

ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

ВАРИНСЬКИЙ ВЛАДИСЛАВ ОЛЕКСІЙОВИЧ

УДК 342.9:34:004.8(477)

ДИСЕРТАЦІЯ
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ТА ПРАВОВІ ЗАСАДИ
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ

12.00.07 «Адміністративне право і процес; фінансове право;
інформаційне право»

Юридичні науки

Подається на здобуття наукового ступеня доктора юридичних наук.

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело. Всі частини тексту дисертації, під час написання яких використовувалися технології штучного інтелекту, перевірені та відредаговані особисто



В. О. Варинський

Одеса – 2026

АНОТАЦІЯ

Варинський В. О. Теоретико-методологічні та правові засади використання штучного інтелекту в Україні. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». – Одеський державний університет внутрішніх справ, Одеса, 2026.

У дисертації здійснено комплексне теоретико-правове та прикладне дослідження інформаційно-правових та адміністративно-правових засад обмеження та публічного адміністрування використання штучного інтелекту (ШІ) в Україні в умовах євроінтеграційного зближення, глобальної цифрової трансформації соціуму та правового режиму воєнного стану. Обґрунтовано закономірну трансформацію предмета інформаційного права від статичного регулювання відносин щодо обігу інформації як самостійного феномену (наприкінці ХХ століття) до комплексного врегулювання суспільних відносин, пов'язаних із процесами її автоматизованого створення, інтерпретації та генерації високоавтономними системами машинного походження. Доведено, що традиційна модель інформаційного регулювання виявляється обмежено ефективною в умовах зростання автономності технологій та їхньої здатності самостійно формувати рішення, які тягнуть за собою юридично значущі наслідки, що зумовлює об'єктивну необхідність переходу до новітньої парадигми публічно-правового впливу.

У роботі розкрито генезис доктринальних підходів до юридичного осмислення штучного інтелекту, що дозволило типізувати три ключові вектори його розуміння в сучасній науковій думці: функціональний (Л. Флориді, О. Баранов), субстанційний (Л. Солум, О. Радутний) та антропоцентричний (Ф. Паскуале, П. Рабінович). На цій основі запропоновано авторську правову дефініцію штучного інтелекту як правової категорії, під якою розуміється високотехнологічна автономна інтелектуальна система машинного походження,

що характеризується внутрішньою здатністю до динамічної адаптації (самонавчання на основі великих масивів даних) і функціональною спроможністю безпосередньо або опосередковано формувати, оптимізувати чи реалізовувати алгоритмічні рішення (прогнози, рекомендації), які мають юридично значущий характер та можуть створювати потенційні ризики для фундаментальних прав і свобод людини, національної безпеки, демократичного врядування та публічного порядку. Здійснено чітке правове розмежування системи III й Інтернету речей (IoT), де останній визначено як цифрову та апаратну інфраструктуру автоматизованого збирання й транскордонного обміну даними між пристроями, яка зберігає людиноорієнтовану модель і позбавлена когнітивних функцій прийняття нелінійних рішень.

На основі компаративного аналізу здійснено поглиблене дослідження міжнародного досвіду правового регулювання III, що дозволило виявити концептуальні, нормативні та інституційні особливості відповідних моделей у провідних юрисдикціях. Виявлено дві протилежні глобальні тенденції розвитку інформаційно-правової політики: універсальний рівень (акти ООН, Окінавська хартія, Женевська декларація 2003 року), де тривалий час III розглядався виключно в межах загального сектору ІКТ без виокремлення його як самостійного об'єкта безпекового регулювання, та європейський регіональний рівень (Рада Європи, ЄС), який сформував упереджувальну, ціннісно орієнтовану модель «керованої автономії». Детально проаналізовано генезис трансформації інструментів «м'якого права» (*soft law*) в імперативні режими «жорсткого права» (*hard law*), кодифіковані у Регламенті (ЄС) 2024/1689 (*Artificial Intelligence Act*) та Рамковій конвенції Ради Європи про III. Розкрито специфіку правових інструментів допуску високоризикових систем на ринок (оцінка відповідності (*conformity assessment*), логування, людський нагляд (*human oversight*), оцінка впливу на фундаментальні права (*FRIA*) та обов'язкова реєстрація в базі даних ЄС з серпня 2026 року). Окремо типізовано диференційовані геополітичні моделі: децентралізовану ризикоорієнтовану модель США та централізовану превентивно-наглядову модель КНР (на

прикладі Тимчасових заходів САС 2025 року щодо інтерактивних послуг ІІІ), де пріоритет національної безпеки та державного контролю переважає над технологічною автономією суб'єктів. Проаналізовано європейський досвід інтеграції *AI Act* із діючими великими інформаційними системами міграції та безпеки (*VIS, Eurodac, EES, ETIAS, ECRIS-TCN*).

У результаті узагальнення зазначених підходів обґрунтовано, що ключовими трендами розвитку правового регулювання ІІІ є перехід від реактивного контролю наслідків до проактивних ризикоорієнтованих моделей управління протягом усього життєвого циклу технології, посилення вимог алгоритмічної прозорості, підзвітності та пояснюваності. Визначено напрями гармонізації національного законодавства України з європейськими стандартами, що передбачають побудову цілісної нормативної архітектури (рамкового закону, взаємоузгоджених змін до базових законів та системи підзаконних актів), які мають реалізовуватися не через механічне копіювання іноземних норм, а шляхом їх адаптації до національної системи публічного адміністрування, структури органів влади та викликів відновлення держави. Систематизовано доктринальні підходи до правосуб'єктності у цифрову епоху: критично проаналізовано концепцію «електронної особи» та доведено її неделіктоздатність через відсутність у ІІІ автономної правової волі, правосвідомості та психоемоційного компонента вини. Обґрунтовано підпорядкування ІІІ правовому режиму джерела підвищеної небезпеки та «мислячої речі» (*res cogitans*), де загальний тягар ризиків покладається на його володільця, та здійснено функціональне розмежування на неавтономний ІІІ (стадія інституційного навчання під телеологічним контролем людини) та автономний ІІІ (здатний виконувати завдання під системним наглядом людини, але без її покрокового керування).

Розроблено концептуальну модель інституціоналізації публічного адміністрування ІІІ в Україні, що ґрунтується на розбудові мережевої (гібридної) системи управління, яка забезпечує чітке розмежування політичних, регуляторних, контрольно-наглядових, правозахисних та судових функцій і

виключає концентрацію всіх повноважень у межах одного органу. Запропоновано інституційну архітектуру, що усуває конфлікт цілей між підтримкою інновацій та захистом прав людини, шляхом законодавчого закріплення *функціональної матриці компетенції*, яка визначає взаємодію суб'єктів: Кабінету Міністрів України (загальне спрямування політики), Міністерства цифрової трансформації України (центральний координатор розвитку та методичного забезпечення), функціонально незалежного Національного компетентного органу нагляду (ЦОВВ зі спеціальним статусом, наділений правами проведення перевірок та застосування фінансових санкцій), секторальних регуляторів, Уповноваженого ВРУ з прав людини (правозахисний контроль) та судових органів (остаточний контроль законності). Обґрунтовано доцільність створення державного реєстру високоризикових систем ШІ та впровадження регуляторного експериментального середовища (*AI Sandbox*) як правового інструменту апробації інноваційних рішень у контрольованому середовищі.

Окремий блок дослідження присвячено розвитку методології аналітичного супроводу та процедурного забезпечення життєвого циклу штучного інтелекту. На основі категоріального апарату теорії права та адміністративного права обґрунтовано необхідність розширення класичної структури механізму правового регулювання (МПР) за рахунок включення новітніх органічно-функціональних елементів: управління ризиками, оцінки відповідності, алгоритмічної прозорості, незалежного аудиту, сертифікації та превентивного державного нагляду. Сформовано теоретико-методологічні засади цілісної ризик-орієнтованої правової політики у сфері ШІ, визначеної як системна діяльність держави з формування диференційованих правових режимів, де зміст заборон та обов'язків корелює із масштабом, тяжкістю й оборотністю впливу конкретної системи. Запропоновано авторський аксіологічний ризик-орієнтований тест адміністративно-правової оцінки допустимості використання систем ШІ, який, на відміну від ринково-функціонального підходу *AI Act*, базується на ієрархії конституційних правових

цінностей і передбачає послідовне чотирирівневе оцінювання впливу технології на: 1) життя і здоров'я людини (аксіологічна основа – ст. 3 Конституції України, ст. 2 ЄКПЛ); 2) національну безпеку та стійкість держави в умовах збройної агресії; 3) фундаментальні права і свободи особи у сфері публічних послуг; 4) демократичне врядування, верховенство права та інституційну спроможність влади (*AI Governance*). Обґрунтовано новий правовий принцип – принцип пропорційності адміністративно-правового впливу, згідно з яким інтенсивність державного втручання та імперативність контролю перебувають у прямій залежності від ступеня потенційної загрози системи ІІІ для об'єктів охорони.

На основі емпіричного аналізу (результатів авторського соціолого-правового опитування 1092 респондентів, даних компаній *Gradus Research*, КМІС та глобальних моніторингових баз *AI Incident Database*, *OECD* та *MIT AI Risk Repository*) здійснено системне зонування та класифікацію систем ІІІ за п'ятьма категоріями ризику: заборонені практики неприйнятної ризику (маніпулятивне застосування, соціальне оцінювання громадян, невивіркове збирання біометрії), високоризикові системи (компоненти безпеки інфраструктури, біометрія, сфери правопорядку, міграції та правосуддя), системи обмеженого ризику (вимоги прозорості й маркування), системи мінімального ризику та моделі ІІІ загального призначення (включаючи моделі із системним ризиком). Систематизовано дванадцять взаємопов'язаних адміністративних процедур, що охоплюють повний життєвий цикл системи ІІІ: від попередньої інвентаризації, класифікації та перевірки менш обмежувальних альтернатив до обов'язкового оцінювання впливу на основоположні права (*HRIA/FRIA*), ведення Державного реєстру високоризикових систем із паспортом ризику, забезпечення моделей людського контролю (*human-in-the-loop* чи *human-on-the-loop*), післяринкового моніторингу, повідомлення про серйозні інциденти протягом 72 годин та забезпечення індивідуального права особи на зрозуміле змістовне пояснення факторів автоматизованого рішення. Доведено, що особливості воєнного стану вимагають застосування прискорених або спеціальних закритих процедур для сфер оборони, розвідки та безпеки із

обов'язковим збереженням законності, документування та персональної відповідальності військової посадової особи в межах стандарту *meaningful human control* (значущого людського контролю) над застосуванням сили.

У дисертації здійснено комплексний галузевий аналіз меж допустимої алгоритмізації суспільних відносин у найбільш аксіологічно чутливих секторах суспільного життя. Визначено правові межі використання медичного ШІ, де на основі шести фундаментальних принципів ВООЗ диференційовано правові режими: автономні режими (*human-out-of-the-loop*) визначено допустимими виключно на етапах первинного скринінгу та доклінічного моделювання, тоді як безпосереднє встановлення остаточного діагнозу та планування терапії вимагають обов'язкового збереження людиноцентричного стандарту медичної допомоги та клінічного розсуду лікаря як суб'єкта юридичної відповідальності. Обґрунтовано концепцію правової недопустимості алгоритмічної деформації дискреційних повноважень правоохоронних органів та правосуддя, яка виключає існування автономного алгоритмічного правозастосування чи підміну індивідуального суддівського розсуду автоматизованими висновками алгоритмів із закритою логікою («чорних скриньок»). Доведено, що ШІ в цих сферах має виступати виключно як допоміжний інструмент інформаційно-аналітичної підтримки за умов його пояснюваності, прозорості та можливості незалежного аудиту.

Обґрунтовано правомірність транскордонного застосування баз даних розпізнавання обличчя в умовах відсічі збройній агресії для ідентифікації причетних до воєнних злочинів виключно за наявності чіткої правової підстави та жорстких часових обмежень. Встановлено межі правомірного використання систем ШІ в освіті та науковій діяльності, що передбачають недопустимість імітації авторства, підміни самостійної когнітивної діяльності й руйнування академічної свободи, визначивши інструменти ШІ засобами технічного та інформаційного супроводу.

Сформовано цілісну теоретико-методологічну концепцію публічного адміністрування використання систем ШІ, що інтегрує людиноцентричну,

ризикоорієнтовану, сервісну та безпекову парадигми. Розкрито концептуальний дуалізм аксіолого-правового виміру ІІІ, який полягає у доктринальному співіснуванні гуманістичної та трансгуманістичної моделей розвитку, де саме праву належить визначальна роль у забезпеченні людської автономії.

Розроблено та обґрунтовано комплексну трирівневу модель нормативного вдосконалення, основу якої становить проєкт рамкового Закону України «Про безпечне та відповідальне використання систем штучного інтелекту» (що поєднує ринковий та правозахисний підходи), узгоджений пакет змін до чинних базових актів (включаючи доповнення ЗУ «Про адміністративну процедуру» статтею 69-1 яка прямо регламентує алгоритмічно підтримані рішення та встановлює обов'язок посадової особи формувати відтворюваний алгоритмічний слід, а також зміни до законів про захист персональних даних, публічні закупівлі, електронні реєстри та доступ до інформації) та процедурні постанови Кабінету Міністрів України, що у своїй сукупності забезпечує створення ефективного, адаптивного та цілісного механізму *AI governance* в Україні відповідно до найкращих європейських стандартів.

Ключові слова: теоретико-методологічні засади, правові засади, штучний інтелект, система штучного інтелекту, публічне адміністрування, інформаційне право, адміністративна процедура, ризик-орієнтований підхід, аксіологія, людський контроль, мережева інституційна модель, євроінтеграція, цифровізація, механізм правового регулювання.

SUMMARY

Varynskyi V. O. Theoretical, Methodological, and Legal Framework for the Use of Artificial Intelligence in Ukraine. – Qualification scientific work manuscript.

Thesis for a Doctor of Laws (Doctor of Legal Sciences) degree in Speciality 12.00.07 "Administrative Law and Process; Financial Law; Information Law". – Odesa State University of Internal Affairs, Odesa, 2026.

The thesis provides a comprehensive theoretical-legal and applied study of the information-legal and administrative-legal frameworks for the restriction and public administration of artificial intelligence (AI) systems use in Ukraine under the conditions of European integration alignment, global digital transformation of society, and the legal regime of martial law. The dissertation substantiates the law-governed transformation of the subject matter of information law from the static regulation of relations regarding the circulation of information as an independent phenomenon (at the end of the 20th century) to the complex regulation of social relations associated with the processes of its automated creation, interpretation, and generation by highly autonomous systems of machine origin. It is proved that the traditional model of information regulation turns out to be limitedly effective in the context of the growing autonomy of technologies and their capability to independently shape decisions carrying legally significant consequences, which determines the objective necessity of transitioning to a newer paradigm of public-law influence.

The work reveals the genesis of doctrinal approaches to the legal conceptualisation of artificial intelligence, which allowed for the typification of three key vectors of its understanding in modern scientific thought: functional (L. Floridi, O. Baranov), substantial (L. Solum, O. Radutnyi), and anthropocentric (F. Pasquale, P. Rabinovych). On this basis, the author proposes a novel legal definition of artificial intelligence as a legal category, which is understood as a highly technological autonomous intellectual system of machine origin characterized by an inherent capability for dynamic adaptation (self-learning based on large datasets) and functional capacity to directly or indirectly shape, optimize, or implement algorithmic decisions (predictions, recommendations) that possess a legally significant nature and can create potential risks to fundamental human rights and freedoms, national security, democratic governance, and public order. A clear legal distinction is drawn between the AI system and the Internet of Things (IoT), where the latter is defined as a digital and hardware infrastructure for automated collection and cross-border

exchange of data between devices, which retains a human-oriented model and is devoid of cognitive functions of non-linear decision-making.

Based on a comparative analysis, an in-depth study of international experience in the legal regulation of AI is carried out, revealing conceptual, normative, and institutional features of respective models in leading jurisdictions. Two opposite global trends in the development of information-legal policy are identified: the universal level (UN acts, Okinawa Charter, Geneva Declaration of 2003), where AI was long considered exclusively within the general ICT sector without isolating it as an independent object of security regulation, and the European regional level (Council of Europe, EU), which formed a preventive, value-oriented model of "managed autonomy". The genesis of the transformation of "soft law" instruments into imperative regimes of "hard law", codified in Regulation (EU) 2024/1689 (Artificial Intelligence Act) and the Council of Europe Framework Convention on AI, is analyzed in detail. The specific features of legal instruments for admitting high-risk systems to the market (conformity assessment, logging, human oversight, fundamental rights impact assessment (*FRIA*), and mandatory registration in the EU database from August 2026) are disclosed. Differentiated geopolitical models are categorized separately: the decentralized risk-oriented model of the USA and the centralized preventive-supervisory model of the PRC (exemplified by the CAC 2025 Temporary Measures on interactive AI services), where the priority of national security and state control prevails over the technological autonomy of subjects. The European experience of integrating the AI Act with existing large information systems of migration and security (*VIS*, *Eurodac*, *EES*, *ETIAS*, *ECRIS-TCN*) is analyzed.

As a result of generalizing these approaches, it is substantiated that the key trends in the development of AI legal regulation are the transition from reactive control of consequences to proactive risk-oriented management models throughout the entire lifecycle of technology, strengthening requirements for algorithmic transparency, accountability, and explainability. The directions of harmonization of the national legislation of Ukraine with European standards are determined, providing

for the construction of a holistic normative architecture (a framework law, mutually agreed amendments to basic laws, and a system of secondary legislation), which must be implemented not through mechanical copying of foreign norms, but by adapting them to the national system of public administration, the structure of authorities, and the challenges of state recovery. Doctrinal approaches to legal capacity in the digital era are systematized: the concept of an "electronic person" is critically analyzed, and its non-delictual capacity is proven due to the absence of autonomous legal will, legal consciousness, and the psycho-emotional component of guilt in AI. The subordination of AI to the legal regime of a source of increased danger and a "thinking thing" (*res cogitans*) is substantiated, where the general burden of risks is imposed on its owner, and a functional distinction is drawn between non-autonomous AI (the stage of institutional learning under the teleological control of a human) and autonomous AI (capable of performing tasks under the systemic supervision of a human but without step-by-step guidance).

The thesis develops a conceptual model for the institutionalization of public administration of AI in Ukraine, which is grounded on the development of a network (hybrid) management system ensuring a clear separation of political, regulatory, supervisory, human rights, and judicial functions, and excluding the concentration of all powers within a single body. An institutional architecture that eliminates the conflict of objectives between supporting innovation and protecting human rights is proposed by legally establishing a functional matrix of competence, which defines the interaction of subjects: the Cabinet of Ministers of Ukraine (general direction of policy), the Ministry of Digital Transformation of Ukraine (central coordinator of development and methodological support), the functionally independent National Competent Supervisory Authority (a central executive body with special status, endowed with rights to conduct audits and apply financial sanctions), sectoral regulators, the Ukrainian Parliament Commissioner for Human Rights (human rights control), and judicial bodies (final control of legality). The expediency of establishing a state registry of high-risk AI systems and implementing a regulatory experimental

environment (*AI Sandbox*) as a legal tool for testing innovative solutions within a controlled environment is substantiated.

A separate block of the study is devoted to the development of a methodology for analytical support and procedural management of the artificial intelligence lifecycle. Based on the categorical apparatus of the theory of law and administrative law, the necessity of expanding the classical structure of the mechanism of legal regulation (MLR) by incorporating novel organic-functional elements into it is argued: risk management, conformity assessment, algorithmic transparency, independent audit, certification, and preventive state supervision. The theoretical and methodological foundations of a holistic risk-based legal policy in the field of AI are established, defined as a systemic activity of the state aimed at forming differentiated legal regimes, where the scope of prohibitions and obligations correlates with the scale, severity, and reversibility of a specific system's impact. An original axiological risk-based test for the administrative-legal assessment of AI admissibility is proposed, which, unlike the market-functional approach of the AI Act, is rooted in the hierarchy of constitutional legal values and comprises four successive levels evaluating the technology's impact on: 1) human life and health (axiological basis – Article 3 of the Constitution of Ukraine, Article 2 of the ECHR); 2) national security and state resilience under conditions of armed aggression; 3) fundamental individual rights and freedoms in the sphere of public services; 4) democratic governance, the rule of law, and the institutional capacity of authorities (*AI Governance*). A new legal principle is substantiated – the principle of proportionality of administrative-legal impact, according to which the intensity of state intervention and the imperativeness of control correlate directly with the degree of potential threat the AI system poses to the objects of protection.

