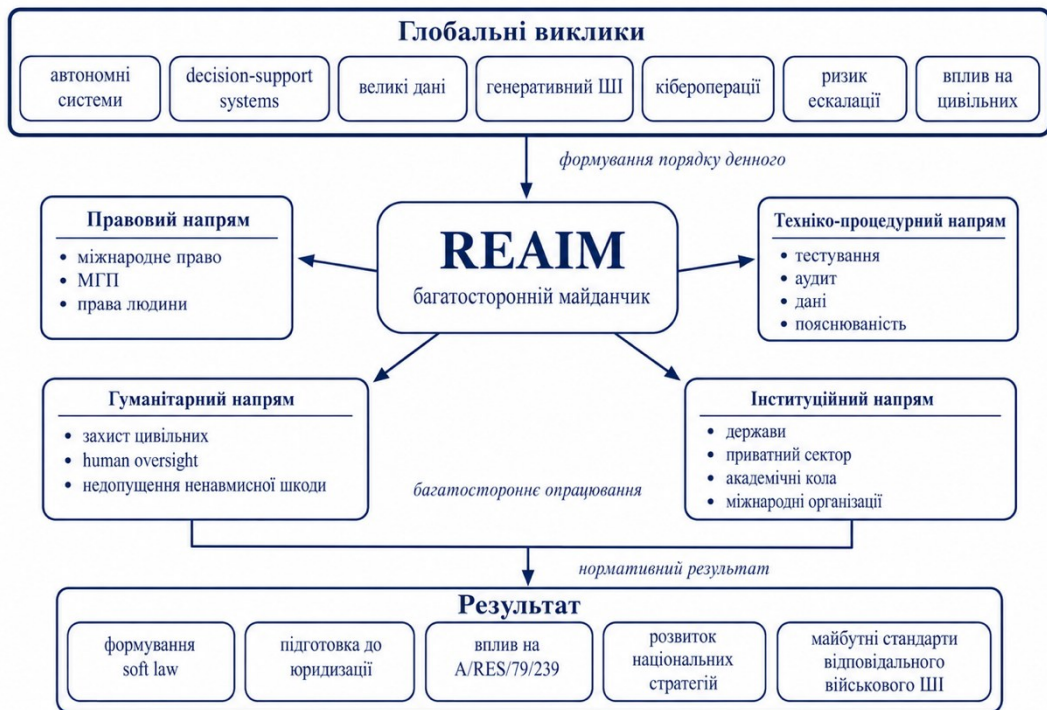


Рис. 9. Функціональна модель REAIM у системі становлення міжнародно-правового регулювання військового ІІІ

Джерело: розроблено автором на основі [288; 289; 290; 292; 293].

Додаток 18.

Таблиця 9. Доктринальні блоки підходу ООН до міжнародно-правового регулювання військового ШІ

Доктринальний блок	Зміст підходу ООН	Міжнародно-правове значення	Практичне значення для держав
Застосовність міжнародного права	Міжнародне право, Статут ООН, МГП і міжнародне право прав людини застосовуються до всіх питань на всіх етапах життєвого циклу військового ШІ	Заперечення технологічного винятку та підтвердження дії чинного права щодо нових військових технологій	Проведення правової експертизи систем ШІ на стадіях розробки, закупівлі, розгортання і використання
Комплексний підхід	Військовий ШІ оцінюється у правовій, гуманітарній, технічній, етичній та безпековій площинах	Формування міжгалузевого підходу до регулювання, що не обмежується лише МГП або технічними стандартами	Створення міжвідомчих процедур оцінки, залучення правників, інженерів, військових, фахівців з кібербезпеки і гуманітарного права
Оцінка наслідків для миру і безпеки	Держави мають продовжувати оцінювати наслідки військового ШІ для міжнародного миру і безпеки	Визнання ШІ фактором стратегічної стабільності, контролю над озброєннями і недопущення ескалації	Проведення національних і міжнародних оцінок ризику, обмін досвідом, участь у багатосторонньому діалозі
Відповідальне застосування	Військовий ШІ має бути людиноцентричним, підзвітним, безпечним, надійним і таким, що заслуговує на довіру	Закріплення мінімальних критеріїв правомірної і підконтрольної інтеграції ШІ у військову сферу	Запровадження human oversight, механізмів аудиту, тестування, підготовки персоналу і документування рішень
Подолання розривів між державами	Необхідне добровільне співробітництво, допомога, передача знань, обмін інформацією і передовим досвідом	Визнання технологічної нерівності як фактора правової і безпекової вразливості	Розбудова потенціалу держав, що розвиваються, участь у програмах обміну знаннями і технічної допомоги

Джерело: розроблено автором за [1; 2; 3; 4; 5].

Додаток 19.



Рис. 3.2.1. Передумови формування універсального підходу ООН до військового ІШ

Рис. 10. Передумови формування універсального підходу ООН до військового ІШ

Джерело: розроблено автором за [1; 2; 3; 4; 5; 6].

Додаток 20.

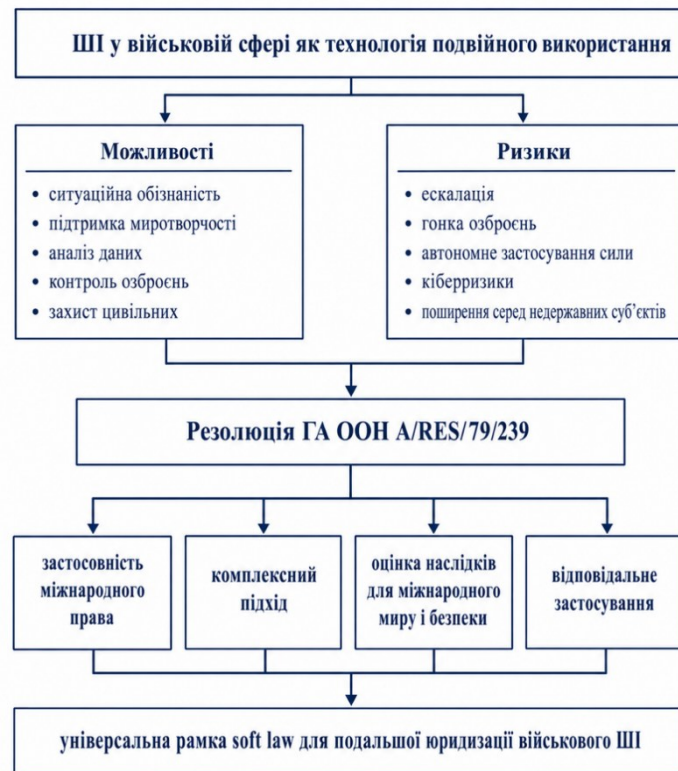


Рис. 3.2.2. Універсальна доктринальна модель ООН щодо військового III

Рис. 11. Універсальна доктринальна модель ООН щодо військового III

Джерело: розроблено автором за [1; 2; 3; 4; 6].