Based on empirical analysis (results of the author's sociological-legal survey of 1092 respondents, data from Gradus Research, KIIS, and global monitoring databases AI Incident Database, OECD, and MIT AI Risk Repository), a systemic zoning and classification of AI systems into five risk categories is carried out: prohibited practices of unacceptable risk (manipulative use, social scoring of citizens,

indiscriminate biometric collection), high-risk systems (safety components of infrastructure, biometrics, law enforcement, migration, and justice spheres), limited risk systems (transparency and content marking requirements), minimal risk systems, and general-purpose AI models (including models with systemic risk). Twelve interconnected administrative procedures covering the full lifecycle of an AI system are systematized: from preliminary inventory, classification, and verification of less restrictive alternatives to mandatory fundamental rights impact assessment (*HRIA/FRIA*), maintaining the State Registry of High-Risk Systems with a risk passport, ensuring models of human control (*human-in-the-loop* or *human-on-the-loop*), post-market monitoring, reporting serious incidents within 72 hours, and ensuring an individual's right to a clear, meaningful explanation of the factors behind an automated decision. It is proved that the specificities of martial law require the application of accelerated or special closed procedures for the defense, intelligence, and security sectors, with the mandatory preservation of legality, documentation, and the personal responsibility of a military official within the standard of *meaningful human control* over the use of force. The thesis provides a complex sectoral analysis of the limits of permissible algorithmization of social relations within the most axiologically sensitive sectors of public life. The legal boundaries for the use of medical AI are determined, where based on the six fundamental principles of the WHO, legal regimes are differentiated: autonomous modes (*human-out-of-the-loop*) are defined as permissible exclusively at the stages of primary screening and pre-clinical modeling, whereas the direct establishment of a final diagnosis and treatment planning require the mandatory preservation of the human-centered standard of medical care and the clinical judgment of a human doctor as a subject of legal liability. The concept of the legal impermissibility of algorithmic deformation of discretionary powers of law enforcement agencies and justice is substantiated, which excludes the existence of autonomous algorithmic law enforcement or the replacement of individual judicial discretion by automated conclusions of algorithms with closed logic ("black boxes"). It is proved that AI in these fields must act exclusively as an auxiliary tool for information-analytical support under conditions of

its explainability, transparency, and the possibility of independent audit. The lawfulness of cross-border application of facial recognition databases under conditions of repelling armed aggression for identifying those involved in war crimes is substantiated exclusively in the presence of a clear legal basis and strict time constraints. The boundaries of lawful use of AI systems in education and scientific activity are established, providing for the impermissibility of imitating authorship, replacing independent cognitive activity, and destroying academic freedom, thereby defining AI tools as means of technical and informational support.

A holistic theoretical and methodological concept of public administration of the use of AI systems is formed, integrating human-centered, risk-based, service, and security paradigms. The conceptual dualism of the axiological-legal dimension of AI is disclosed, consisting in the doctrinal coexistence of humanistic and transhumanistic development models, where law itself holds the decisive role in ensuring human autonomy. A complex three-tiered model of normative improvement is developed and substantiated, the foundation of which is the draft framework Law of Ukraine "On the Safe and Responsible Use of Artificial Intelligence Systems" (combining market and human rights approaches), a harmonized package of amendments to basic acts (including the addition of Article 69-1 to the Law of Ukraine "On Administrative Procedure", which directly regulates algorithmically supported decisions and establishes the obligation of an official to form a reproducible algorithmic trail, as well as amendments to laws on personal data protection, public procurement, public electronic registries, and access to information), and procedural decrees of the Cabinet of Ministers of Ukraine, which in their entirety ensure the creation of an effective, adaptive, and holistic mechanism of *AI governance* in Ukraine in accordance with the best European standards.

Keywords: theoretical and methodological framework, legal framework, artificial intelligence, artificial intelligence system, public administration, information law, administrative procedure, risk-based approach, axiology, human control, network institutional model, European integration, digitization, mechanism of legal regulation.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ
Наукові праці, у яких опубліковано основні наукові результати дисертації
Монографія

1. Варинський В. Штучний інтелект в освіті: проблеми впровадження та регулювання. *Створювальна сила знання* : монографія. Книга друга / авт. кол. ; відп. ред.: І. А. Доннікова, Н. В. Кривцова. Київ : 7БЦ, 2025. С. 145–163.

Статті у наукових виданнях, включених до Переліку наукових фахових видань України

2. Варинський В. О. Сучасні напрямки соціально-правових досліджень штучного інтелекту. *Наукові перспективи*. 2022. №. 12 (30). С. 299–310. DOI: [https://doi.org/10.52058/2708-7530-2022-12\(30\)-299-310](https://doi.org/10.52058/2708-7530-2022-12(30)-299-310)

3. Варинський В. О. Правосуб'єктність штучного інтелекту: міф чи реальність. *Юридична Україна*. 2024. № 11. С. 60–68. DOI: 10.37749/2308-9639-2024-11(263)-6. URL: <https://yur-ukraine.com/pravosubyektnist-shtuchnogo-intelektu-mif-chy-realnist-2/>

4. Варинський В. О. Правосуб'єктність штучного інтелекту: критичний погляд на автономність. *Інформація і право*. 2024. № 4 (51). С. 83–94. DOI: [https://doi.org/10.37750/2616-6798.2024.4\(51\).317919](https://doi.org/10.37750/2616-6798.2024.4(51).317919)

5. Варинський В. О. Стан правового регулювання використання штучного інтелекту у законодавстві України. *Юридична Україна*. 2025. № 1. С. 40–50. DOI: 10.37749/2308-9639-2025-1(265)-6. URL: <https://yur-ukraine.com/stan-pravovogo-regulyuvannya-vykorystannya-shtuchnogo-intelektu-u-zakonodavstvi-ukrayiny>

6. Варинський В. О. Соціально-правові чинники формування довіри до штучного інтелекту (Частина 1). *Право і суспільство*. 2025. № 6. С. 524–532. DOI: <https://doi.org/10.32842/2078-3736/2025.6.73>

7. Варинський В. О. Основні підходи правового регулювання використання штучного інтелекту в освіті. *Актуальні проблеми вдосконалення чинного законодавства України*. 2025. № 69. С. 140–151. DOI: <https://doi.org/10.15330/apiclu.69.1.40-1.51>

8. Варинський В. Алгоритмічне забезпечення охорони громадського порядку : правові межі застосування штучного інтелекту у діяльності правоохоронних органів. *Академічні візії*. 2025. № 48. С. 1–11. URL: <https://www.academy-vision.org/index.php/av/article/view/3189>

9. Варинський В.О. Нормативне регулювання використання штучного інтелекту у правосудді. *Журнал східноєвропейського права*. 2025. № 140. С. 291 – 299. DOI: <http://doi.org/10.71404/2409-6415.140.35>

10. Варинський В. О. Правова парадигма довіри до штучного інтелекту (Частина II). *Право і суспільство*. 2026. № 1. С. 258–264. DOI <https://doi.org/10.32842/2078-3736/2026.1.1.33>

11. Варинський В. О. Етичні та правові ризики застосування штучного інтелекту у правоохоронній діяльності та діяльності спецслужб. *Вісник Пенітенціарної асоціації України*. 2026. №1 (35). С. 245–256. DOI: <https://doi.org/10.34015/2523-4552.2026.1.22>

12. Варинський В. О. AI Act як ризик-орієнтована модель правового обмеження застосування штучного інтелекту у правоохоронній діяльності та діяльності спецслужб. *Південноукраїнський правничий часопис*. 2026. № 1. С. 134–141. DOI : <https://doi.org/10.32850/sulj.2026.1.23>

13. Варинський В. Правове регулювання обмеження використання штучного інтелекту в медицині: основні міжнародні підходи. *Український часопис міжнародного права*. 2026. № 1. С. 21–33. DOI: <https://doi.org/10.36952/ujil.2026.1.3>

14. Варинський В. О. Оцінка впливу високоризикових систем штучного інтелекту на права людини як інструмент правової політики України. *Академічні візії*. 2026. Вип 53. DOI: <https://doi.org/10.66556/2786-586X.53.varynskyi-v>

Статті у закордонних виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus

15. Varynskyi V., Varynska A., Kostytsky M., Kushakova-Kostytska N. Information security and information hygiene on internet media. *Nexo Revista*

Científica. 2021. Vol. 34. № 1. P. 120–128. DOI: <https://doi.org/10.5377/nexo.v34i01.11291>

16. Varynskyi V., Shelever N., Yankovyi M., Pylyp V., Antalovtsi O., Halahan O. Use of the “electronic court” service as a means of citizens' access to the judiciary. *Lex Humana*. 2023. Vol. 16. № 1. P. 249–266. URL: <https://seer.ucp.br/seer/index.php/LexHumana/article/view/2891>

17. Rudenko O., Rafalskyi I., Yermak O., Varynskyi V., Konoplia Y. The potential and prospects of artificial intelligence use in strategic planning: issues of security and defense. *AD ALTA: Journal of Interdisciplinary Research*. 2024. Vol. 14/02-XLIV. P. 6–12. URL: https://www.magnanimitas.cz/ADALTA/140244/papers/A_01.pdf

18. Rudenko O., Zaika O., Varynskyi V., Kulchii I., Myroshnychenko A. Digitization of local self-government based on the use of artificial intelligence in the context of sustainable development. *Edelweiss Applied Science and Technology*. 2024. Vol. 8. № 6. P. 1467–1480. DOI: <https://doi.org/10.55214/25768484.v8i6.2263>

Статті у наукових періодичних виданнях інших держав

19. Varynskyi V. Health-saving technologies in the context of globalization. *International Journal of Recent Technology and Engineering (IJRTE)*. 2019. Vol. 8. Issue 4S. P. 63–67. DOI: 10.35940/ijrte.D1023.1184S19

20. Varynskyi V., Donnikova I., Savinova N. Artificial intelligence in education: tool, object, «subject» of learning. *Journal of International Legal Communication*. 2023. Vol. 10. № 3. P. 46–55. DOI: <https://doi.org/10.32612/uw.27201643.2023.10.3.pp.46-55>

Наукові праці, які засвідчують апробацію матеріалів дисертації

1. Варинський В.О., Савінова Н.А. Два епізоди кримінальної юстиції майбутнього: футуристичний прогноз. *Наукові читання присвячені пам'яті професора Т.А. Денисової* : збірник матеріалів (м. Запоріжжя, 10 березня 2022 р.). Класичний приватний університет. Запоріжжя : КПУ, 2022. С. 308–311.

2. Варинський В. Філософські засади концепції інтернету речей.

Людина має право: соціально-гуманітарний дискурс у контексті реформаційних процесів в Україні: матеріали круглого столу (м. Одеса, 17 листопада 2022 р.). Одеса : ОДУВС, 2022. С. 15–18. URL: <http://dspace.pdpu.edu.ua/jspui/bitstream/123456789/16985/1/SviRLYTSKAIA.pdf#page=16>

3. Варинський В.О. Основні настанови резолюції Європарламенту про цивільно-правові норми в робототехніці та штучний інтелект: дайджест основних підходів. *Вдосконалення правового регулювання прав та основних свобод людини і громадянина* : матеріали щорічної Всеукраїнської науково-практичної конференції молодих вчених (м. Івано-Франківськ, 5-6 травня 2023 р.). Івано-Франківськ, 2023. С. 78–81. URL: <https://law.cnu.edu.ua/wp-content/uploads/sites/100/2024/12/youth2023-r.pdf>

4. Варинський В. Штучний інтелект та освіта. *Створювальне знання: освіта для майбутнього* : матеріали 6-го круглого столу в рамках науково-освітнього міжнародного проєкту «Створювальне знання: науково-освітні практики 3.0» (м. Одеса, 9 червня 2023 р.). Одеса : НУОМА, 2023. С. 5–8. URL: http://onma.edu.ua/wp-content/uploads/2023/09/Materialy_6-go_kruglogo-stolu_23.pdf

5. Варинський В. Штучний інтелект та проблеми безпеки. *Сучасна парадигма публічного управління* : збірник тез V Міжнародної науково-практичної конференції (м. Львів, 30 листопада – 2 грудня 2023 р.) / За наук. ред. к.е.н., доцента Стасишина А.В. Львів: ЛНУ імені Івана Франка. Львів, 2024. С. 512–515. URL: https://nung.edu.ua/sites/default/files/2024-06/Збірник_5_Парадигма_2024.pdf

6. Варинський В.О. Ризики використання елементів штучного інтелекту в розробках автономної зброї: на шляху визначень нормативних обмежень. *Штучний інтелект у правовій практиці: межі та можливості*: матеріали Всеукраїнського круглого столу (м. Львів, 15 березня 2024 р.). Львів: ЛьвДУВС, 2024. С. 45–49. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/7424/1/15_03_2024.pdf

7. Варинський В. О., Савінова Н. А. Ефективність удосконалення законодавства та штучний інтелект. *Проблеми інформаційного забезпечення та розвитку парламентського контролю в контексті Європейської та Євроатлантичної інтеграції України* : матеріали науково-практичної конференції (м. Київ, 25 квітня 2024 р.). Київ; Одеса : Фенікс, 2024. С. 107–111. URL: https://ippi.org.ua/sites/default/files/konferenciya_25.04.2024.pdf

8. Варинський В. Правосуб'єктність штучного інтелекту: впродовження ідей О. А. Баранова. *Україна в умовах соціальної та цифрової трансформації: шляхи до сталого розвитку та повоєнної відбудови* : матеріали науково-практичної конференції (м. Київ, 22 листопада 2024 р.). ДНУ «Інститут інформації, безпеки і права Національної академії правових наук України». Київ; Одеса : Фенікс, 2024. С. 185–191. URL: https://ippi.org.ua/sites/default/files/ukrayina_v_umovah_socialnoyi_ta_cifrovoyi_transformaciyi_maket.pdf

9. Варинський В. Ризики використання ШІ в правосудді: огляд проблеми. *Трансформаційні процеси правотворчої діяльності та парламентського контролю* : матеріали науково-практичної конференції (м. Київ, 30 жовтня 2025 р.). Київ; Одеса : Фенікс, 2025. С. 97–101. URL: https://ippi.org.ua/sites/default/files/zbirnik_tez_30.10.2025.pdf

10. Варинський В. Основні критерії заборон використання ШІ за AI Act. *Україна в умовах соціальної та цифрової трансформації : теоретичні моделі правового регулювання штучного інтелекту* : матеріали науково-практичної конференції (м. Київ, 5 листопада 2025 р.). Київ; Одеса : Фенікс, 2025. С. 116–120. URL: https://ippi.org.ua/sites/default/files/zbirnik_tez_05.11.2025_1.pdf

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	22
ВСТУП.....	23
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНО-ПРАВОВОГО ТА АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ.....	43
1.1. Генеза інформаційно-правового регулювання штучного інтелекту та його співвідношення з Інтернетом речей	43
1.2. Аксіологічний вимір використання штучного інтелекту.....	69
1.3. Соціальні очікування і перестороги щодо впровадження штучного інтелекту як емпірична основа ризикоорієнтованого правового регулювання.....	83
Висновки до розділу 1.....	94
РОЗДІЛ 2. МІЖНАРОДНІ ТА НАЦІОНАЛЬНІ ПРАВОВІ ЗАСАДИ ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ.....	99
2.1. Міжнародно-правові стандарти безпечного та відповідального використання штучного інтелекту.....	103
2.2. Правовий статус суб'єктів створення, впровадження та використання штучного інтелекту.....	138
2.3. Стан адміністративно-правового та інформаційно-правового регулювання використання штучного інтелекту в Україні	169
Висновки до розділу 2.....	190
РОЗДІЛ 3. ОБМЕЖЕННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОКРЕМИХ СФЕРАХ ПРАВОВІДНОСИН.....	193
3.1. Соціальні передумови обмеження використання штучного інтелекту в окремих сферах життєдіяльності людини.....	193
3.2. Правове регулювання використання штучного інтелекту в автономній зброї.....	209

3.3. Правове регулювання обмеження використання штучного інтелекту в медицині.....	235
3.4.Правове регулювання обмеження використання штучного інтелекту в правоохоронній діяльності та діяльності спецслужб.....	264
3.5.Правове регулювання обмеження використання штучного інтелекту в правосудді.....	285
3.6.Правове регулювання обмеження використання штучного інтелекту в освіті та науці.....	313
Висновки до розділу 3.....	328
РОЗДІЛ 4. ФОРМУВАННЯ СУЧАСНОЇ ІНСТИТУЦІЙНОЇ МОДЕЛІ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ В УМОВАХ ЄВРОІНТЕГРАЦІЇ	335
4.1. Ризик-орієнтована правова політика та адміністративні процедури обмеження використання штучного інтелекту в Україні.....	336
4.2. Напрями розвитку інституційної моделі публічного адміністрування та вдосконалення законодавства України у сфері використання штучного інтелекту в умовах євроінтеграції	381
Висновки до розділу 4.....	406
ВИСНОВКИ.....	413
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	426
ДОДАТКИ.....	490

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

- ШІ** – штучний інтелект (Artificial intelligence – AI)
- ІоТ** – інтернет речей (Internet of things)
- ІТ** - інформаційні технології (Information Technology)
- ООН** – Організація Об'єднаних Націй
- ЄС** – Європейський Союз
- РЄ** – Рада Європи
- ОБСЄ** – Організація безпеки і співробітництва в Європі
- ВРУ** – Верховна Рада України
- КМУ** – Кабінет Міністрів України
- РНБО** – Рада Національної Безпеки та Оборони
- ВС** – Верховний Суд
- ОПУ** – Офіс Президента України
- МЦТУ** – Міністерство цифрові трансформації України
- МОУ** – Міністерство оборони України
- NATO** – Південноатлантичний альянс (North Atlantic Treaty Organization)
- NASA** – Національне управління з аероавтики і досліджень космічного простору США (National Aeronautics and Space Administration)
- ВООЗ** – Всесвітня організація охорони здоров'я
- СІМІС** - Цивільно-військове співробітництво (Civil-Military Co-operation)
- ІпсЗ** – інформаційно-психологічна зброя

ВСТУП

Обґрунтування вибору теми дослідження. Стрімкий розвиток технологій штучного інтелекту (далі – ШІ) став одним із визначальних чинників сучасної цифрової трансформації суспільства, державного управління та економіки. Системи штучного інтелекту дедалі активніше використовуються у сфері публічного адміністрування, правосуддя, охорони здоров'я, фінансової діяльності, оборони, національної безпеки, освіти, транспортної інфраструктури та інших сферах, у яких результати їх функціонування безпосередньо впливають на реалізацію прав, свобод і законних інтересів людини. Водночас розширення масштабів використання ШІ зумовлює виникнення якісно нових суспільних відносин, які потребують адекватного правового регулювання.

Сучасний розвиток ШІ характеризується переходом від допоміжних інформаційних технологій до автономних систем, здатних приймати рішення, що мають юридично значущі наслідки. Така трансформація зумовлює необхідність переосмислення традиційних підходів до правового регулювання, оскільки існуючі правові механізми були сформовані для регулювання діяльності людини та класичних інформаційних систем і не враховують особливостей функціонування автономних алгоритмічних моделей, генеративного штучного інтелекту, великих мовних моделей та інших сучасних AI-систем.

Особливої актуальності зазначена проблема набуває в умовах інтеграції України до Європейського Союзу та необхідності гармонізації національного законодавства із Регламентом (ЄС) 2024/1689 про встановлення гармонізованих правил щодо штучного інтелекту (AI Act), який започаткував принципово нову ризик-орієнтовану модель правового регулювання використання штучного інтелекту. Водночас імплементація європейських стандартів не може обмежуватися формальним перенесенням положень AI Act до національного законодавства, оскільки вони повинні бути адаптовані до особливостей системи публічного адміністрування України, структури органів державної влади,

національного законодавства та існуючих механізмів реалізації владних повноважень.

Базовим документом державної політики в Україні в сфері регулювання ІІІ залишається Концепція розвитку штучного інтелекту в Україні, затверджена Кабінетом Міністрів України ще у 2020 році, на її виконання Кабінет Міністрів України у 2025 році затвердив План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки.

Україна демонструє вражаючі темпи цифрової трансформації, що створює фундамент для впровадження ІІІ: 1-ше місце у світі за Індексом електронної участі ООН (E-Participation Index), що свідчить про найвищий рівень залучення громадян до демократичних процесів через цифрові інструменти; 5-те місце у світі за Індексом онлайн-послуг ООН (Online Services Index) у 2024 році Україна піднялася на 97 позицій з 2018 року [155; 156]; 40-ве місце серед 195 країн у Government AI Readiness Index 2025 від Oxford Insights, при цьому показник цифровізації державних послуг досяг 99,63%, що відносить Україну до 10-ки країн Східної Європи у сфері розвитку ІІІ [256]. Отже, досягнутий Україною рівень цифрової трансформації створює об'єктивні передумови для масштабного використання технологій ІІІ. Масштабність та невідворотність цього процесу підтверджуються останніми макроекономічними та соціологічними маркерами 2025 – 2026 років. На глобальному рівні, за прогнозами аналітичних агентств Gartner та MarketsandMarkets, світові витрати на ІІІ, які у 2025 році становили 1,48 трлн дол. США, вже у 2026 році перетнули межу у 2 трлн дол. США, демонструючи стрімку капіталізацію ринку з тенденцією досягнення 2,4 трлн дол. США до 2032 року [388; 290].

На національному рівні зазначені тенденції віддзеркалюються у безпрецедентній динаміці залученості населення: за даними дослідницьких компаній Gradus Research та КМІС (січень – березень 2026 року), до 85% українців використовують ІІІ регулярно або фрагментарно, причому найвища залученість фіксується серед молоді віком 18–29 років (58% регулярних користувачів) [234]. Концентрація споживчого попиту навколо безкоштовних

версій домінуючих мультимодальних сервісів (ChatGPT, Gemini) у поєднанні з низькою готовністю індивідуальних користувачів інвестувати у платний контент (лише 6%) свідчить про те, що масова інтеграція технологій ШІ в Україні відбувається стихійно та переважно поза межами корпоративного або суворого відомчого контролю. Водночас це актуалізує необхідність формування сучасних теоретико-методологічних і правових засад їх використання.

Попри активний розвиток міжнародного та європейського правового регулювання використання ШІ, в Україні досі відсутня цілісна концепція правового забезпечення його використання. Чинне законодавство чітко не визначає системи суб'єктів публічного адміністрування у сфері штучного інтелекту, їх компетенції, повноважень, адміністративно-правового статусу, порядку взаємодії, механізмів державного контролю, розподілу юридичної відповідальності, реалізації принципу змістовного людського контролю (meaningful human oversight) та адміністративно-правових гарантій захисту прав людини при використанні систем ШІ. Необхідність імперативного втручання публічної адміністрації та побудови жорстких правових бар'єрів обумовлюється стрімкою ескалацією правопорушень та інцидентів, пов'язаних із деструктивним або технічно недосконалим функціонуванням алгоритмічних моделей. Згідно з верифікованими даними глобальних моніторингових платформ AI Incident Database, OECD та MIT AI Risk Repository, кількість інцидентів у сфері ШІ зростає на 35–45% щороку, причому понад 58% із них безпосередньо зумовлені генеративними технологіями [464].

Тільки за останній звітний період зафіксовано сотні критичних інцидентів, архітектоніка яких чітко диференціюється за категоріями правової шкоди: дезінформація та деструктивний контентний вплив (28%), алгоритмічна дискримінація й упередженість (22%), а також прямі помилки у сфері фізичної та цифрової безпеки (14%) [464]. Особливу небезпеку для правопорядку становлять протиправні прояви у вигляді дипфейків (технології підробки голосу та відео), які виступають інструментарієм у понад 80% випадків

масштабного кібершахрайства та фінансових махінацій. Ба більше, фіксація випадків генерації чат-ботами небезпечного контенту, що призводив до закликів до насильства або депресивних станів користувачів (зокрема, за участю найбільш поширеного інструменту ChatGPT), свідчить про наявність латентних екзистенційних та безпекових ризиків навіть у межах найбільш технологічно захищених систем [464].

Не менш важливою є необхідність формування сучасної доктрини адміністративно-правового регулювання використання штучного інтелекту, яка враховуватиме не лише технологічні особливості AI-систем, а й конституційні засади діяльності держави, принцип верховенства права, пріоритет прав і свобод людини, принципи належного врядування, цифрової трансформації та людиноцентризму. Відсутність таких доктринальних підходів істотно ускладнює вироблення ефективної державної політики у сфері використання штучного інтелекту, побудову дієвого механізму адміністративно-правового регулювання та визначення місця штучного інтелекту в системі публічного адміністрування.

Актуальність дисертаційного дослідження обумовлюється також практичними потребами держави. Використання систем ШІ вже сьогодні є одним із ключових напрямів цифровізації публічного управління, розвитку електронного урядування, цифрових адміністративних послуг, систем підтримки прийняття управлінських рішень, правоохоронної діяльності, оборонного сектору та відновлення України. За таких умов виникає об'єктивна необхідність створення ефективного адміністративно-правового механізму, який забезпечуватиме баланс між стимулюванням інноваційного розвитку та належним рівнем захисту прав людини, суспільних інтересів і національної безпеки.

Таким чином, актуальність теми дослідження зумовлена сукупністю взаємопов'язаних чинників: відсутністю цілісної адміністративно-правової доктрини використання штучного інтелекту в Україні; необхідністю адаптації європейських стандартів AI Governance до національної системи публічного

адміністрування; потребою у формуванні теоретико-методологічних засад адміністративно-правового регулювання використання штучного інтелекту, а також практичною необхідністю вдосконалення механізму державного управління процесами створення, впровадження, використання та контролю за застосуванням систем ІІІ.

Ступінь наукової розробленості проблеми. Аксіолого-правовий та методологічний фундамент роботи побудовано на засадах людиноцентричного розуміння права, пріоритетності фундаментальних свобод особи та її захисту від ризиків алгоритмічної автономізації. Вихідним орієнтиром у цьому контексті стали загальнотеоретичні підходи П. Рабіновича щодо людиноцентричного розуміння права, які в умовах зростання технологічних загроз, пов'язаних із використанням автономних цифрових систем, безпосередньо корелюють із західними концепціями відповідальності за технологічне майбутнє Г. Йонаса (H. Jonas), Х. Дрейфуса (H. Dreyfus) та доктриною проєктування, чутливого до ціннісних імперативів (Value Sensitive Design – Б. Фрідман (B. Friedman), Д. Генрі (D. G. Hendry), А. Борнінг (A. Borning).

На цьому фундаментальному підґрунті в українській юридичній науці сформувався напрям, присвячений концептуалізації цифрового правопорядку та визначенню правової природи штучного інтелекту, базові засади якого закладено у загальнотеоретичних працях О. Баранова, М. Карчевського та О. Костенка. Поряд із цим, на осмислення конкретних онтологічних та правових викликів функціонування алгоритмічних систем зорієнтовані дослідження К. Некіт, О. Радутного та О. Харитонової. Напрацювання зазначених авторів, присвячені проблематиці правової природи штучного інтелекту, відсутності у нього автономної юридичної волі та специфіці цивільно-правових ризиків, дозволяють чітко диференціювати штучний інтелект як самостійний цифровий феномен від суміжних технологічних систем, насамперед Інтернету речей (IoT).

У свою чергу, питання модернізації правової політики держави в умовах цифровізації та адаптації національного законодавства до європейських

стандартів висвітлено у працях Д. Белова, О. Ковальчук, О. Олійник, В. Пилипчука, О. Павлюк, Т. Попової, Є. Тимошенко, Ю. Тюрі.

Доктринальні положення та окремі аспекти адміністративно-правового й інформаційно-правового характеру щодо формування та реалізації державної політики були предметом вивчення таких вчених як: В. Авер'янов, О. Баранов, К. Беляков, Ю. Битяк, В. Василенко, В. Галунько, В. Грохольський, А. Денисова, Д. Журавльов, Д. Калаянов, Р. Калюжний, В. Колпаков, С. Кудінов, М. Корнієнко, В. Пядишев, Н. Свиридчук, В. Стефанюк, С. Тімченко, , Т. Тур, Т. Фулей, І. Цюприк, Ю. Шемшученко, М. Янишівського, Х. Ярмачі та ін. На галузевому рівні найбільш розробленими у вітчизняній доктрині є питання алгоритмізації та деліктних ризиків у діяльності органів судової влади, що відображено у працях Я. Берназюка, О. Гиляки, О. Карпушової, та В. Рядінської. Водночас процесуальні загрози, межі предиктивного моделювання та ризики порушення фундаментальних прав особи у сфері кримінальної юстиції, правоохоронної діяльності та забезпечення безпеки стали предметом ґрунтовного вивчення у дослідженнях Н. Глинської, І. Гловчук, Д. Клепки, А. Нікітіна, Ю. Рєпіної, Н. Савінової, Г. Тетерятник, І. Тітка та О. Торбаса. Окреслена галузева проблематика суттєво розширюється зарубіжним доктринальним досвідом. Зокрема, у працях М. Еберса (M. Ebers), А. Ренди (A. Renda), а також у доповідях OECD та Ada Lovelace Institute обґрунтовано необхідність секторальних обмежень використання ШІ у сферах охорони здоров'я, національної оборони та освіти і науки.

Водночас аналіз сучасного стану наукової розробленості проблематики свідчить, що переважна більшість досліджень присвячена окремим правовим аспектам використання ШІ: визначенню його правової природи, питанням цивільної, кримінальної чи інформаційно-правової відповідальності, захисту персональних даних, етичним засадам функціонування алгоритмічних систем або аналізу окремих положень AI Act. Такий підхід не забезпечує цілісного розуміння систем ШІ як об'єкта адміністративно-правового та інформаційного регулювання та не дозволяє сформулювати комплексну модель державного впливу

на процеси його створення, впровадження, використання й контролю. Саме тому предметом цього дослідження є не окремі правові інститути, а теоретико-методологічні та правові засади використання штучного інтелекту, які розглядаються крізь призму механізму адміністративно-правового регулювання, системи його суб'єктів, принципів, форм, методів, адміністративно-правових режимів та гарантій забезпечення прав людини. Такий підхід дозволяє перейти від дослідження окремих правових проблем до формування цілісної доктринальної концепції адміністративно-правового забезпечення використання систем ШІ в Україні.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Тема дисертаційного дослідження узгоджується з положеннями: 1) п. 4 розділу 1 та 47 розділу 3 Стратегії національної безпеки України (Указ Президента України від 14.09.2020 р. № 392/2020); 2) п.п. 4 та 5 Стратегії кібербезпеки України (Указ Президента України від 26.08.2021 р. № 447/2021); 3) п. 1.2 розділу II Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 27 роки (Указ Президента України від 11.05.2023 р. № 273/2023); 4) п. 16 Плану заходів на 2025 рік реалізації Стратегії кібербезпеки України (Розпорядження КМУ від 07.03.2025 р. № 204-р); 5) п.п. 3, 7, 11, 13 Тематики наукових досліджень та науково-технічних (експериментальних) розробок на 2025–2029 роки (наказ МВС від 21.05.2024 р. № 326); 6) темою науково-дослідних робіт Одеського державного університету внутрішніх справ «Пріоритетні напрямки розвитку реформування правоохоронних органів в умовах розгортання демократичних процесів у державі» (номер державної реєстрації 0123U103538), Тем кафедри адміністративного права та адміністративного процесу ОДУВС «Забезпечення адміністративно-правовими засобами прав і свобод людини і громадянина в Україні» (реєстраційний номер 0125U001209), кафедри кримінального аналізу та інформаційних технологій ОДУВС «Інформаційні технології: сучасний стан, особливості в умовах війни та післявоєнний період» (реєстраційний номер 0123U103748).

Мета і завдання дослідження. *Метою дослідження є формування теоретико-методологічних та правових засад використання штучного інтелекту в Україні, а також обґрунтування напрямів удосконалення національного законодавства відповідно до європейських стандартів правового регулювання штучного інтелекту.*

Для досягнення зазначеної мети поставлено такі *завдання*:

- дослідити генезу інформаційно-правового регулювання систем штучного інтелекту та його співвідношення з Інтернетом речей;
- розкрити аксіологічні засади використання систем штучного інтелекту та визначити систему цінностей, що підлягають охороні в процесі його створення, впровадження та використання;
- проаналізувати соціальні очікування, ризики та суспільні перестороги щодо використання штучного інтелекту як емпіричну основу формування ризик-орієнтованої моделі правового регулювання;
- систематизувати міжнародно-правові стандарти безпечного, відповідального та людиноцентричного використання систем штучного інтелекту та визначити механізми їх імплементації в національну правову систему;
- розкрити особливості правового статусу суб'єктів створення, впровадження та використання систем штучного інтелекту;
- провести комплексний аналіз стану правового регулювання використання систем штучного інтелекту в Україні;
- встановити соціально-правові передумови обмеження використання систем штучного інтелекту в окремих сферах суспільних відносин;
- визначити правові межі використання систем штучного інтелекту в автономних системах озброєння;
- охарактеризувати особливості правового регулювання та обмеження використання систем штучного інтелекту у сфері охорони здоров'я;
- розкрити особливості правового регулювання використання штучного інтелекту у правоохоронній діяльності та діяльності спеціальних служб;

- визначити межі допустимого використання систем штучного інтелекту у сфері правосуддя та гарантії забезпечення людського контролю під час ухвалення юридично значущих рішень;
- з'ясувати особливості правового регулювання використання систем штучного інтелекту в освіті та науковій діяльності;
- обґрунтувати концептуальні засади ризик-орієнтованої правової політики та адміністративних процедур у сфері використання штучного інтелекту в Україні;
- розробити сучасну інституційну модель публічного адміністрування використання систем штучного інтелекту в Україні в умовах європейської інтеграції та визначити напрями вдосконалення її адміністративно-правового забезпечення;
- сформулювати комплекс пропозицій щодо вдосконалення законодавства України та механізмів публічного адміністрування у сфері використання систем штучного інтелекту.

Об'єкт та предмет дослідження. *Об'єктом* дослідження є суспільні відносини, що виникають у процесі розроблення, впровадження та використання систем штучного інтелекту в Україні, а також у зв'язку з необхідністю мінімізації їхнього деструктивного впливу на права і свободи людини, національну безпеку та демократичні інститути в умовах цифрової трансформації соціуму.

Предмет дослідження – теоретико-методологічні та правові засади використання штучного інтелекту в Україні

Методи дослідження. Методологічну основу дослідження становить комплекс загальнонаукових та спеціально-юридичних методів, системне застосування яких зумовлене специфікою правового регулювання використання штучного інтелекту, міждисциплінарною природою алгоритмічних систем і потребою модернізації вітчизняного законодавства.

Застосування *діалектичного методу* дозволило розкрити суперечливі тенденції інтеграції штучного інтелекту – посилення його технологічного

потенціалу за одночасного зростання ризиків для прав людини й національної безпеки, а також простежити еволюцію правової політики від реактивного регулювання до проактивних ризик-орієнтованих моделей (розділи 1 – 4).

За допомогою *системного методу* досліджено внутрішні та зовнішні зв'язки між фундаментальними засадами конституційного, адміністративного та інформаційного права України й нормами спеціального законодавства, що регулює стратегічні сфери суспільних відносин, а також визначено місце секторальних обмежень використання алгоритмічних систем у загальній структурі публічно-правового регулювання (розділи 2 – 4).

Структурно-функціональний та аксіологічний методи застосовано для правової оцінки ціннісних засад обмеження використання штучного інтелекту крізь призму імперативів людської гідності, свободи, справедливості, недискримінації та пропорційності. Це дозволило обґрунтувати ризик-орієнтовану модель як легітимний та ефективний превентивний інструмент забезпечення балансу інтересів особи, суспільства й демократичної держави (розділи 1 – 4).

Застосування *когнітивного методу* дозволило дослідити специфіку сприйняття автономності алгоритмічних систем у сучасній правовій свідомості та здійснити концептуальне переосмислення юридичних категорій у сфері цифровізації (розділи 1 – 4).

Завдяки *емпірико-соціологічним методам* (анкетуванню, аналізу результатів авторських опитувань та узагальненню емпіричних даних інших дослідників) з'ясовано реальний стан суспільних очікувань і занепокоєнь щодо інтеграції штучного інтелекту в Україні. Отримані результати дозволили емпірично обґрунтувати вектори та межі нормативних обмежень і правових гарантій на національному рівні (підрозділи 1.3, 3.1).

Використання *прогностичного методу* уможливило визначення довгострокових векторів розвитку цифрового простору в Україні та обґрунтування орієнтирів проактивної правової політики держави, спрямованої на випередження потенційних технологічних загроз (розділи 2 – 4).

Історико-правовий метод дав змогу простежити генезу науково-доктринальних уявлень про штучний інтелект та еволюцію підходів до юридичного визначення його правової природи на різних етапах технологічного розвитку. Це дозволило виявити закономірності переходу від загальних декларативних принципів до сучасних комплексних моделей правового обмеження використання алгоритмічних систем (розділ 1 – 2).

Порівняльно-правовий метод використано для зіставлення вітчизняних підходів із правом Європейського Союзу (насамперед Регламентом ЄС про штучний інтелект), стандартами Ради Європи та правовими моделями окремих іноземних держав (США, Японії, Великої Британії) щодо встановлення заборонених і високоризикових практик використання ШІ (розділи 2 – 4).

Формально-юридичний метод та *метод правового моделювання* застосовано для критичного аналізу чинних і проєктних нормативно-правових актів, з'ясування доктринального змісту юридичних дефініцій, виявлення системних прогалин і колізій, а також побудови авторської секторальної моделі обмежень використання штучного інтелекту та формулювання концептуальних пропозицій щодо вдосконалення правового регулювання (розділи 1 – 4).

Емпіричну базу дисертаційного дослідження становлять матеріали офіційних звітів, аналітичних доповідей, рекомендацій та експертних висновків міжнародних і європейських інституцій, практику Європейського суду з прав людини, документи Європейської комісії, Європейської ради з питань штучного інтелекту, національних регуляторних органів держав-членів Європейського Союзу, рішення судів, результати соціологічних, статистичних та аналітичних досліджень, присвячених суспільному сприйняттю, ризикам та особливостям використання технологій штучного інтелекту в різних сферах суспільних відносин, а також результати проведеного автором опитування 1092 респондентів з питань використання ШІ в Україні.

Наукова новизна отриманих результатів. Наукова новизна дисертаційного дослідження полягає в тому, що воно є першою в Україні комплексною теоретико-прикладною розвідкою, у якій на основі аксіологічних

імперативів людиноцентризму та стандартів Європейського Союзу сформовано теоретико-методологічні та правові засади використання штучного інтелекту й визначено стратегічні орієнтири проактивної правової політики держави в умовах цифровізації суспільних відносин.

Найбільш вагомі результати дослідження, що визначають його наукову новизну та винесені на захист, полягають у такому:

уперше:

- сформульовано авторську дефініцію штучного інтелекту як правової категорії, відповідно до якої його визначено як високотехнологічну автономну інтелектуальну систему машинного походження, що характеризується внутрішньою здатністю до динамічної адаптації (самонавчання на основі великих масивів даних) і функціональною спроможністю безпосередньо або опосередковано формувати, оптимізувати чи реалізовувати алгоритмічні рішення (прогнози, рекомендації), які мають юридично значущий характер та можуть створювати потенційні ризики для фундаментальних прав і свобод людини, національної безпеки, демократичного врядування та публічного порядку;

- запропоновано та обґрунтовано концептуальні основи адміністративно-правового механізму використання систем ШІ, який визначено як багаторівневу динамічну систему взаємопов'язаних принципів, суб'єктів, правових режимів та засобів контролю; визначено нормативну архітектуру цього механізму, що реалізується через розроблену комплексну трирівневу модель (горизонтальний рамковий Закон України «Про безпечне та відповідальне використання систем штучного інтелекту», системні зміни до базового процесуального й інформаційного законодавства та підзаконні акти Кабінету Міністрів України);

- визначено адміністративно-правове зонування (межі) допустимості використання систем ШІ, відповідно до якого правомірність застосування алгоритмічних систем визначається не галузевою сферою їх функціонування, а динамічним співвідношенням ступеня автономності технології, рівня ризику,

інтенсивності втручання у права людини та спроможності здійснення ефективного людського контролю;

- розроблено авторський аксіологічний ризик-орієнтований тест адміністративно-правової оцінки допустимості використання систем штучного інтелекту, який, на відміну від ринково-функціональної моделі класифікації AI Act, ґрунтується на конституційній ієрархії правових благ та передбачає послідовне оцінювання потенційного впливу систем ШІ на: 1) життя і здоров'я людини; 2) національну безпеку та стійкість держави; 3) фундаментальні права, свободи та законні інтереси особи; 4) демократичне врядування, верховенство права й інституційну спроможність публічної влади;

- обґрунтовано новий правовий принцип – принцип пропорційності адміністративно-правового впливу при використанні ШІ, відповідно до якого інтенсивність регуляторного тиску, державного контролю та імперативність адміністративних процедур перебувають у прямій залежності від ступеня потенційної загрози, яку конкретна система ШІ створює для об'єктів адміністративно-правової охорони;

- розроблено засади адміністративної процедури використання високоризикових систем ШІ, яка інтегрує в єдиний послідовний адміністративний процес інвентаризацію, оцінювання ризиків, оцінку відповідності, оцінювання впливу на основоположні права людини (HRIA/FRIA), державну реєстрацію, алгоритмічний аудит, змістовний людський контроль, післяринковий моніторинг та реагування на інциденти;

- запропоновано гібридну мережеву інституційну модель публічного адміністрування у сфері ШІ, яка визначає функціональну систему та правила взаємодії суб'єктів формування державної політики (Кабінет Міністрів України, Мінцифри), незалежного нагляду й контролю (Національний компетентний орган, секторальні регулятори), парламентського правозахисного контролю (Уповноважений ВРУ з прав людини) та судового захисту;

- запропоновано систему адміністративно-правових інструментів супроводу життєвого циклу ШІ, до складу якої включено паспорт ризику

системи ШІ, інтегроване адміністративне досьє, Державний реєстр високоризикових систем, алгоритмічний аудит та модель «відтворюваного алгоритмічного сліду» в адміністративному провадженні;

удосконалено:

- класифікацію етапів та моделей міжнародно-правового реагування на технологічні виклики, яку побудовано з урахуванням еволюції регуляторних моделей від етичного саморегулювання (soft law) до юридично обов'язкового ризик-орієнтованого регулювання (hard law) систем штучного інтелекту, що дало змогу визначити закономірності трансформації міжнародних стандартів у національний правовий механізм;

- наукові підходи до формування понятійно-категоріального апарату дослідження шляхом уточнення змісту та юридичного наповнення категорій «штучний інтелект як об'єкт публічного адміністрування», «механізм адміністративно-правового регулювання використання ШІ», «адміністративно-правовий режим системи штучного інтелекту», «високоризикова система ШІ» та «адміністративно-правовий ризик»;

- класифікацію систем штучного інтелекту в контексті правового регулювання шляхом її доповнення кумулятивними юридично значущими критеріями: рівнем автономності, здатністю до адаптивності, класом ризику, процесуальним контекстом сфери застосування та моделлю необхідного людського контролю;

- функціонально-правовий підхід до оцінки людського контролю за використанням автономних систем озброєння та військових технологій ШІ, відповідно до якого визначальним критерієм визначено не технічну архітектуру взаємодії людини і алгоритму (human-in/on/out-of-the-loop), а реальну здатність військової посадової особи здійснювати змістовний юридично значущий контроль над прийняттям рішення про застосування сили та нести персональну відповідальність за його наслідки;

- теоретичні підходи до визначення адміністративно-правового статусу суб'єктів створення та експлуатації систем ШІ на основі їх

функціонального розмежування залежно від конкретної ролі у життєвому циклі технології та рівня їхньої спроможності контролювати алгоритмічні й правові ризики (розробників, постачальників, розгортувачів та органів нагляду);

- розуміння системи правових засобів регулювання використання систем ШІ шляхом їх групування за функціональним призначенням на регулятивні, превентивні, контрольні-наглядові, інформаційні, процедурні та гарантійні інструменти;

- наукові бачення щодо реалізації ризикоорієнтованої державної правової політики у сфері ШІ шляхом адаптації положень *AI Act* та Рамкової конвенції Ради Європи до правової системи України з урахуванням викликів відновлення держави та режиму воєнного стану;

дістало подальшого розвитку:

- концептуальний дуалізм аксіологічного-правового виміру використання систем ШІ, який полягає у доктринальному співіснуванні гуманістичної та трансгуманістичної моделей технологічного розвитку, що дозволило довести визначальну роль права у забезпеченні пріоритету прав людини, людської автономії та суспільного контролю над використанням автономних алгоритмічних систем;

- теоретико-методологічна доктрина адміністративно-правового регулювання систем ШІ, яка базується на інтеграції людиноцентричної, ризикоорієнтованої, сервісної та безпекової парадигм публічного адміністрування і визначає систему принципів, режимів та інструментів забезпечення правомірного функціонування цифрових технологій;

- доктринальні положення щодо людиноцентричного адміністративно-правового регулювання використання систем ШІ як фундаментальної основи забезпечення балансу між прискореним технологічним розвитком, загальносуспільними інтересами та превентивним захистом прав особи;

- теоретичні засади адміністративно-правового забезпечення алгоритмічної прозорості, підзвітності, пояснюваності та алгоритмічної

справедливості як базових юридичних гарантій захисту прав громадян від упередженості чи помилок систем штучного інтелекту;

- диференційована адміністративно-правова модель допустимої автономії медичного штучного інтелекту, відповідно до якої встановлено правові режими та межі використання систем ШІ залежно від етапу надання медичної допомоги із обов'язковим збереженням остаточного клінічного розсуду за лікарем-людиною;

- концепція правової недопустимості алгоритмічної деформації дискреційних повноважень правоохоронних і судових органів, відповідно до якої впровадження систем ШІ не може призводити до заміщення індивідуального суддівського розсуду чи дискреційної юрисдикції органів правопорядку автоматизованими алгоритмічними висновками, а вимагає обов'язкового збереження персональної відповідальності суб'єкта владних повноважень;

- наукові підходи до визначення меж допустимого використання систем ШІ в освітньому та науковому просторі, що передбачають чітку диференціацію правомірного інформаційно-технічного супроводу від недопустимого заміщення системами ШІ самостійної когнітивної діяльності й академічної свободи.

Практичне значення отриманих результатів полягає в тому, що сформульовані в роботі висновки, рекомендації та пропозиції можуть бути безпосередньо використані:

- у правотворчій діяльності – при підготовці змін до законодавства України, розробленні спеціальних нормативно-правових актів у сфері використання ШІ, а також при формуванні проактивних секторальних напрямів державної правової політики (лист народної депутатки, голови підкомітету з питань вищої освіти Комітету ВРУ з питань освіти, науки та інновацій, д.ю.н., професора Юлії Гришиної від 22.04.2026 (Додаток Б); при розробленні процедур, стандартів і внутрішніх регламентів використання систем ШІ, а також при впровадженні процедур оцінювання впливу на фундаментальні права

людини (FRIA) (довідка про провадження результатів дослідження до Association «METAVERSE-UA», підписана Phd, старшим офіційним членом міжнародної Робочої групи з нагляду за етикою штучного інтелекту, що входить до складу Комітету зі стандартів штучного інтелекту (C/AISC) Асоціації стандартів Інституту інженерів з електротехніки та електроніки (IEEE SA) О. Костенком № 140720266-07-14 від 14.07.2026) (Додаток В);

– у діяльності судових та правоохоронних органів – для запобігання забороненим практикам застосування ШІ у сфері правопорядку та здійснення правосуддя, розподілу відповідальності між суб'єктами їх розроблення, впровадження і використання, а також оцінки доказів, оброблених за допомогою таких систем;

– в освітньому процесі – при викладанні навчальних дисциплін «Кримінальний аналіз», «Пошук інформації з відкритих джерел (OSINT) працівниками кримінальної поліції», «Протидія кіберзлочинності» для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю «Правоохоронна діяльність», «Інформаційна та кібернетична безпека» для здобувачів другого (магістерського) рівня вищої освіти за спеціальністю «Системний аналіз», розроблення освітніх програм, навчально-методичного забезпечення, а також у науково-дослідній роботі здобувачів вищої освіти (акт впровадження в освітній процес ОДУВС від 15.07.2026 б/н) (Додаток Г);

– у науковій діяльності – при виконанні НДР «Пріоритетні напрями реформування правоохоронних органів в умовах розвитку демократичних процесів у державі» (реєстраційний номер 0123U103538) та теми кафедри кримінального аналізу та інформаційних технологій ОДУВС «Інформаційні технології: сучасний стан, особливості в умовах війни та післявоєнний період» (реєстраційний номер 0123U103748) (акт впровадження у наукову діяльність ОДУВС від 15.07.2026 б/н) (Додаток Г).

Апробація результатів дослідження. Висновки і положення дисертаційного дослідження обговорювалися на кафедрі адміністративного права та процесу Одеського державного університету внутрішніх справ, а

також міжкафедральному семінарі. Основні положення дисертаційного дослідження оприлюднені на міжнародних та всеукраїнських конференціях, засіданнях круглих столів, у тому числі: «Наукові читання, присвячені пам'яті професора Т.А. Денисової» (м. Запоріжжя, 10 березня 2022 р.); «Людина має право: соціально-гуманітарний дискурс у контексті реформаційних процесів в Україні» (м. Одеса, 17 листопада 2022 р.); «Вдосконалення правового регулювання прав та основних свобод людини і громадянина» (м. Івано-Франківськ, 5-6 травня 2023 р.); «Створювальне знання: освіта для майбутнього» (м. Одеса, 9 червня 2023 р.); «Сучасна парадигма публічного управління» (м. Львів, 30 листопада – 2 грудня 2023 р.); «Штучний інтелект у правовій практиці: межі та можливості» (м. Львів, 15 березня 2024 р.); «Проблеми інформаційного забезпечення та розвитку парламентського контролю в контексті Європейської та Євроатлантичної інтеграції України» (м. Київ, 25 квітня 2024 р.); «Україна в умовах соціальної та цифрової трансформації: шляхи до сталого розвитку та повоєнної відбудови» (м. Київ, 22 листопада 2024 р.); «Трансформаційні процеси правотворчої діяльності та парламентського контролю» (м. Київ, 30 жовтня 2025 р.); «Україна в умовах соціальної та цифрової трансформації: теоретичні моделі правового регулювання штучного інтелекту» (м. Київ, 5 листопада 2025 р.).

Публікації. Результати наукового дослідження висвітлено в 30 публікаціях, серед них: 1 розділ в колективній монографії; 13 статей у наукових виданнях, включених до Переліку наукових фахових видань України; 4 – у виданнях, що індексуються в міжнародних наукометричних базах даних Scopus та Web of Science; 2 – у наукових періодичних виданнях інших держав із напрямку, з якого підготовано дисертацію; 10 – тези доповідей на наукових, науково-практичних конференціях, семінарах та засіданнях круглих столів.

Особистий внесок здобувача. Висновки та пропозиції, викладені у дисертації становлять особистий здобуток автора.

У статті «Information security and information hygiene on internet media» (авторський внесок 60 %) з А. Варинською, М. Костицьким, Н. Кушаковою-

Костицькою автором проаналізовано поняття інформаційної безпеки та правові механізми протидії фейковій інформації. У статті з «Use of the “electronic court” service as a means of citizens' access to the judiciary» (авторський внесок 50 %) з Н. Шелевер, М. Янковим, В. Пилип, О. Анталовці здобувачем охарактеризовано основні правові ризики використання штучного інтелекту та цифрових технологій у сфері правосуддя й обґрунтовано необхідність забезпечення балансу між цифровізацією судочинства, захистом прав людини та принципом верховенства права. У статті «The potential and prospects of artificial intelligence use in strategic planning: issues of security and defense» (авторський внесок 45 %) з О. Руденко, І. Рафальським, О. Єрмак, Ю. Конопля дисертантом обґрунтовано необхідність людиноорієнтованого підходу до розроблення та застосування штучного інтелекту в оборонній сфері з урахуванням вимог прозорості, підзвітності та мінімізації правових ризиків. У статті «Digitization of local self-government based on the use of artificial intelligence in the context of sustainable development» (авторський внесок 45 %) з О. Руденко, О. Заїка, І. Кульчій, А. Мирошніченко автором розглянуто можливості використання штучного інтелекту для аналізу даних та підвищення ефективності правоохоронної діяльності за умови забезпечення належного захисту прав людини. У статті «Artificial intelligence in education: tool, object, «subject» of learning» (авторський внесок 80 %) з І. Донніковою та Н. Савіною дисертантом розкрито особливості використання штучного інтелекту у сфері освіти, визначено потенційні ризики його застосування та окреслено механізми правового регулювання. У статті «Electronic means of ensuring fair justice: contemporary and development prospects» (авторський внесок 50 %) з Н. Шелевер, М. Бурдоносовою, О. Рогач, В. Пилип проаналізовано концепцію цифровізації судочинства в сучасних умовах та виокремлено основні групи ризиків використання штучного інтелекту у забезпеченні справедливого правосуддя. У дисертації ідеї та матеріали кандидатської дисертації не використовувалися.

Структура та обсяг дисертації. Структура роботи зумовлена метою та завданнями дослідження і складається зі вступу, чотирьох розділів, що включають 14 підрозділів, висновків до розділів, загальних висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 562 сторінки. Із них основний текст займає 403 сторінки, список використаних джерел (531 найменування) – 64 сторінки, додатки – 73 сторінки.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНО-ПРАВОВОГО ТА АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

1.1. Генеза інформаційно-правового регулювання штучного інтелекту та його співвідношення з Інтернетом речей

Починаючи із другої половини ХХ століття динамічний розвиток інформаційних технологій і визнання інформації стратегічним ресурсом суспільного поступу [300], [91], [122] зумовили становлення нового типу суспільства – інформаційного, характерною ознакою якого Б. Кормич назвав «стрімке зростання всепроникної інформації про всі сторони його життєдіяльності» [122, с. 17]. Закономірним наслідком цих процесів стала трансформація правового регулювання у цій сфері. Як зазначає Л. Коваленко, «новітні реалії в економічному та соціальному житті сучасної епохи призводять до того, що починають складатися нові правові відносини, що дають поштовх до формування галузей права, покликаних стати основою для вирішення складних економічних та соціальних проблем в Україні» [104, с. 175].

Отже, усвідомлення визначальної ролі інформаційного чинника сприяло виокремленню інформаційного права як самостійного напрямку юридичної науки, предметом якого стали суспільні відносини, пов'язані зі створенням, збиранням, обробленням, поширенням, зберіганням та захистом інформації. Теоретичні засади цього напрямку сформовано у працях українських вчених І. В. Арістової [7; 8; 9; 10; 11], О. А. Баранова [17; 18; 19; 20; 21], В. М. Брижка [29; 30; 31], О. Д. Довганя [72; 73], Р. А. Калюжного [91; 92], М. В. Карчевського [94; 95; 96; 97; 98; 99], Л. П. Коваленко [104; 105; 106], І. Ф. Коржа [118; 119; 120], Б. А. Кормича [122; 123], О. А. Костенка [126; 127; 128; 129; 130; 131; 132; 133], С. С. Кудінова [137], В. Г. Пилипчука [175; 176; 177], П. М. Рабіновича [223; 224], Ю. І. Тюрі [252; 253], В. М. Фурашева [262; 263], О. І. Харитонової та Є. О. Харитонova [265; 266; 267] та інших. Їхні

наукові розробки заклали доктринальне підґрунтя сучасного інформаційного права, сформували методологічні засади його розвитку та визначили тенденції подальшої трансформації правового регулювання в умовах інтенсивної цифровізації суспільства.

Аналіз праць зазначених дослідників свідчить, що розбудова будь-якої правової доктрини неможлива без осмислення її базових категорій. У цьому контексті ключового значення для з'ясування еволюції предмета інформаційного права набуває поняття «інформація». Його тлумачення у законодавчому дискурсі відтворює ключові зміни, пов'язані із розвитком інформаційного суспільства. Так, у первісній редакції Закону України «Про інформацію» від 2 жовтня 1992 року інформація визначалася як «документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі» [199]. Натомість у чинній редакції Закону під інформацією розуміють «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [200]. Порівняльний аналіз наведених законодавчих визначень дає підстави стверджувати, що початкова законодавча дефініція була зорієнтована тільки на документування або публічне поширення відомостей, а сучасний законодавчий підхід охоплює будь-які дані та нові (електронні) форми їх існування. Це свідчить про адаптацію інформаційного законодавства до цифрової трансформації суспільних відносин, у яких інформація дедалі частіше існує, обробляється та передається в електронному середовищі. Зміна законодавчого тлумачення інформації відображає не лише розвиток термінології, а й еволюцію самого предмета інформаційно-правового регулювання. Така тенденція, орієнтована на оновлення змісту понять, є методологічно обґрунтованою, оскільки, на думку І. В. Арістової, накопичення нових даних, пов'язаних з інформацією, потребує коригування їх змісту [11, с. 107].

Отже, якщо наприкінці XX століття предметом інформаційно-правового регулювання була інформація як самостійний феномен суспільного життя, то

сьогодні, внаслідок цифровізації та ускладнення архітектури інформаційного суспільства, він закономірно охоплює суспільні відносини, пов'язані з автоматизованим створенням, аналізом, інтерпретацією та генерацією інформації системами штучного інтелекту. У зв'язку з цим інформаційне право вже не обмежується регулюванням інформаційних відносин у традиційному розумінні, а охоплює питання використання алгоритмічних систем, забезпечення людського контролю та захисту прав людини в умовах функціонування інтелектуальних цифрових технологій. Саме тому розвиток систем штучного інтелекту можна розглядати як новий етап еволюції інформаційного права. Цю тенденцію відзначають В. М. Бесчастний, М. В. Костицький та Н. В. Кушакова-Костицька, зазначаючи, що «інформаційне суспільство, орієнтир на створення якого було заявлено на початку ХХІ століття, трансформувалося за останні п'ять років у цифрове, яке принципово відрізняється від нього як за змістом, так і за формою» [27, с. 9]. Така трансформація зумовлена тим, що системи штучного інтелекту перестають бути лише інструментом оброблення інформації та поступово перетворюються на самостійний чинник розвитку цифрового суспільства. На думку В. М. Підгородинського, «цифрові досягнення останніх десятиліть є настільки значущими, що їх розглядають як універсальні, глобальні чинники, від яких залежить буття особистості, держави, соціуму тощо» [178, с. 84].

Зростання автономності та функціональних можливостей цифрових технологій актуалізувало питання визначення меж людського контролю, розподілу юридичної відповідальності між учасниками відповідних правовідносин і формування нових моделей правового регулювання взаємодії людини, суспільства та штучного інтелекту.

За таких умов першочергового значення набуває визначення правової природи штучного інтелекту та його сутнісних характеристик. Як справедливо зазначає М. Р. Карільйо, «юридичний аналіз базується на неформалістичній науковій методології. Це означає, що необхідно розглянути природу та

характеристики III як попередній крок до визначення його правової парадигми» [314].

З цієї точки зору вивчення генези штучного інтелекту як наукової ідеї та технологічного напрямку розвитку є необхідною передумовою формування концептуальних теоретико-методологічних засад його правового регулювання. Саме тому вироблення сучасної моделі правового регулювання штучного інтелекту потребує попереднього з'ясування еволюції доктринальних підходів до його розуміння, технологічних особливостей та співвідношення з Інтернетом речей (IoT).

Витоки концепції штучного інтелекту сягають давніх міфологічних уявлень про створення штучних істот, однак наукового змісту ця ідея набула лише у XX столітті з розвитком кібернетики, математичної логіки та теорії обчислюваності. Наукові розвідки К. Геделя, С. Кліні, Р. Петер, Е. Поста, А. Тюрінга та А. Черча заклали теоретичні засади розвитку досліджень у сфері штучного інтелекту. Попри періоди технологічного сповільнення та переоцінки можливостей, цей напрям розвитку зберіг наступність і сьогодні демонструє практичні результати, що зумовлюють необхідність його комплексного правового осмислення.

Уперше у науковий обіг термін «штучний інтелект» увів професор Дартмутського коледжу Дж. Маккарті, використавши його для позначення експериментів із «навчання» машин, тобто здатності машин до опанування форми, абстракцій і мови. Метою цих досліджень було формування здатності машин до алгоритмічного моделювання когнітивних операцій людини. Запропонована Дж. Маккарті концепція започаткувала обчислювальний підхід до розуміння штучного інтелекту, у межах якого людський інтелект розглядався як сукупність формалізованих операцій, що можуть бути відтворені засобами обчислювальної техніки [436].

У 1960-х роках дослідження у сфері штучного інтелекту набули системного характеру. Важливу роль у їх розвитку відіграла The International Joint Conference on Artificial Intelligence (IJCAI) [461]. На цьому етапі

основними напрямками досліджень були моделювання когнітивних процесів, машинне навчання, оброблення природної мови та взаємодія інтелектуальних систем із зовнішнім середовищем [420].

Подальший розвиток досліджень зумовив поступову трансформацію уявлень про штучний інтелект: від його розуміння в межах обчислювального підходу як системи формальної обробки символів до самотійного міждисциплінарного концепту, що став об'єктом не лише технічного, а й філософського, етичного та соціального осмислення. Водночас на цьому етапі правові виміри штучного інтелекту ще не набули самотійного значення. Основна увага дослідників була зосереджена на оцінці його технологічних можливостей, тоді як питання правового регулювання та потенційних обмежень використання лише починали окреслюватися у критичних оглядах.

Одним із найвідоміших критиків обчислювального підходу до штучного інтелекту був Х. Дрейфус, який довів, що людський розум не функціонує як механізм для формальної обробки символів, оскільки когнітивна діяльність нерозривно пов'язана з тілесністю, практичним досвідом, соціокультурним контекстом та живою взаємодією зі світом [350].

Критика Х. Дрейфуса стала важливим етапом переосмислення природи штучного інтелекту, започаткувавши відхід від його суто технічного розуміння. Поступовий розвиток технологій ШІ та розширення сфер його застосування зумовили перенесення цієї проблематики у площину правових досліджень, що сприяло формуванню методологічних підходів до його правового осмислення. Серед них, на нашу думку, особливе значення мають функціональний, субстанційний та антропоцентричний підходи.

У межах функціонального підходу штучний інтелект розглядається крізь призму виконуваних ним функцій, особливостей використання та правового регулювання. Зокрема, у працях Л. Флоріді штучний інтелект осмислюється як складова інформаційного середовища, значення якої визначається характером її функціонування та впливом на людину і суспільство [379]. В українській правовій доктрині функціональний підхід до осмислення штучного інтелекту

простежується у працях О. А. Баранова, Б. А. Кормича, В.П. Пилипчука, Ю. М. Тюрі та інших вчених, у яких досліджуються правові й інформаційно-аналітичні аспекти використання систем штучного інтелекту.

У межах субстанційного підходу основна увага зосереджується на правовій природі штучного інтелекту, можливості визнання його самостійним суб'єктом права та здатності до самостійної участі у правовідносинах. Предметом наукових дискусій при цьому є питання щодо наявності у систем штучного інтелекту таких ознак, як самосвідомість, автономна воля, моральне агентство та здатність бути носієм суб'єктивних прав і юридичних обов'язків. В українському науково-правовому дискурсі концептуальні засади та критичний аналіз цієї проблематики представлено у дослідженнях О. А. Баранова, тоді як безпосередній розвиток концепцій субстанційної квазісуб'єктності, автономії волі алгоритмів та цивільно- чи кримінально-правових фікцій відображено у працях М. В. Карчевського, О. В. Костенка, К. Г. Некіт, О. Е. Радутного, Є. О. Харитонова, О. І. Харитонові.

У межах антропоцентричного підходу визначальне значення мають питання забезпечення пріоритету прав і свобод людини, людський контроль над функціонуванням систем штучного інтелекту та захист фундаментальних прав у цифровому середовищі. Зазначений підхід знайшов відображення у працях – І. М. Берзелюка, О. С. Гиляки, В. М. Підгородинського, П. М. Рабіновича.

Водночас зазначені підходи не вичерпують методології правового дослідження штучного інтелекту. Вони характеризують насамперед способи осмислення його природи.

Натомість формування ефективної моделі правового регулювання потребує застосування спеціальних регуляторних підходів, серед яких особливого значення набувають ризик-орієнтований та секторальний підходи. Особливості їхнього впровадження та нормативного закріплення в національному правовому полі будуть розглянуті у наступних розділах дослідження.

Аналіз наведених підходів дозволяє дійти висновку, що їх різноманітність зумовлена насамперед різним розумінням природи штучного інтелекту. Як слушно зазначає О. І. Харитонova, «в основі поглядів на штучний інтелект лежить імпліцитне припущення, що термін «інтелект» можна використовувати однаково для позначення як людського інтелекту, так і ШІ. Однак це не охоплює повного обсягу концепції. У випадку людей інтелект – це здатність, яка стосується людини в її повноті, тоді як у контексті штучного інтелекту «інтелект» розуміється функціонально, часто з припущенням, що діяльність, характерна для людського розуму, може бути розбита на оцифровані кроки, які машини можуть відтворити» [265, с. 39]. Саме це протиставлення цілісної людської природи та суто функціонального відтворення мислення машиною пояснює розмежування між антропоцентричним, субстанційним та функціональним векторами наукового пошуку.

Подібний підхід до осмислення взаємозв'язку між людським мисленням і його технологічним моделюванням простежується також у працях інших дослідників. Зокрема, О. В. Павлюк визначає штучний інтелект як «здатність машин і програм аналізувати отриману інформацію, робити висновки та приймати на їх основі рішення» [170, с. 43]. Дослідниця наголошує, що основними характеристиками таких систем є здатність постійно навчатися, накопичувати знання та застосовувати їх на практиці, тобто виконувати окремі функції, притаманні людському мисленню.

Таке уподібнення алгоритмічних процесів когнітивним функціям людини підкреслює складність формування автентичного понятійного апарату для правового регулювання штучного інтелекту без використання антропоморфних аналогій.

Однак у площині правотворчості подібні теоретичні конструкції виявляються недостатніми. На відміну від наукових концепцій, що апелюють до аналогій із людським мисленням, вітчизняний і європейський законодавці спираються на функціонально-технологічні критерії, придатні для нормативного визначення та правозастосування. Так, у вітчизняному

правовому полі першим кроком офіційного нормування стало Розпорядження Кабінету Міністрів України від 02 грудня 2020 року № 1556-р, яким було схвалено Концепцію розвитку штучного інтелекту в Україні. У цьому документі ШІ визначено як «організовану сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань» [215]. Своєю чергою, наднаціональне регулювання зосереджується на юридично значущих характеристиках систем штучного інтелекту, насамперед на рівні їх автономності, адаптивності та здатності формувати результати, які можуть впливати на права, свободи, законні інтереси людини та інші суспільні відносини. Показовим є визначення, закріплене в AI Act, відповідно до якого «штучний інтелект – це машинна система, розроблена для роботи з різними рівнями автономності, яка може демонструвати адаптивність після розгортання та на основі отриманих вхідних даних формувати прогнози, рекомендації чи рішення, що впливають на фізичне або віртуальне середовище» [472].

Узагальнюючи це дефініційне розмаїття, варто погодитися з висновком Є. А. Тимошенко, яка слушно зазначає, що «єдине визначення штучного інтелекту не може претендувати на повне охоплення його рис та ознак, оскільки сама структура та сукупність технологічних особливостей в основі штучного інтелекту передбачає його застосування та дослідження в розрізних напрямках» [248, с. 45].

Отже, різноманітність наведених методологічних підходів відображає неоднорідність самого об'єкта дослідження. З огляду на це вважаємо, що *штучний інтелект доцільно розглядати не як однорідне явище, а як сукупність різних технологічних моделей, що відрізняються за рівнем автономності, функціональним призначенням, способом функціонування та ступенем*

наближення до людських когнітивних здібностей.

Одним із перших кроків до теоретичного осмислення неоднорідності штучного інтелекту стала запропонована Д. Серлем диференціація сильного та слабого штучного інтелекту (strong AI та weak AI) [482].

Така диференціація має принципове значення для правового аналізу, оскільки дає змогу відмежувати гіпотетичні моделі від технологій, що вже функціонують у реальних суспільних відносинах.

На думку Д. Серля, для сильного штучного інтелекту, фізичні особливості реалізації не мають вирішального значення, оскільки визначальною є програма, яка має бути не лише моделлю розуму, а й самостійною системою мислення [482, С. 25]. Натомість слабкий штучний інтелект розглядається як інструмент для моделювання або дослідження окремих когнітивних процесів [71, с. 14].

Однак у сучасних умовах сильний ШІ, як зазначає М. В. Карчевський, залишається гіпотетичною технологією [98, с. 33], тоді як слабкий ШІ набув широкого практичного застосування, орієнтованого на вирішення конкретних завдань і саме тому становить першочерговий об'єкт сучасного правового регулювання.

Розвиваючи ідею класифікації штучного інтелекту, О. А. Баранов виокремлює три основні типи ШІ: слабкий, сильний і штучний суперінтелект [15, с. 21], які кореспондують із сучасною технологічною класифікацією вузького (прикладного) ШІ, загального ШІ та штучного суперінтелекту. Запропонована класифікація підтверджує доцільність диференційованого підходу до правового регулювання штучного інтелекту, оскільки відображає істотні відмінності між окремими типами ШІ за рівнем їх автономності та функціональними можливостями. Проте для комплексного визначення правового режиму сучасних систем штучного інтелекту цього недостатньо, оскільки вони функціонують не ізольовано, а як складові ширшого цифрового середовища, що забезпечує безперервне збирання й оброблення великих масивів даних. У зв'язку з цим виникає необхідність розмежування штучного

інтелекту та Інтернету речей (IoT) [16, С. 7], які, попри тісну технологічну взаємодію, мають різну правову природу, що зумовлює відмінності у підходах до їх правового регулювання.

Таке розмежування є не лише технологічно, але й концептуально обґрунтованим, оскільки IoT формує середовище функціонування інтелектуальних систем і дає змогу конкретизувати об'єкт правового регулювання, коло суб'єктів відповідальності, рівень автономності технологічних систем і межі юридичної відповідальності за наслідки їх функціонування.

Таким чином, паралельно з розвитком штучного інтелекту сформувався окремий технологічний напрям – Інтернет речей (IoT), у межах якого здійснюється інтеграція фізичних об'єктів у цифрове середовище за допомогою електронних пристроїв та інформаційно-комунікаційних технологій. Саме для позначення концепції мережевої взаємодії фізичних об'єктів, здатних автоматично передавати дані без безпосередньої участі людини, британський дослідник К. Ештон у 1999 році увів у науковий обіг термін «Інтернет речей».

У зв'язку з цим об'єкти сфери IoT доцільно розглядати як елементи технологічної інфраструктури цифрового суспільства, а не як самостійних суб'єктів правовідносин, оскільки вони виконують переважно функції збирання, передавання та обміну даними і не здійснюють властивих системам штучного інтелекту функцій аналізу інформації, автономного ухвалення рішень та самостійного виконання інтелектуальних операцій.

На сучасному етапі сама ідея ШІ значною мірою відійшла від окремих вихідних задумів її засновників, оскільки нинішні підходи нерідко зводяться до розуміння ШІ як «будь-якої системи, яка сприймає навколишнє середовище та виконує дії, які максимізують її шанси досягти поставлених цілей» [480, с. 55].

Вважаємо, що для правового дискурсу подібне «розмивання» поняття ШІ до будь-якої ефективної автономної системи є методологічно небезпечним. Якщо в технічній літературі допустимим є широке функціональне тлумачення ШІ як програмного комплексу, здатного автономно оптимізувати процес

досягнення певної мети, то у праві така невизначеність унеможлиблює встановлення адресатів правових норм, меж допустимого використання відповідних технологій та суб'єктів відповідальності. Тому *право потребує не максимально широкої, а правочутливої дефініції, яка дозволяє виокремити системи, здатні істотно впливати на права людини, публічне управління та безпеку.*

З огляду на зазначене у межах цього дослідження *термін штучний інтелект (ШІ) пропонується використовувати не щодо будь-яких «розумних» чи алгоритмізованих систем, а стосовно автономних інтелектуальних систем, які характеризуються здатністю до адаптації або самонавчання та спроможністю впливати на юридично значущі сфери суспільних відносин. У зв'язку з цим у подальшому поняття штучний інтелект вживається як правова категорія, зміст якої визначається не стільки з рівнем людиноподібності системи, скільки зі ступенем її впливу на суспільні відносини та потенціалом породжувати ризики для прав людини, демократії, верховенства права та публічного порядку.*

Науковий і технологічний розвиток штучного інтелекту супроводжувався поступовим переосмисленням його первинної концепції. У прагненні досягти технологічного лідерства поняття ШІ дедалі частіше зводили до автономної системи, здатної отримувати інформацію із зовнішнього середовища, аналізувати її та діяти відповідно до поставленої мети.

У ранньому інтелектуальному дискурсі термін «штучний інтелект» використовувався значно ширше. Представники наукової фантастики, футурології та перші дослідники застосовували для позначення машин, здатних не тільки імітувати, а й відтворювати окремі когнітивні функції людини, зокрема навчання та розв'язання проблем [480, с. 2].

Нині ж штучний інтелект переважно описують із позицій функціональної ефективності та раціональності дій, що зміщує акцент із когнітивної природи інтелекту на практичні результати функціонування систем. Саме тому до систем ШІ нерідко відносять пошукові системи, рекомендаційні алгоритми,

системи оброблення природної мови, безпілотний транспорт, автоматизовані системи прийняття рішень та інші цифрові технології, орієнтовані на виконання спеціалізованих завдань.

Разом із тим розвиток цифрових технологій поступово розмежував окремі напрями їх функціонування. Унаслідок цього частина технологій, які раніше асоціювалися зі штучним інтелектом, нині дедалі частіше розглядається у межах самостійних технологічних напрямів [438], зокрема Інтернету речей (Internet of Things, далі – IoT).

Функціональне визначення штучного інтелекту як системи, здатної сприймати навколишнє середовище та діяти для досягнення поставлених цілей, значною мірою зближує його із технологіями Інтернету речей. Унаслідок цього між ШІ та IoT виникає певна термінологічна невизначеність: одні дослідники ототожнюють ці поняття, тоді як інші розглядають Інтернет речей як окремий технологічний напрям або середовище функціонування систем штучного інтелекту.

Термінологічна невизначеність у розмежуванні ШІ та IoT, на яку вказують вчені, зокрема О. В. Костенко [128, с. 131], істотно ускладнює формування ефективного правового регулювання, оскільки перешкоджає чіткому визначенню предмета регулювання, кола технологій, на які поширюються спеціальні нормативні вимоги, та відповідного правового режиму. У цьому контексті слушною є позиція П. М. Рабіновича, який наголошує на необхідності точності, універсальності та об'єктивності юридичних дефініцій [224]. З огляду на це виникає потреба у системному аналізі понятійного апарату сфери Інтернету речей, що дозволить визначити критерії його відмежування від суміжних інтелектуальних систем.

Аналіз еволюції наукових уявлень про Інтернет речей свідчить, що на початку XXI століття ця технологія сприймалася переважно як футурологічна концепція. Однак стрімке поширення технологій Інтернету речей та ускладнення її функціональних характеристик зумовили формування різних методологічних підходів до її осмислення, що стало підґрунтям для тривалої

наукової дискусії. Узагальнення наукових позицій дає підстави виокремити два основні напрями її розвитку: техніко-технологічний, соціально-філософський та правовий (нормативно-регулятивний).

Соціально-філософське розуміння Інтернету речей акцентує увагу не стільки на його інженерній архітектурі, скільки на трансформації взаємодії людини, речей і цифрового середовища, зокрема, у працях Х. Дрю, Е. Брауна та А. Джиліса [309; 389]. Дослідники описують IoT як сукупність фізичних об'єктів, оснащених датчиками, засобами оброблення даних, програмним забезпеченням та іншими технологіями, що забезпечують їх взаємодію й обмін даними через Інтернет або інші комунікаційні мережі. За такого підходу IoT розглядається не лише як сукупність взаємопов'язаних пристроїв, а як нове інфраструктурне середовище цифрової взаємодії людини, технічних систем та інформаційних потоків.

Попри тісний технологічний взаємозв'язок із системами штучного інтелекту, Інтернет речей виконує іншу функцію. Якщо основним призначенням IoT є забезпечення збирання, передавання та обміну даними між фізичними об'єктами, то штучний інтелект орієнтований на їх аналіз, інтерпретацію, формування висновків та підтримку або автономне ухвалення рішень. Саме функціональна спеціалізація цих технологій зумовлює необхідність їх розмежування як самостійних об'єктів правового регулювання.

Такий підхід узгоджується з позицією О. А. Баранова, який, аналізуючи перспективи розвитку штучного інтелекту, зазначає, що у майбутньому ШІ «буде використовуватися у всіх сферах людської діяльності, в яких спостерігається низька ефективність, яка обумовлена наявністю природної обмеженості когнітивних можливостей людини» [13, с. 33]. Отже, визначальною ознакою штучного інтелекту є не сам факт цифрової взаємодії чи обміну даними, а спрямованість на відтворення окремих когнітивних функцій людини шляхом аналізу інформації, навчання та вироблення рішень.

Таким чином, *Інтернет речей (IoT) забезпечує технологічну інфраструктуру функціонування цифрових систем, тоді як штучний інтелект*

реалізує когнітивну функцію оброблення інформації та вироблення рішень. Саме різне функціональне призначення цих технологій зумовлює їх самостійне значення як об'єктів правового регулювання.

Запропоноване О. А. Барановим визначення Інтернету речей конкретизує його технологічне призначення як сукупності «взаємодіючих технічних систем і комплексів, що складаються з мікропроцесорів, сенсорів, пристроїв, систем передачі даних, локальних та/або розподілених обчислювальних ресурсів і програмних засобів, призначених для реалізації суспільних відносин» [19, с. 100], шляхом використання мережі Інтернет, даних та відповідних програмно-технічних засобів.

Ширше тлумачення пропонує К. Некіт, уточнюючи, що IoT варто розглядати як комплекс відповідних компонентів, які використовуються для задоволення інтересів фізичних і юридичних осіб, а також інтересів держави та суспільства, з урахуванням багатогранності цього поняття та різноманітності сфер застосування [163].

Попри значну кількість запропонованих у науковій та нормативній літературі дефініцій IoT (за окремими оцінками – понад 140) [425], єдиний підхід до розуміння цього явища досі не сформовано. Переважна більшість визначень ґрунтується на технічному підході, який характеризує Інтернет речей як мережу взаємопов'язаних пристроїв, оснащених засобами збирання, передавання й обміну даними через мережу Інтернет [79].

Подібний підхід відображено і в Рекомендації Міжнародного союзу електрозв'язку (ITU) «Overview of the Internet of Things», відповідно до якої IoT визначається як глобальна інфраструктура інформаційного суспільства, що забезпечує надання розширених послуг шляхом взаємодії фізичних і віртуальних об'єктів на основі інформаційно-комунікаційних технологій [407].

Якщо техніко-технологічний напрям зосереджується на архітектурі мереж, протоколах передавання даних і функціонуванні цифрової інфраструктури, а соціально-філософський – на трансформації повсякденного життя, суспільних відносин і цифрової культури, то правовий напрям

формується як відповідь на нові виклики та ризики, породжені розвитком Інтернету речей. У межах цього підходу осмислення Інтернету речей концентрується на трьох взаємопов'язаних напрямках.

По-перше, безперервне й автономне збирання інформації «розумними» пристроями у приватній сфері людини істотно ускладнює застосування традиційних механізмів надання згоди на обробку персональних даних. Це зумовлює перехід від реактивної моделі захисту приватності до концепції *Privacy by Design*, відповідно до якої гарантії захисту прав людини інтегруються безпосередньо в архітектуру цифрових систем ще на етапі їх проектування

По-друге, автономне функціонування IoT-пристроїв у фізичному середовищі (зокрема автономного транспорту, медичних сенсорів чи промислових систем) актуалізує проблему розподілу юридичної відповідальності за шкоду, спричинену їх використанням. У зв'язку з цим одним із ключових завдань правового регулювання стає визначення меж відповідальності розробника програмного забезпечення, виробника обладнання, постачальника цифрових сервісів та користувача.

По-третє, широке поширення Інтернету речей зумовлює інституціоналізацію кібербезпеки як самостійного юридичного обов'язку. Вимоги щодо належного рівня захисту IoT-пристроїв поступово трансформуються із технічних рекомендацій у юридично обов'язкові стандарти, що знаходить відображення у сучасному європейському та національному законодавстві.

Таким чином, узагальнення соціально-філософського, технічного та правового підходів дає підстави розглядати *Інтернет речей* як багаторівневу цифрову інфраструктуру взаємопов'язаних фізичних і віртуальних об'єктів, функціонування якої забезпечується безперервним обміном даними у межах єдиного цифрового середовища. На відміну від систем штучного інтелекту, визначальним функціональним призначенням Інтернету речей є не автономне вироблення рішень, а забезпечення інформаційної взаємодії між фізичними та

цифровими об'єктами шляхом збирання, передавання та обміну даними. Відповідно, юридична специфіка Інтернету речей полягає у регулюванні інформаційної взаємодії між фізичними та цифровими об'єктами, тоді як юридична специфіка штучного інтелекту полягає у регулюванні процесів алгоритмічного формування, оцінювання та використання рішень, здатних впливати на права, свободи й законні інтереси людини.

Масштабне поширення технологій Інтернету речей зумовило формування глобальної цифрової інфраструктури, у межах якої здійснюються безперервне збирання, передавання та обмін значними масивами даних. За даними IoT Analytics, кількість підключених IoT-пристроїв у світі продовжує стабільно зростати і, за прогнозами, до 2030 року може перевищити 40 млрд, що свідчить про стрімкий розвиток цього сектору цифрової економіки. Саме у такому інформаційному середовищі функціонує значна частина сучасних систем штучного інтелекту [405].

На це свого часу звертав увагу О. А. Баранов, який пов'язував розвиток технологій Інтернету речей із необхідністю оброблення великих масивів даних та ухвалення рішень у режимі реального часу. На думку вченого, саме поєднання технологій IoT з алгоритмами штучного інтелекту забезпечує можливість ефективного аналізу інформації та підтримки процесу прийняття рішень [16, с. 7]. Такий підхід ще раз підтверджує, що Інтернет речей і штучний інтелект перебувають у відносинах функціональної взаємодії: IoT забезпечує інформаційну інфраструктуру функціонування цифрових систем, тоді як ШІ реалізує когнітивну функцію аналізу даних і вироблення рішень.

Поряд із перевагами впровадження Інтернету речей зростають і пов'язані з ним ризики, насамперед у сфері інформаційної та кібербезпеки. Саме питання безпеки сьогодні розглядаються як один із визначальних чинників подальшого розвитку IoT та його правового регулювання. Такий підхід узгоджується із положеннями Закону України «Про основні засади забезпечення кібербезпеки України», який розглядає захист інформаційно-комунікаційних систем і

критичної інформаційної інфраструктури як один із пріоритетних напрямів державної політики у сфері кібербезпеки [205].

Особливої актуальності набуває проблема визначення суб'єктів відповідальності за порушення безпеки IoT-систем, оскільки розподіл функцій між виробниками, операторами, власниками та користувачами нерідко ускладнює встановлення особи, відповідальної за наслідки функціонування відповідної цифрової інфраструктури.

Попри високий рівень автоматизації, Інтернет речей зберігає людиноорієнтовану модель функціонування, передбачаючи можливість людського контролю за роботою відповідних систем. Саме ця ознака істотно відрізняє сучасний IoT від автономних моделей штучного інтелекту.

Інфраструктурний характер Інтернету речей визначає специфіку правових ризиків, які супроводжують його функціонування. На відміну від штучного інтелекту, основні виклики IoT пов'язані не з автономним виробленням рішень, а із забезпеченням інформаційної безпеки, кіберзахисту та належним визначенням суб'єктів відповідальності за функціонування відповідної цифрової інфраструктури.

Якщо ризики використання штучного інтелекту пов'язані передусім із когнітивною автономністю систем та їх впливом на права і свободи людини, то ризики Інтернету речей мають переважно інфраструктурний характер і стосуються забезпечення безпеки цифрових мереж, цілісності даних та визначення суб'єктів відповідальності. Така специфіка IoT сформувалася у процесі його технологічної еволюції – від концепції мережевої взаємодії окремих пристроїв до базової цифрової інфраструктури сучасного суспільства.

Первинне розуміння Інтернету речей ґрунтувалося не лише на мережевому з'єднанні фізичних об'єктів, а насамперед на автономізації процесів збирання, передавання та оброблення даних. Подальший розвиток IoT супроводжувався поступовим розширенням сфер його застосування — від окремих мережевих пристроїв до масштабної цифрової інфраструктури, інтегрованої у промисловість, транспорт, енергетику, охорону здоров'я та інші

сфери суспільного життя. Сьогодні IoT дедалі більше розглядається як базова цифрова інфраструктура сучасного суспільства, у межах якої функціонує значна частина інтелектуальних систем.

Розвиток IoT засвідчив перехід від моделі «Інтернету людей» до моделі «Інтернету речей», у якій поряд із взаємодією між людьми дедалі більшого значення набуває автоматизований обмін даними між технічними системами.

Такий перехід має не лише технологічне, а й правове значення, оскільки масове збирання, передавання та оброблення даних у межах цифрової інфраструктури зумовлюють необхідність формування нових підходів до інформаційної безпеки, захисту даних, стандартизації, визначення суб'єктів відповідальності та нормативного контролю.

Стратегічне значення IoT підтверджується його включенням до пріоритетних напрямів цифрового розвитку у провідних країнах світу, а також діяльністю Міжнародного союзу електрозв'язку та Європейського Союзу щодо стандартизації відповідних технологій. Це свідчить про поступове формування міжнародних засад правового й технічного регулювання Інтернету речей.

Становлення Інтернету речей як складової цифрової інфраструктури сучасного суспільства зумовило його активне впровадження у різні сфери суспільного життя, у межах яких формуються нові моделі цифрової взаємодії та автоматизованого управління.

На основі IoT реалізуються численні цифрові рішення, зокрема концепції «розумного міста», інтелектуальні транспортні системи, автоматизовані логістичні комплекси та інші моделі цифрової взаємодії.

Таким чином, Інтернет речей формує цифрове середовище функціонування інтелектуальних систем, однак не є тотожним штучному інтелекту. Окремі елементи IoT можуть використовуватися у системах ШІ, проте самі по собі не наділені когнітивними властивостями, притаманними штучному інтелекту.

Водночас сучасний розвиток штучного інтелекту засвідчує, що його еволюція пов'язана не лише зі зростанням автономності інтелектуальних

систем, а й із формуванням моделей ефективної взаємодії людини й технології, що дістали узагальнену назву гібридного інтелекту [443]. Проте поняття «гібридний інтелект» поки що не набуло усталеного змісту, що зумовлено дискусійністю підходів до розуміння взаємодії людини та штучного інтелекту.

На думку Д. Деллерманна, А. Калми, Н. Ліпуша та Т. Вайгеля Вебера, гібридний інтелект ґрунтується на поєднанні когнітивних можливостей людини та штучного інтелекту з метою досягнення результатів, недосяжних для кожного з них окремо [342]. У зв'язку з цим дискусійним залишається питання, чи можуть моделі взаємодії людини з елементами IoT розглядатися як окремий прояв гібридного інтелекту. Водночас, на нашу думку, взаємодію людини з елементами IoT не слід ототожнювати із самостійними проявами штучного інтелекту, оскільки вирішальна роль в ухваленні рішень у таких моделях належить людині, тоді як технічні компоненти виконують допоміжні функції. Таке розмежування має принципове значення для визначення суб'єктного складу правовідносин і меж юридичної відповідальності.

Дискусії щодо природи гібридного інтелекту безпосередньо пов'язані з різним розумінням самого поняття «інтелект», що зумовлює необхідність звернення до його базового змісту. Інтелект (англ. *intelligence*) походить від латинського *intellectus* і означає здатність навчатися, розуміти, робити судження та формувати обґрунтовані висновки [312]. Значно ширше це поняття трактується у психології, де інтелект визначають як відносно стійку структуру розумових здібностей особистості. Зокрема його пов'язують із системою розумових операцій, когнітивним стилем, стратегіями розв'язання проблем та здатністю адаптуватися до нових умов, з ефективністю індивідуального підходу до ситуації, що вимагає пізнавальної активності, з когнітивним стилем та ін. [311; 445]. У тлумачному словнику української мови інтелект визначено як «розум, здатність людини думати, мислити» [436].

Отже, незалежно від галузі знань, у якій досліджується інтелект, його визначальними ознаками залишаються здатність до сприйняття й аналізу інформації, навчання, формування суджень та ухвалення рішень. Саме ці

характеристики становлять концептуальну основу сучасного розуміння штучного інтелекту, оскільки дають змогу відмежувати його від інших цифрових технологій, що здійснюють лише збирання, передавання чи оброблення даних.

Таким чином, для цілей правового дослідження вирішального значення набуває не загальне розуміння інтелекту як розумової здатності людини, а виокремлення тих когнітивних функцій, які потенційно можуть бути відтворені технічними системами. Саме такий підхід дає змогу перейти від аналізу категорії «інтелект» до осмислення сутності штучного інтелекту як самостійного об'єкта правового регулювання.

Узагальнюючи когнітивні ознаки інтелекту, подібного висновку доходить О. А. Баранов. Дослідник визначає штучний інтелект як «інтелект, що має штучне походження та імітує (моделює) певну сукупність когнітивних функцій, еквівалентних відповідним когнітивним функціям людини» [13, с. 45].

Однією з таких функцій штучного інтелекту є формування та вибір оптимального рішення. На відміну від автоматизованого виконання запрограмованих команд, процес ухвалення рішень передбачає визначення мети, аналіз можливих альтернатив, оцінку їх наслідків та вибір оптимального варіанта відповідно до встановлених критеріїв. Саме така послідовність дій становить зміст сучасної теорії ухвалення рішень [235].

Таким чином, *здатність до ухвалення рішень і здатність виконувати запрограмовані дії є різними функціональними характеристиками цифрових систем*. Виконання алгоритмічних команд властиве як роботизованим пристроям, так і системам Інтернету речей. Наприклад, робот-пилосос оминає перешкоди, дрон здійснює маневрування, а бортовий комп'ютер автомобіля повідомляє про необхідність технічного обслуговування. Проте всі ці системи реалізують наперед визначені алгоритми і не здійснюють самостійного когнітивного аналізу інформації чи вироблення рішень у тому значенні, яке вкладається у поняття штучного інтелекту.

На відміну від систем Інтернету речей, які реалізують наперед визначені

алгоритми, системи штучного інтелекту потенційно здатні не лише формувати рішення на основі аналізу даних, а й реалізовувати їх у процесі взаємодії із зовнішнім середовищем. Зокрема, системи автономного керування транспортними засобами аналізують дорожню ситуацію, прогнозують розвиток подій та обирають подальшу модель поведінки, що наближає їх до окремих форм людської когнітивної діяльності.

У зв'язку з цим визначення штучного інтелекту потребує подальшого уточнення в частині автономної реалізації сформованих рішень. Принципового значення для визначення його функціональної природи та вироблення моделі правового регулювання набуває питання, чи охоплює штучний інтелект лише процес вироблення рішень, чи також їх автономну реалізацію.

Сучасне розуміння штучного інтелекту (ШІ) поступово виходить за межі суто технічного моделювання когнітивних функцій людини й охоплює питання автономності функціонування відповідних систем. Міждисциплінарна природа цього феномена зумовлює різні підходи до його розуміння: у біології ШІ пов'язують із вищою нервовою діяльністю, у філософії – з проблемами свідомості та етики, у сфері інформаційних технологій – з обробкою даних [308]. Саме таке розширення змісту поняття та його складність зумовили відсутність єдиного підходу до дефініції як у науковій доктрині, так і в правотворчій практиці. Попри стрімкий розвиток технологій, універсального визначення штучного інтелекту досі не вироблено.

Відсутність універсального визначення штучного інтелекту не перешкодила формуванню перших підходів до його правового регулювання. На початковому етапі вони були зосереджені переважно на виробленні етичних принципів використання автономних систем, а не на нормативному визначенні самого поняття ШІ.

Розуміння сутнісних відмінностей між ШІ та Інтернетом речей дозволяє глибше проаналізувати генезу їх нормативного регулювання, де початковий фокус зміщувався від контролю за фізичними об'єктами до правового регулювання автономних інтелектуальних систем. Одним із перших кроків на

цьому шляху стало розроблення у Південній Кореї «Етичного статуту роботів» (2007) [475]. Цей документ охопив увесь життєвий цикл робототехнічних систем – від проектування до утилізації. У Статуті закріплено п'ять ключових принципів: безпеку, надійність, етичність, правову відповідальність розробників і виробників, а також автономність роботів за умови обов'язкового людського контролю. Окрему увагу приділено захисту персональних даних та протидії зловживанню технологіями, зокрема у військовій сфері. Закладені у Статуті етичні принципи стали підґрунтям для подальшого розвитку корейського законодавства, яке еволюціонувало від регулювання робототехнічних систем до спеціального правового регулювання технологій штучного інтелекту. Сучасний етап цієї еволюції відображено у Рамковому законі про розвиток штучного інтелекту та встановлення довіри. У пункті 1 статті 2 цього Закону закріплено дефініцію ШІ як «електронної реалізації людських інтелектуальних здібностей, таких як навчання, міркування, сприйняття, судження та розуміння мови» [367]. Таке визначення чітко відокремлює ШІ від систем IoT, оскільки акцентує увагу саме на когнітивних функціях (навчанні та судженні), а не на процесах збирання чи передавання даних.

Міжнародний досвід свідчить, що на початковому етапі нормативне осмислення відповідних технологій було зосереджене на безпеці матеріальних носіїв ШІ. Зокрема, у «Новій стратегії роботів» Японії (2015) [456] пріоритетами визначено безпечне впровадження робототехніки нового покоління та її адаптацію до потреб суспільства.

Логічним продовженням цієї тенденції стала «Дорожня карта робототехніки США» (2016) [297]. Її положення відображають новий етап розвитку технологічної парадигми, у межах якої робототехніка, Інтернет речей та технології штучного інтелекту розглядаються як взаємопов'язані складові єдиної цифрової екосистеми. Документ визначає пріоритетні напрями розвитку робототехніки, серед яких особливу увагу приділено безпечній взаємодії людини й робота, інтеграції роботизованих систем з інфраструктурою IoT,

розвитку ко-роботів (cobots), а також широкому впровадженню сервісної робототехніки у медицині, сільському господарстві та логістиці. Аналіз положень Дорожньої карти дає підстави зробити висновок, що IoT у цій моделі виконує переважно функцію інфраструктури збору та передавання даних, тоді як штучний інтелект забезпечує їх інтелектуальну обробку та підтримку ухвалення рішень.

Паралельно з формуванням державного бачення розвитку робототехнічних технологій доктринальне осмислення ШІ було спрямоване на його систематизацію та класифікацію. Однією з найбільш відомих стала класифікація, запропонована у 2016 році американським дослідником А. Хінце, який виокремив чотири типи ШІ [396], зокрема реактивні машини (Reactive Machines), що реагують лише на поточний стан без використання попереднього досвіду; системи з обмеженою пам'яттю (Limited Memory), здатні накопичувати інформацію та навчатися на основі попередніх даних; системи з теорією розуму (Theory of Mind), які потенційно можуть розпізнавати емоції, наміри та психічні стани людини; самосвідомий штучний інтелект (Self-aware AI), наділений власною самосвідомістю [396].

Водночас А. Хінце наголошує, що на сучасному етапі розвитку технологій реально існують лише перші два типи систем, тоді як системи з теорією розуму та самосвідомий штучний інтелект залишаються теоретичними моделями. Такий стан розвитку технологій значною мірою зумовив прагматичний підхід до нормативного визначення штучного інтелекту у США. Попри закріплення базової дефініції ШІ у розділі 15 U.S.C. § 9401 (Definitions) у Законі про Національну ініціативу у сфері штучного інтелекту (2020) [454], який визначає його як керовану машиною систему, здатну формувати прогнози, рекомендації або ухвалювати рішення, у країні тривалий час не існувало єдиного кодифікованого правового регулювання. Натомість Сполучені Штати сформували децентралізовану модель, у межах якої правове регулювання здійснюється через виконавчі акти Президента, відомчі рекомендації та нормативні акти окремих штатів.

Показовим прикладом такого підходу є законодавство Каліфорнії № 331 (AB 331), у якому штучний інтелект визначається як система машинного навчання, здатна на основі визначених людиною цілей формувати прогнози, рекомендації або рішення [313]. Такий підхід свідчить, що американський законодавець зосереджується на регулюванні функціональних можливостей реально існуючих систем штучного інтелекту, не поширюючи нормативне визначення на гіпотетичні форми, пов'язані із самосвідомістю чи іншими вищими когнітивними характеристиками.

Важливим етапом розвитку американської політики у сфері штучного інтелекту стало оприлюднення у 2022 році «Плану Білля про права штучного інтелекту» (Blueprint for an AI Bill of Rights) [304], Цей документ запропонував концептуальні засади оцінювання автоматизованих систем, що мають значний вплив на життєдіяльність суспільства.

Попри важливе значення для формування засад відповідального використання штучного інтелекту, Blueprint for an AI Bill of Rights має рекомендаційний характер і не встановлює нормативного визначення ШІ. Це ще раз підтверджує особливість американської моделі, у межах якої акцент зміщується з уніфікації понятійного апарату на формування принципів безпечного, прозорого та людиноцентричного застосування інтелектуальних систем.

Нову сторінку в інституційному осмисленні штучного інтелекту відкрило оприлюднення Китаєм у 2018 році «Білої книги зі стандартизації штучного інтелекту», у якій запропоновано комплексну систему стандартизації ШІ. На відміну від американського підходу, орієнтованого переважно на функціональне визначення та принципи використання інтелектуальних систем, китайська модель розглядає штучний інтелект як багаторівневу інформаційну систему, інтегровану в загальну цифрову інфраструктуру. В основу моделі покладено два взаємопов'язані виміри: «інтелектуальний інформаційний ланцюг», що охоплює процес переходу від даних до інформації, знань, інтелектуального прийняття рішень і виконання, та «ланцюг створення цінності

ІТ», який відображає місце ІІІ у структурі цифрової інфраструктури – від базових технологій до промислової екосистеми [291]. При цьому безпека, конфіденційність, етика та управління визначаються як невід'ємні структурні компоненти системи штучного інтелекту.

Такий підхід має важливе методологічне значення, оскільки демонструє, що Інтернет речей не ототожнюється зі штучним інтелектом, а розглядається як інфраструктурне середовище його функціонування. Водночас сам ІІІ постає центральною ланкою цифрової екосистеми, яка забезпечує інтелектуальну обробку даних, формування рішень та координацію взаємодії її компонентів.

На відміну від китайського підходу, зорієнтованого на концептуальне моделювання архітектури ІІІ, у європейських країнах у цей період пріоритетного розвитку набули моделі секторального правового регулювання окремих видів автономних систем. Однією з перших стала Естонія, яка у 2017 році врегулювала використання роботів-кур'єрів для доставки товарів і поштових відправлень. Того ж року Німеччина внесла зміни до Закону про дорожній рух (Straßenverkehrsgesetz), дозволивши експлуатацію транспортних засобів із частково або повністю автоматизованими функціями керування за умови збереження можливості контролю та своєчасного втручання людини-водія. Одночасно було встановлено базові вимоги до таких систем, зокрема щодо дотримання правил дорожнього руху, розпізнавання ситуацій, у яких керування має бути передано людині, та своєчасного інформування водія про необхідність такої передачі. Аналогічні підходи до секторального регулювання автономних систем поступово почали впроваджувати й інші держави, зокрема Данія та Канада [459].

Підґрунтя для формування спільної європейської моделі правового регулювання штучного інтелекту було закладено Резолюцією Європейського парламенту 2015/2103(INL) [370], у якій уперше запропоновано концептуальні підходи до правового регулювання автономних роботизованих систем.

У Резолюції автономні роботизовані системи характеризувалися через такі ознаки, як автономність, здатність до навчання, адаптивність та відсутність

біологічної природи. Виокремлення здатності до навчання й адаптивності стало принципово новим підходом, оскільки дало змогу відійти від сприйняття робіт як статичних елементів інфраструктури Інтернету речей і заклало підґрунтя для індивідуалізованої оцінки автономних систем залежно від їхніх функціональних характеристик.

Подальшим етапом розвитку європейського підходу стало ухвалення у 2024 р. AI Act (Regulation (EU) 2024/1689), яким запроваджено класифікацію систем ШІ залежно від рівня ризику їх застосування, без встановлення універсального визначення цього поняття.

Україна також поступово долучилася до формування сучасної моделі правового регулювання штучного інтелекту. Важливими етапами стали схвалення у 2020 році Концепції розвитку штучного інтелекту в Україні [215], затвердження Плану заходів з її реалізації [195], а також подальша адаптація національної політики до європейських підходів, зокрема шляхом оприлюднення у 2024 році Білої книги з регулювання штучного інтелекту на сайті Міністерство цифрової трансформації України [152]. Ці документи засвідчили поступовий перехід від загального визначення пріоритетів розвитку технологій до формування ризикоорієнтованої моделі правового регулювання, гармонізованої із сучасними підходами Європейського Союзу.

Таким чином, аналіз нормативних актів, програмних документів та наукових доктрин свідчить, що наприкінці XX – у першій чверті XXI століття сформувався новий напрям розвитку інформаційного права, пов'язаний із правовим регулюванням цифрових технологій. Його характерною особливістю став перехід від пошуку універсального визначення штучного інтелекту до вироблення диференційованих моделей правового регулювання, заснованих на функціональному призначенні технологій, рівні їхньої автономності, сфері застосування та потенційних ризиках.

Важливим концептуальним здобутком цього етапу стало розмежування штучного інтелекту та Інтернету речей як самостійних об'єктів правового регулювання. Якщо Інтернет речей забезпечує інфраструктуру збору,

передавання й обміну даними, то штучний інтелект здійснює їх інтелектуальну обробку, формує рішення та забезпечує їх реалізацію. Саме ця функціональна відмінність зумовлює необхідність формування для зазначених технологій диференційованих правових режимів.

Водночас сучасні технічні, філософські та правові підходи переважно зосереджені на визначенні юридичної природи цих технологій, залишаючи відкритими питання їх аксіологічних засад і допустимих меж використання. У зв'язку з цим наступний етап дослідження потребує звернення до аксіологічного виміру використання штучного інтелекту.

1.2. Аксіологічний вимір використання штучного інтелекту

Інтеграція автономних систем ухвалення рішень, тотальна алгоритмізація архітектоники соціальних практик та поступове делегування сутнісних функцій людського суб'єкта до систем штучного інтелекту генерують системні виклики для правопорядку, етичного дискурсу й архітектури безпеки. Зазначене зумовлює необхідність їх рефлексії у фундаментальній аксіологічній площині.

На рівні сучасного доктринального осмислення етики ШІ дедалі більшого методологічного значення набуває концепція ціннісно-чутливого проєктування (Value Sensitive Design), обґрунтована у працях Б. Фрідман, Д. Г. Гендрі та А. Борнінга, яка передбачає інтеграцію гуманістичних принципів у технічний дизайн інформаційних систем [383, с. 63]. Це зумовлює переосмислення утилітарних підходів: прагматична ефективність технологій втрачає статус самодостатнього критерію та підпорядковується вимогам захисту фундаментальних прав і свобод людини [382].

У межах зазначеної парадигми автономні системи не розглядаються як аксіологічно нейтральні, оскільки їх функціонування зумовлюється нормативно-ціннісними установками, закладеними на етапі розроблення. Досліджуючи цей феномен, Б. Верхей [522] наголошує на контекстуальній та нормативній релятивності рішень ШІ, обґрунтовуючи, що одна й та сама

модель алгоритмічної поведінки може отримувати різну оцінку залежно від соціокультурного контексту та аксіологічної системи, яка лежить в основі її функціонування.

Зазначений підхід має принципове значення для правового регулювання штучного інтелекту, оскільки передбачає оцінку автономних систем не лише за критеріями технічної ефективності, а й з позицій відповідності фундаментальним правам і цінностям. За таких умов прозорість, експлікативність і контрольованість алгоритмічних рішень постають не лише технічними вимогами, а й фундаментальними аксіолого-правовими категоріями.

У сучасних реаліях автономні системи ШІ здійснюють не просто лінійний алгоритмічний вибір, а опосередковану аксіологічну ієрархізацію альтернативних рішень. Це актуалізує проблему визначення етичних, соціальних та правових засад, що мають становити онтологічну основу функціонування інтелектуальних агентів. Як наслідок, сучасні парадигми нормативного та етичного регулювання ШІ дедалі частіше апелюють до людиноцентричних принципів. Репрезентативним вираженням цієї тенденції є «Етичні настанови щодо надійного штучного інтелекту» («Ethical Guidelines for Trustworthy AI») [358], розроблені Експертною групою Європейської Комісії. Концептуальну основу цього документа формують принципи поваги до людської автономії, запобігання заподіяння шкоди, справедливості та зрозумілості алгоритмічних процесів. Фактично йдеться про адаптацію класичних гуманістичних та правових цінностей до умов функціонування високотехнологічного середовища й автономних систем ухвалення рішень.

Оскільки проблематика штучного інтелекту дедалі більше виходить за межі суто інженерного чи технічного дискурсу та стосується питань людської гідності, свободи волі, приватності, справедливості, відповідальності й меж допустимого втручання технологій у суспільне життя, саме система суспільних цінностей визначає критерії допустимого використання штучного інтелекту та

формує аксіологічне підґрунтя для подальшого правового регулювання його застосування.

У цьому контексті особливого значення набуває концепція «етики відповідальності» Г. Йонаса, який наголошував, що технологічний прогрес настільки розширив масштаби людського впливу, що традиційна етика вже не здатна повною мірою охопити наслідки людської діяльності, а тому розвиток новітніх технологій потребує формування нових підходів до відповідальності, безпеки та обмеження ризиків [414].

Показово, що навіть у преамбулі Резолюції Європейського парламенту від 16 лютого 2017 року з рекомендаціями Комісії з норм цивільного права у сфері робототехніки зазначено, що людство стоїть на порозі ери, у якій все більш складні роботи, боти, андроїди та інші прояви штучного інтелекту здатні започаткувати нову промислову революцію, що, ймовірно, не залишить жодної сфери суспільного життя недоторканою, а тому законодавча влада має враховувати як правові, так і етичні наслідки такого технологічного розвитку [370].

Такий образний виклад у документах Європейського парламенту не є випадковим, оскільки у світі триває інтенсивна конкуренція у сфері розроблення і впровадження ШІ, яка «нагадує гонку за освоєння космосу в попередньому сторіччі» [50, с. 66]. З огляду на це експерти у сфері ШІ, цифрової безпеки, етики технологій та їх правового впорядкування дедалі частіше акцентують увагу на ризиках, пов'язаних із втратою належного людського контролю над автономними системами, потенційним обмеженням прав людини та трансформацією базових суспільних цінностей, а також наголошують на необхідності міжнародного унормування використання ШІ. Зокрема, Й. Бенжіо зазначає, що сучасна конкуренція у цій сфері створює ризик втрати належного людського контролю над автономними системами, у зв'язку з чим потребує міжнародної координації та встановлення чітких «червоних ліній» [303] задля недопущення неприйнятних ризиків для людини і суспільства.

Подібне поєднання високих очікувань та суспільних пересторог щодо розвитку ШІ характерне і для сучасного міжнародного дискурсу. Так, Е. Горвіц зазначає, що «нещодавні досягнення в галузі штучного інтелекту викликають як подив, так і тривогу» [391], оскільки значний трансформаційний потенціал автономних систем одночасно поєднується з ризиками та викликами, які потребують відповідального підходу до їх розроблення і впровадження. У цьому аспекті особливого значення набувають концепції відповідального та надійного ШІ, спрямовані на забезпечення безпечного, підконтрольного та людиноцентричного розвитку автономних технологій.

Такі тенденції простежуються і в сучасному міжнародному політико-правовому дискурсі та підтверджуються результатами соціологічних і міждисциплінарних досліджень. Соціологічні служби, зокрема при великих технологічних та ІТ-компаніях, здійснюють дослідження рівня суспільної стурбованості щодо впровадження цифрових технологій і систем ШІ [319], тоді як дослідницькі центри та аналітичні лабораторії оцінюють потенційні ризики їх використання [496]. Водночас представники академічних та експертних кіл у сфері безпеки, права та етики технологій дедалі частіше акцентують увагу на викликах неконтрольованого розвитку штучного суперінтелекту [299], загрозах його використання у деструктивних цілях, а також необхідності превентивного нормативного врегулювання ШІ задля забезпечення належного захисту прав людини, безпеки та базових суспільних цінностей [460; 466; 129; 267].

Плюралізм філософських, футурологічних та правових підходів до осмислення феномену штучного інтелекту унаочнює проблему не лише його дефінітивного визначення, а й формування адекватного методологічного інструментарію для його дослідження. Тривалий час вагомим чинником суспільного сприйняття ШІ залишався науково-фантастичний дискурс, у межах якого автономні системи репрезентувалися у двох протилежних вимірах: або як техноутопічний символ вдосконалення людини, або як джерело екзистенційних загроз і втрати людського контролю.

Як наслідок, сучасне суспільне сприйняття ШІ характеризується

глибокою амбівалентністю – від технооптимістичних очікувань соціального прогресу до побоювань щодо потенційної втрати людиною онтологічної автономії, суб'єктності та монополії на ухвалення рішень. М. Бенасаяг, аналізуючи цей феномен крізь призму сучасних метанаративів, обґрунтовано доводить, що трансгуманістичні концепції нерідко сприяють некритичному сприйняттю новітніх технологій та формуванню уявлення про їхню апріорну когнітивну перевагу над людиною [300].

Водночас, альтернативний вектор наукового дискурсу розглядає розвиток ШІ як прояв суспільного прагнення до інноваційного розвитку [22]. Згідно з цією неогуманістичною парадигмою, ШІ сам по собі не становить іманентної загрози для суверенності людської особистості за умови чіткого нормативно-правового визначення меж його втручання. Автономія та свобода людини не втрачають свого визначального значення, якщо «незалежність людської особистості та її свобода не наражаються на неминучу небезпеку через розвиток штучного інтелекту – за умови, однак, що ми залишимося пильними перед вторгненням технологій у приватне життя» [386].

У межах цього дослідження *штучний інтелект розглядається* не крізь призму гіпотетичних футурологічних припущень щодо можливості чи неможливості створення «надлюдського» інтелекту, а насамперед у *контексті його впливу на систему соціокультурних цінностей та моделі правового регулювання відповідних суспільних відносин*. Зазначений методологічний підхід зумовлений тим, що універсальні загальнолюдські цінності становлять аксіологічний фундамент правопорядку [171] й визначають межі допустимого втручання технологій у сферу суверенних прав і свобод людини.

У контексті цивілізаційного розвитку простежується концептуальне розходження між гуманістичною і трансгуманістичною правовими парадигмами. Якщо класичний гуманістичний підхід ґрунтується на пріоритетності людської гідності, автономії особистості та збереженні контролю людини над технологіями, то радикальні трансгуманістичні концепції легітимізують поступове розширення меж біотехнологічного й

цифрового втручання у природу людини, допускаючи прогресуючий трансфер окремих її екзистенційних функцій до автономних агентів.

З огляду на це, у сучасному доктринальному дискурсі дедалі більшого значення набуває формування ціннісно-правових меж розвитку та використання ШІ, спрямованого на мінімізацію системних ризиків, зумовлених неконтрольованою еволюцією автономних технологій.

Важливою концептуальною ознакою такого підходу є певне зближення етичних і правових аспектів функціонування автономних систем. У зв'язку з цим, як зазначає М.-Р. Каррільйо, етичні та правові підходи до регулювання ШІ нерідко змішуються, хоча вони мають різну природу та різні механізми впливу [314]. Водночас і етика, і право формують моделі суспільної поведінки, що стає особливо актуальним в умовах інтенсифікації алгоритмічного ухвалення рішень.

У правовому вимірі це означає, що правовий контекст не обмежується концептуальною чи формальною системою норм, а визначається соціальними цілями та соціальними наслідками. Саме тому в умовах цифровізації система правових норм повинна залишатися зрозумілою для безпосередніх суб'єктів правовідносин, а акти її реалізації – належним чином обґрунтованими, виправданими та легітимними. З огляду на це ефективність правового регулювання ШІ значною мірою залежить від того, наскільки відповідні норми узгоджуються із суспільними ціннісними уявленнями про справедливість, безпеку, допустимість та межі використання автономних систем.

У цьому контексті важливим є суспільне сприйняття автономних технологій. На сучасному етапі розвитку технологій оцінки потенційних небезпек використання ШІ залишаються доволі варіативними – від прогнозування локальних негативних наслідків до сценаріїв глобальних цивілізаційних ризиків. Так, аналізуючи узагальнені побоювання щодо поширення штучного інтелекту, Ж.-Г. Ганасія виокремлює низку ризиків, пов'язаних із перспективами розвитку та використання систем ШІ, зокрема:

- 1) скорочення потреби у людській праці внаслідок заміщення окремих

професій і видів діяльності автоматизованими системами;

2) ризики для автономії людини, а також для забезпечення її свободи, приватності та безпеки;

3) побоювання щодо можливого домінування «розумних машин» над людиною та втрати людством контролю над автономними системами [386].

Окреслені ризики демонструють етичну складність поєднання потреби у стимулюванні розвитку ШІ з необхідністю встановлення правових меж його використання. Відтак йдеться не про заперечення технологічного розвитку як такого, а про необхідність визначення меж допустимого використання автономних систем залежно від потенційного впливу на права людини, безпеку та систему суспільних цінностей.

Водночас останніми роками зростає кількість застережень з боку практиків, науковців та експертів щодо ризиків нерегульованого використання ШІ в окремих сферах суспільного життя. Насамперед це стосується збирання та обробки персональних даних, використання технологій розпізнавання обличчя, функціонування безпілотних літальних і морських систем, а також застосування автономних технологій у військовій сфері [298].

Одну з причин пересторог щодо використання ШІ у зв'язку з відсутністю у нього морально-етичної складової, яка апріорі не входить до природи автономних систем, В. Еверс пояснює тим, що сучасні технології лише відтворюють або вдосконалюють окремі функції людського інтелекту, не охоплюючи всієї складності людського досвіду, морального вибору та багатоманітності соціальних взаємодій [371]. Саме це, на його думку, є однією з ключових перепон для повної інтеграції людини та штучного інтелекту.

Оскільки правові системи сучасних держав розвиваються у напрямі посилення гуманістичних тенденцій, реалізації принципу соціальної справедливості, а також поглиблення процесів демократизації та глобалізації [78, с. 284], право як основний регулятор суспільних відносин виступає носієм відповідних ціннісних орієнтирів. У зв'язку із цим одним із ключових завдань права є забезпечення гуманістичної парадигми в усіх сферах суспільного

розвитку, у тому числі й у сфері використання технологій штучного інтелекту.

Разом з тим відсутність належного правового врегулювання окремих суспільних відносин, пов'язаних із використанням ІІІ, створює ризики порушення принципу соціальної справедливості. У цьому контексті слушною є позиція М. І. Іншина та В. І. Щербини, які звертають увагу на тенденцію до «вимивання соціальної справедливості» з права [89, с. 237]. Повною мірою це стосується і відсутності належних обмежень щодо використання ІІІ у певних сферах суспільного життя або за окремими критеріями допустимості його застосування.

Не менш важливим чинником є і стрімкість розвитку цифрових технологій, які нерідко випереджають міжнародне та національне нормотворення, швидко інтегруючись у суспільні відносини завдяки своїй функціональності, доступності та практичній ефективності. Така ситуація зумовлена тим, що більшість стратегічних міжнародних актів, які впливають на тенденції розвитку технологій, орієнтована переважно на підтримку інновацій і цифрову трансформацію суспільства.

Зокрема, подібний підхід відображено у п. 2 преамбули Окінавської хартії глобального інформаційного суспільства. У ній зазначено, що інформаційно-комунікаційні технології мають сприяти економічним та соціальним змінам завдяки здатності допомагати людям використовувати знання та ідеї [458].

Водночас у розділі 1 цього документа революційний вплив інформаційно-комунікаційних технологій названо одним із ключових чинників формування сучасного суспільства, тоді як у розділі 2 наголошено на необхідності спрямувати цей вплив на сталий економічний розвиток, суспільний добробут, соціальну злагоду, зміцнення демократії, прозоре управління, захист прав людини, культурне різноманіття та підтримання міжнародного миру й стабільності [458].

Такий стимулювальний підхід до розвитку інформаційних технологій простежується і в інших міжнародних актах щодо інформаційного суспільства (Декларація принципів Організації об'єднаних націй «Побудова

інформаційного суспільства – глобальна задача у новому тисячолітті» [195]). Починаючи з періоду становлення, це, відповідно, було відображено й в національному законодавстві багатьох держав, зокрема України: Постанова Верховної Ради України «Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні» [210], Постанова Кабінету Міністрів України «Про запровадження Національної системи індикаторів розвитку інформаційного суспільства» [193], Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [206], Постанова Верховної Ради України «Про Рекомендації парламентських слухань на тему: «Стратегія інноваційного розвитку України на 2010–2020 роки в умовах глобалізаційних викликів» [211], а також у сучасних документах – Про схвалення Стратегії розвитку штучного інтелекту в Україні на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2026–2028 роках : проєкт розпорядження Кабінету Міністрів України [216], Про схвалення Концепції розвитку електронної охорони здоров'я : розпорядження Кабінету Міністрів України від 28 груд. 2020 р. № 1671-р. [214]. Про схвалення Концепції Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року : розпорядження Кабінету Міністрів України від 13 квіт. 2024 р. № 320-р. [213].

Утім, паралельно з підтримкою інновацій дедалі гостріше постає питання правових меж використання ШІ. Водночас окремі розробники та представники технологічного сектору наголошують, що на сучасному етапі розвитку штучного інтелекту значна частина потенційних загроз є суто прогностичними, оскільки автономні системи все ще перебувають на ранніх стадіях розвитку.

Разом із тим у суспільстві дедалі більше занепокоєння викликає не стільки сам факт існування систем ШІ, скільки тенденція до передавання їм функцій прийняття рішень у сферах, пов'язаних із безпекою, правами людини та суспільно значущими процесами, що у разі недосконалості або непрозорості таких систем може призводити до суттєвих негативних наслідків.

Через складність прогнозування наслідків розвитку ШІ це питання дедалі частіше стає предметом обговорення не тільки у науковому, а й в суспільному дискурсі. Так, за метафоричним висловом С. Гокінга, успіх у створенні повноцінного штучного інтелекту може виявитися як найбільшою подією в історії цивілізації, так і найбільшою загрозою для неї[419].

Подібні перестороги висловлюють і представники технологічного сектору. Вони звертають увагу на складність прогнозування рівня майбутніх можливостей автономних систем та потенційних наслідків їх використання. Зокрема, І. Маск неодноразово наголошував на необхідності обережного підходу до розвитку ШІ та збереження належного людського контролю над такими системами[390].

У цьому контексті особливого значення набуває проблема делегування системам ШІ функцій прийняття рішень у сферах безпеки, управління, оборони, обробки персональних даних та інших суспільно значущих процесів. За таких умов визначального значення набуває питання, чи здатні автономні системи враховувати морально-етичні критерії, які лежать в основі людського прийняття рішень. Саме відсутність у ШІ такої складової розглядається багатьма дослідниками як один із ключових викликів його інтеграції у суспільні відносини.

У зв'язку із цим у сучасному науковому та політико-правовому дискурсі дедалі частіше порушується питання про те, що встановлення правових меж використання ШІ є не менш важливим завданням, ніж стимулювання його подальшого технологічного розвитку.

Згідно з Рекомендаціями експертної групи ЄС щодо ШІ (AI HLEG), він повинен бути: «(1) законний – з дотриманням усіх чинних законів і правил; (2) етичний – повага до етичних принципів і цінностей; (3) надійним – як з технічної точки зору, так і з урахуванням соціального середовища» [358].

Водночас розвиток цифрових технологій уже сьогодні демонструє тенденцію до поступового розширення можливостей автоматизованих систем щодо аналізу поведінки людини, її звичок, уподобань, переміщень та

комунікативної активності. Сучасні цифрові сервіси, системи персоналізованих рекомендацій, технології «розумного будинку», автономні транспортні системи та інші елементи цифрового середовища здатні накопичувати значні масиви поведінкових даних користувачів, аналізувати їх та формувати моделі прогнозування людської поведінки [310].

У цьому контексті особливого значення набуває проблема впливу технологічних систем на формування цифрової залежності та поведінкової моделі людини. Зокрема, К. Мей звертає увагу на зростання комунікативної залежності людини в умовах розвитку інформаційного суспільства та цифрових технологій [444, с. 124].

За умов накопичення великих масивів даних (Big Data) та розвитку аналітичних можливостей автономних систем потенціал впливу ШІ на поведінкові моделі, інформаційні пріоритети та процеси прийняття рішень людиною суттєво зростає. Саме тому питання прозорості, підконтрольності та правових меж використання таких технологій набувають не лише технічного, але й аксіологічного значення.

Сьогодні дедалі більше уваги правників та дослідників привертає проблема маніпулятивного впливу на свідомість людини в умовах розвитку інформаційного суспільства та цифрових технологій [167; 65]. Попри те, що питання юридичної відповідальності за подібні форми впливу залишається недостатньо врегульованим, протягом останніх десятиліть у науковому дискурсі активно обговорюється необхідність формування відповідних правових механізмів протидії таким практикам. Приміром, Н. Савінова у своїх дослідженнях, звертає увагу на небезпеку безкарності умисного впливу на свідомість людини в умовах розвитку інформаційного суспільства, а також на ризики формування поведінкових девіацій під впливом сучасних інформаційних технологій [230].

З огляду на зазначені загрози, особливого значення як механізму забезпечення безпечного розвитку технологій набуває право. Як зазначає О. Радзивілл, в умовах девальвації моральних імперативів у цифровому

суспільстві саме право покликане забезпечити його безпечний розвиток [226]. Такий підхід вимагає створення умов, за яких нівелюються як очевидні небезпеки для подальшого існування індивіда, так і причини, що спонукають до дій, здатних генерувати подібні загрози.

Показовою у цьому контексті є еволюція підходів до регулювання штучного інтелекту у транснаціональних корпораціях, зокрема на прикладі компанії Bosch [76]. Сформульовані компанією у 2020 році антропоцентричні етичні принципи – безпека, надійність, прозорість і обов'язковий людський контроль, реалізований через моделі *human-in-the-loop*, *human-on-the-loop* та *human-in-command*, – відображали ціннісний консенсус щодо недопустимості автономізації ШІ на шкоду людині. Подальший розвиток міжнародного та європейського правового регулювання засвідчив поступовий перехід від корпоративних етичних стандартів до юридично обов'язкових вимог. Зокрема, закладені у зазначених підходах принципи знайшли нормативне відображення у Регламенті (ЄС) 2024/1689 (AI Act), який закріпив обов'язковість людського нагляду, прозорості та управління ризиками під час використання високоризикових систем штучного інтелекту.

На тлі стрімкого розвитку генеративних систем штучного інтелекту проблема подолання морально-етичних і безпекових обмежень їх функціонування залишається однією з ключових для розробників автономних технологій, поступово виходячи за межі суто технічної проблематики та набуваючи значення аксіолого-правового виклику.

На початковому етапі розвитку таких систем, зокрема у матеріалах Швейцарської вищої технічної школи Цюріха (ETH Zürich), ChatGPT характеризувався як нейронна мережа, здатна генерувати тексти, максимально наближені до природного людського мовлення. Зазначалося, що за умови коректного використання цей інструмент «може писати есе, презентації, вірші та програмний код. Він може узагальнювати та перекладати текст, а також розв'язувати, оцінювати та створювати домашні завдання та завдання для іспитів» [284]. Водночас розвиток генеративних моделей засвідчив, що їх

функціональні можливості значно ширші. Сучасні нейромережі демонструють високий рівень здатності до імітації природної мови, узагальнення й аналізу інформації, перекладу, створення різножанрових текстових матеріалів, мультимодальної взаємодії та автоматизації окремих інтелектуальних процесів.

Разом з тим розвиток генеративних моделей ШІ породжує і нові виклики. Серед основних ризиків – можливість створення маніпулятивного або недостовірного контенту, поширення дезінформації, відтворення дискримінаційних упереджень, а також використання подібних систем у шахрайських цілях. Окреме занепокоєння викликає потенційне застосування генеративних моделей для автоматизованого створення шкідливого програмного забезпечення та фальсифікованих цифрових документів. Це актуалізує потребу у формуванні не тільки етичних механізмів контролю за такими технологіями, а й правових.

Аналіз чинного законодавства України свідчить, що відповідальність за значну частину суспільно небезпечних діянь, які можуть бути вчинені із використанням генеративного штучного інтелекту, вже передбачена нормами різних галузей права. Так, адміністративна відповідальність за поширення неправдивих чуток, здатних викликати паніку серед населення, встановлена статтею 173-1 Кодексу України про адміністративні правопорушення [109]; право на захист честі, гідності, ділової репутації та спростування недостовірної інформації гарантується статтею 277 Цивільного кодексу України [187]; кримінальна відповідальність за виправдовування збройної агресії Російської Федерації або дискредитацію Збройних Сил України передбачена статтею 436-2 Кримінального кодексу України [135]. Водночас зазначені норми є технологічно нейтральними й не враховують специфіки використання генеративного штучного інтелекту як нового способу або інструмента вчинення відповідних правопорушень.

Показовим у цьому контексті є законопроект № 15379, зареєстрований у Верховній Раді України 3 липня 2026 року, яким пропонується посилити кримінальну відповідальність за шахрайські діяння, вчинені із використанням

інформаційно-комунікаційних систем або систем штучного інтелекту [184]. Його поява засвідчує поступовий перехід від технологічно нейтрального регулювання до врахування специфіки штучного інтелекту як нового способу вчинення суспільно небезпечних діянь.

Подібні законодавчі ініціативи унаочнюють процес, у межах якого суто технологічні ризики (як-от генерація дезінформації чи дипфейків) трансформуються у правові категорії через призму захисту інтересів особи та суспільства. За таких умов у правотворчій діяльності загрози, породжені алгоритмічними системами, дедалі частіше розглядаються не лише як технічна проблема, а як посягання на фундаментальні суспільні цінності – безпеку, майнову стабільність і достовірність інформаційного простору.

Таким чином, аксіологічний вимір використання штучного інтелекту формується навколо фундаментального протиріччя між динамікою технологічного прогресу та імперативом збереження гуманістичних засад суспільного розвитку. Саме цей ціннісний дуалізм визначає вектор сучасної еволюції правового регулювання ШІ. Законодавча практика дедалі більше зміщується від суто прагматичного стимулювання інновацій до захисту людської гідності, забезпечення прозорості алгоритмічних рішень і збереження обов'язкового людського контролю над автономними системами. З огляду на це, аксіологічні орієнтири трансформуються із абстрактних філософських категорій у методологічну основу ризикоорієнтованої моделі права. Це зумовлює необхідність переходу від теоретико-аксіологічного осмислення проблематики до емпіричного аналізу суспільних очікувань, правових пересторог і ціннісних запитів щодо інтеграції штучного інтелекту у сучасні суспільні відносини.

1.3. Соціальні очікування і перестороги щодо впровадження штучного інтелекту як емпірична основа ризикоорієнтованого правового регулювання

Глобальне значення штучного інтелекту зумовлене його здатністю забезпечувати високий рівень оброблення великих масивів даних, прогнозування та автоматизованого ухвалення рішень. Водночас масштабне впровадження таких технологій у медицину, науку, економіку, освіту та публічне управління супроводжується глибинними соціальними, етичними та правовими викликами. Алгоритмізація суспільних процесів, трансформація ринку праці, посилення цифрового контролю, потенційна дискримінація та звуження автономії людського волевиявлення суттєво змінюють архітектуру суспільних відносин.

В українських реаліях зазначені виклики набувають особливої гостроти, оскільки розвиток і впровадження технологій штучного інтелекту відбуваються в умовах одночасної цифрової трансформації держави, воєнного стану та масштабної перебудови ключових суспільних інститутів. За таких обставин аналіз громадських очікувань і пересторог перестає бути суто соціологічним інтересом, набуваючи значення емпіричної основи для формування праксеологічно обґрунтованої ризикоорієнтованої секторальної моделі правового регулювання штучного інтелекту в Україні..

Інтеграція технологій ШІ у повсякденне життя безпосередньо залежить від рівня суспільної довіри до алгоритмічних рішень, що зумовлює необхідність емпіричного вивчення громадської думки. З цією метою протягом 2023–2025 рр. у межах дисертаційного дослідження було проведено авторське соціологічне опитування «Очікування від впровадження штучного інтелекту», результати якого представлені у додатках до роботи (Додаток Г). Репрезентативну вибірку дослідження становили 1092 респонденти, диференційовані за віком, рівнем освіти та типами населених пунктів за чисельністю населення ознакою. Отриманий матеріал відображає структуру

суспільних очікувань і пересторог щодо використання штучного інтелекту та створює фактологічну основу для визначення соціально прийнятних меж його правового регулювання.

Результати проведеного опитування засвідчили неоднорідність та амбівалентність суспільного сприйняття ШІ. Зокрема, потенційні загрози та ризики впровадження інтелектуальних систем викликають занепокоєння у 43,7 % респондентів, тоді як 32,0 % опитаних не вбачають у цифровізації суттєвих ризиків для безпеки. Водночас 24,3 % респондентів не змогли чітко визначити власне ставлення до цього питання.

Проведене опитування показало, що позитивні очікування респондентів пов'язані насамперед із багатофункціональністю ШІ: з високою швидкістю оброблення інформації, автоматизацією рутинних процесів та небезпечної праці, економією часу та здатністю працювати з великими масивами даних, що сприятиме підвищенню ефективності професійної діяльності. Потенційна неупередженість, об'єктивність, прозорість, на думку респондентів, допоможуть мінімізувати вплив людського фактору, зокрема корупційних ризиків. Крім того ШІ сприймають як високоточний аналітичний інструмент, здатний підвищувати безпеку та оптимізацію державного управління.

Виявлені суспільні очікування мають чітко виражений правовий вимір, оскільки кожна з виокремлених позицій відображає певний ціннісно-нормативний запит до правового регулювання штучного інтелекту. У цьому контексті *суспільний запит виступає важливим орієнтиром для формування державної правової політики у сфері цифровізації, визначаючи її стратегічні пріоритети та завдання*. Відтак, отримані емпіричні дані актуалізують необхідність розробки нормативно-правових механізмів, спрямованих на стимулювання інновацій, адаптацію трудового законодавства до умов автоматизації та створення сприятливого регуляторного середовища для безпечного використання технологій ШІ. Саме вони визначають соціально прийнятні межі використання автономних систем, впливають на рівень довіри до цифрових технологій та забезпечують демократичну легітимність майбутніх

політико-правових рішень.

Як показують результати, суспільне сприйняття ІІІ ґрунтується переважно на його практичній корисності, водночас саме ці можливості зумовлюють виникнення найбільших суспільних пересторог, пов'язаних із масштабами та наслідками його застосування.

Аналіз відповідей респондентів дає змогу згрупувати основні перестороги щодо використання штучного інтелекту за кількома взаємопов'язаними напрямками.

Насамперед респонденти висловлювали побоювання щодо витіснення людини автономними системами, скорочення робочих місць та втрати професійної конкурентоспроможності. Значна частина відповідей також стосувалася ризиків самонавчання ІІІ, втрати людського контролю над автономними системами і передавання їм повноважень щодо самостійного ухвалення рішень.

Окрему групу становили перестороги, пов'язані з деградацією людського мислення внаслідок надмірного делегування когнітивних функцій автономним системам, а також можливістю використання ІІІ як інструменту маніпулятивного впливу на суспільну свідомість через поширення пропаганди, дезінформації та нав'язування моделей поведінки.

Респонденти висловлювали занепокоєння щодо втрати гуманістичних цінностей, послаблення міжособистісної взаємодії та непрогнозованості подальшого розвитку взаємодії людини і штучного інтелекту.

Аналіз відповідей засвідчив, що суспільне сприйняття використання штучного інтелекту істотно різниться залежно від сфери його застосування. Найвищий рівень підтримки респонденти висловили щодо освіти і науки (90,8 %), ІТ-сфери (72,7 %), медійної сфери та реклами (64,7 %), транспорту (35,2 %), медицини і ветеринарії (31,4 %), екології (31,2 %), воєнної сфери (29,4 %) та правоохоронної діяльності (25,4 %). Водночас найбільші перестороги викликає використання ІІІ у медицині і ветеринарії (61,9 %), освіті і науці (57 %), державному управлінні (36,7 %), воєнній сфері (34,7 %), правосудді (17,8 %),

політиці (16,9 %) та правоохоронній діяльності (15,7 %).

Порівняння отриманих результатів свідчить, що рівень суспільної підтримки використання ШІ визначається насамперед характером функцій, які покладаються на автономні системи. Якщо у сферах, де штучний інтелект виконує допоміжну роль, його використання пов'язують із підвищенням ефективності, точності та безпеки, то у сферах, пов'язаних із реалізацією владних повноважень, захистом прав людини чи ухваленням соціально значущих рішень, рівень суспільних пересторог істотно зростає. Це свідчить про стійкий суспільний запит на збереження вирішальної ролі людини у здійсненні функцій, що безпосередньо впливають на права, свободи та безпеку особи.

Водночас результати опитування засвідчили ще одну закономірність: пріоритетні сфери використання штучного інтелекту значною мірою збігаються зі сферами, щодо яких респонденти висловлювали найбільші перестороги. Така амбівалентність суспільного сприйняття свідчить, що, визнаючи значний технологічний потенціал штучного інтелекту, суспільство не готове делегувати йому виконання функцій, пов'язаних із реалізацією владних повноважень, захистом прав людини та ухваленням рішень, які мають істотні соціальні наслідки.

Показовою у цьому контексті є сфера освіти і науки. На перший погляд парадоксальним видається те, що вона одночасно посідає одне з перших місць як серед пріоритетних напрямів використання ШІ, так і серед сфер, щодо яких респонденти висловлюють найбільші перестороги. Це свідчить не про заперечення використання ШІ, а про високий рівень суспільної чутливості до проблем академічної доброчесності, достовірності результатів інтелектуальної діяльності та збереження провідної ролі людини у процесах навчання й наукового пізнання.

Водночас високий рівень підтримки використання ШІ в ІТ-сфері, медіа, рекламі, транспорті та екології пояснюється переважно сприйняттям цих сфер як технологічно орієнтованих, у яких автоматизація не вступає у безпосередній

конфлікт із вимогами моральної оцінки, емпатії чи персональної відповідальності.

Натомість у медицині, воєнній сфері та правоохоронній діяльності підтримка використання ІІІ поєднується з істотними пересторогами щодо втрати людського контролю, можливих ризиків для життя і здоров'я, обмеження прав людини та делегування автономним системам соціально значущих рішень. Така закономірність ще раз підтверджує, що суспільне схвалення використання ІІІ залежить не стільки від сфери його застосування, скільки від характеру функцій, які передаються автономним системам.

Оскільки традиційні моделі нормативного регулювання виявилися недостатньо адаптованими до темпів розвитку новітніх технологій, механізми м'якого права стали однією з перших глобальних відповідей на соціальні та етичні виклики, пов'язані з використанням штучного інтелекту.

Однією з наймасштабніших міжнародних ініціатив у цій сфері стала започаткована у 2016 р. IEEE «Глобальна ініціатива з етики автономних та інтелектуальних систем» [404] (*The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems*), результатом якої стала концепція Ethically Aligned Design. Її основна ідея полягає в узгодженні розвитку технологій штучного інтелекту з етичними цінностями, пріоритетом людського добробуту та культурним контекстом їх застосування. Особливу увагу документ приділяє прозорості алгоритмів, запобіганню алгоритмічній упередженості, захисту персональних даних, етичному проєктуванню та забезпеченню людського контролю над функціонуванням інтелектуальних систем.

Запропонований підхід засвідчив, що ефективне регулювання штучного інтелекту потребує врахування не лише технічних і правових, а й соціальних чинників, зокрема рівня суспільної довіри, очікувань і пересторог. Саме ця ідея стала одним із методологічних орієнтирів проведеного у межах дисертаційного дослідження соціологічного опитування.

Водночас сучасні дослідники наголошують, що штучний інтелект лише частково піддається класичним моделям правового регулювання. Зокрема, Г.

Марчант зазначає, що системи ШІ охоплюють різні сфери економіки, юрисдикції та суспільних відносин, а ризики їх використання виходять за межі традиційних механізмів регуляторного контролю, охоплюючи проблеми технологічного безробіття, алгоритмічної упередженості, трансформації взаємодії людини і машини та автономізації інтелектуальних систем [432].

У роботах Г. Марчанта, Е. Маєр та М. Скенлон підкреслюється, що соціальні й етичні аспекти є невід'ємною складовою розвитку новітніх технологій [433], *а їх ігнорування під час формування правової політики вже не є ані політично, ані суспільно прийнятним. Це зумовлює необхідність інтеграції механізмів оцінки соціальних та етичних наслідків у процес правового регулювання* [434].

У цьому контексті суспільні перестороги щодо використання штучного інтелекту виконують функцію раннього виявлення потенційних правових і соціальних ризиків та формують емпіричну основу для моделювання соціально-правової карти ризиків ШІ в Україні. Такий аналітичний інструмент дає змогу визначити зони підвищеної суспільної чутливості, межі довіри до алгоритмічних рішень і сфери, у яких правове регулювання потребує запровадження спеціальних обмежень або режимів посиленого контролю.

В умовах цифрової трансформації України, що відбувається на тлі воєнних викликів і масштабної інституційної перебудови, така карта ризиків набуває не лише теоретичного, а й прикладного значення як орієнтир для формування проактивної ризикоорієнтованої правової політики.

Особливу увагу серед високоризикових сфер привертає застосування ШІ у воєнній сфері, насамперед у контексті автономної зброї. Результати опитування засвідчили високий рівень суспільних пересторог щодо делегування автономним системам повноважень, пов'язаних із застосуванням летальної сили. Попри усвідомлення їхнього значення для обороноздатності держави в умовах війни, такі системи пов'язуються з ризиками втрати людського контролю, розмивання відповідальності та виникнення складних етичних дилем. У правовому вимірі це підтверджує суспільний запит на

збереження вирішальної ролі людини під час ухвалення рішень про застосування сили, що узгоджується із сучасними міжнародними підходами до забезпечення змістовного людського контролю (*meaningful human control*) над автономними системами озброєння та обмеження використання повністю автономної летальної зброї.

Як засвідчили результати проведеного опитування, суспільні перестороги щодо використання ІІІ значною мірою формуються під впливом інформаційного простору, медійного дискурсу та особистого досвіду взаємодії з відповідними технологіями. Водночас значна частина респондентів ототожнює системи штучного інтелекту з автоматизованими системами або технологіями Інтернету речей.

Додатковий аналіз результатів опитування із застосуванням інструментів Big Data підтвердив загальні тенденції суспільного сприйняття ІІІ та не вплинув на сформульовані висновки щодо пріоритетних напрямів правового регулювання. Отримані результати дають підстави стверджувати, що суспільні перестороги щодо використання ІІІ відображають потенційні ризики порушення різних груп фундаментальних прав людини, а відтак мають враховуватися при формуванні ризикоорієнтованої моделі його правового регулювання.

Проведене дослідження засвідчило, що зафіксовані побоювання громадян узгоджуються із закріпленими у національному законодавстві та міжнародних стандартах підходами до захисту цивільних, соціальних, економічних і культурних прав людини.

Зокрема, побоювання щодо цифрового контролю актуалізують необхідність забезпечення права на повагу до приватного життя та захист персональних даних, гарантованих статтею 32 Конституції України [115], статтею 8 Конвенції про захист прав людини і основоположних свобод [112] та положеннями Загального регламенту Європейського Союзу про захист даних (GDPR) [472]. Перестороги, пов'язані з автоматизацією праці, узгоджуються не лише з положеннями статті 43 Конституції України [115], що гарантує право

на працю, а й зі статтею 6 Міжнародного пакту про економічні, соціальні і культурні права [147], а також принципом недискримінації, закріпленим у статті 24 Конституції України [115] та статті 14 Конвенції про захист прав людини і основоположних свобод [112]. Антропологічні й екзистенційні побоювання зумовлюють необхідність забезпечення людської гідності та свободи думки, гарантованих статтями 3 і 34 Конституції України [115] та статтями 1 і 10 Хартії основоположних прав Європейського Союзу [346].

В аспекті вікової диференціації респондентів виявлено аналогічні побоювання щодо автоматизації праці, які мають особливу специфіку серед молоді. Окрім зазначених вище конституційних гарантій, перестороги цієї групи соціуму додатково актуалізують положення статті 23 Загальної декларації прав людини та статті 1 Європейської соціальної хартії (переглянутої). У комплексі з міжнародно-правовими актами ці норми деталізують обов'язки держави щодо забезпечення права на перше робоче місце, професійну реалізацію, справедливі умови праці та захист молодих спеціалістів від технологічного безробіття

Побоювання щодо впливу штучного інтелекту на освіту та інтелектуальне становлення особи актуалізують нормативний зміст права на освіту, гарантованого статтею 53 Конституції України та конкретизованого у статті 3 Закону України «Про освіту» [205], відповідно до якого метою освіти є всебічний розвиток людини, формування її компетентностей, талантів, інтелектуальних і творчих здібностей. Зазначені положення знаходять своє відображення у статті 26 Загальної декларації прав людини, статті 13 Міжнародного пакту про економічні, соціальні і культурні права та статтях 9, 10 і 17 Європейської соціальної хартії (переглянутої). Відтак, високий рівень суспільної чутливості до використання ШІ в освітній сфері підтверджує актуальність людиноцентричного підходу, відповідно до якого технологічний розвиток має сприяти всебічному розвитку особистості, а не підміняти інтелектуальну діяльність людини.

Особливе місце у сфері освіти і науки посідають питання забезпечення

академічної доброчесності, яка виступає етичним та правовим критерієм допустимості використання ІІІ у сфері освіти та науки. За умов добросовісного використання ІІІ сприймається респондентами як інструмент підвищення ефективності навчальної та наукової діяльності, однак у разі зловживань – як фактор ризику для достовірності знань, справедливості академічного середовища та збереження інтелектуальної автономії людини. Найбільш виразно цей суспільний запит проявляється у сфері вітчизняної освіти та науки, яка в умовах війни, поширення дистанційного навчання та активної цифровізації освітнього середовища є однією з найбільш динамічних сфер інтеграції генеративних систем ІІІ. У цьому аспекті результати проведеного опитування переконливо засвідчують суспільний запит на нормативне врегулювання використання ІІІ – від забезпечення академічної доброчесності й прозорості автоматизованих систем до визначення меж допустимого використання генеративних технологій у навчальному та науковому процесах.

Отримані результати підтверджують, що ключовим чинником конфліктності сприйняття використання ІІІ у сфері освіти і науки є проблема академічної доброчесності. У суспільній свідомості генеративні технології сприймаються не лише як засіб підвищення ефективності навчальної та наукової діяльності, а й як потенційне джерело недоброчесної конкуренції, девальвації інтелектуальної праці та послаблення пізнавальної автономії людини. Це актуалізує необхідність формування спеціальних механізмів правового регулювання використання генеративних систем ІІІ, спрямованих на забезпечення академічної доброчесності, прозорості їх застосування та збереження пріоритету людської інтелектуальної діяльності.

Наступною сферою, що за результатами проведеного опитування характеризується найвищим рівнем суспільної чутливості, є медицина і ветеринарія. Високий потенціал інтелектуальних систем у діагностиці, прогнозуванні та аналізі медичних даних поєднується з найвищим рівнем суспільних пересторог, що відображає фундаментальну дилему між технологічною ефективністю та гуманістичною природою медичної діяльності:

автоматизовані системи можуть виконувати допоміжні аналітичні функції, однак остаточне клінічне рішення має залишатися за лікарем. У правовому вимірі це зумовлює необхідність особливо обережного та диференційованого підходу до регулювання медичного ШІ, спрямованого на забезпечення безпеки, прозорості та відповідальності під час використання алгоритмічних систем, а також збереження вирішальної ролі лікаря у процесі ухвалення клінічних рішень. Отримані результати підтверджують доцільність нормативного закріплення принципу «людина в контурі управління» (*human-in-the-loop*), відповідно до якого фінальне клінічне рішення та правова відповідальність за його наслідки мають залишатися за лікарем.

Життєво критичні ризики, що зумовлюють суспільні перестороги щодо використання ШІ у медичній сфері, значною мірою корелюють із ризиками його застосування у діяльності правоохоронних органів та спеціальних служб. Використання систем розпізнавання обличчя, автоматизованого моніторингу чи прогнозування поведінки потенційно створює загрози для фундаментальних прав людини, насамперед права на повагу до приватного життя, гарантованого статтею 8 Конвенції про захист прав людини і основоположних свобод, а також права на справедливий суд, передбаченого статтею 6 цієї Конвенції [113]. Саме тому використання ШІ у правоохоронній діяльності вже сьогодні належить до найбільш чутливих сфер з погляду забезпечення прав людини.

Результати проведеного опитування підтверджують наявність суспільного запиту на встановлення чітких меж допустимого використання ШІ у правоохоронній діяльності, зокрема у сфері автоматизованого спостереження, розпізнавання обличчя та прогнозування поведінки. Для України, яка одночасно вирішує завдання забезпечення національної безпеки та захисту фундаментальних прав людини, особливого значення набуває пошук балансу між безпековими потребами держави та правами людини. Аналогічні ризики виникають й у сфері правосуддя, де використання автоматизованих систем попри потенціал підвищення ефективності судочинства, може призводити до

втрати індивідуального підходу, людяності та створювати загрози реалізації права на справедливий суд.

Сприйняття використання ШІ у сфері правосуддя значною мірою залежить від рівня суспільної довіри до судової системи. За недостатньої довіри до людського фактору автоматизовані системи можуть розглядатися як інструмент мінімізації суб'єктивності, корупційних ризиків і нерівності під час здійснення правосуддя. Водночас їх застосування породжує нові правові ризики, пов'язані з алгоритмічною упередженістю, непрозорістю автоматизованих рішень та можливим обмеженням гарантій права на справедливий суд, передбаченого статтею 6 Конвенції про захист прав людини і основоположних свобод [113]. Це підтверджує необхідність збереження вирішальної ролі людини у здійсненні правосуддя та недопустимість повного делегування судових повноважень системам штучного інтелекту.

Загалом результати проведеного дослідження засвідчили, що суспільні перестороги щодо використання ШІ формують цілісну соціально-правову карту ризиків, яка окреслює найбільш чутливі сфери застосування автономних систем та визначає пріоритетні напрями їх правового регулювання. Водночас встановлено, що сприйняття таких ризиків зумовлюється не лише технологічними характеристиками ШІ, а й рівнем інституційної довіри, потребою у збереженні людського контролю, забезпеченні фундаментальних прав людини та недопущенні недоброчесної конкуренції. Це підтверджує необхідність формування в Україні комплексної ризикоорієнтованої моделі правового регулювання штучного інтелекту, чутливої до специфіки окремих сфер його застосування.

З урахуванням рівня суспільних пересторог та ризиковості використання ШІ у різних сферах суспільного життя подальше дослідження буде зосереджене на аналізі правових механізмів обмеження його використання у найбільш соціально чутливих сферах. Відповідно до результатів проведеного авторського опитування та інших наведених вище соціологічних досліджень до таких сфер належать: воєнна сфера; медицина та фармакологія; правоохоронна діяльність і

діяльність спеціальних служб; правосуддя; освіта і наука.

Саме у цих сферах найбільш гостро проявляються ризики для життя і здоров'я людини, фундаментальних прав і свобод, принципів справедливості, академічної доброчесності та суспільної довіри до державних інституцій. Це зумовлює необхідність формування спеціальних механізмів правового регулювання, заснованих на ризикоорієнтованому підході, диференційованих правових режимах та збереженні вирішальної ролі людини під час ухвалення суспільно значущих рішень.

Отримані результати підтверджують, що суспільні перестороги можуть розглядатися як один із емпіричних індикаторів потенційних правових ризиків, який має враховуватися під час формування державної правової політики та вдосконалення нормативно-правового регулювання у сфері штучного інтелекту. Це зумовлює необхідність подальшого комплексного аналізу ризиків і правових механізмів обмеження використання ШІ у найбільш соціально чутливих високоризикових сферах, що становить предмет дослідження третього розділу дисертації.

Висновки до розділу 1

1. Простежено генезис осмислення штучного інтелекту та обґрунтовано еволюцію наукових підходів до його розуміння від міфологізованих уявлень про «мислячу машину», художньо-фантастичних образів і ранніх кібернетичних концепцій, у межах яких ШІ розглядався переважно як інженерно-технічна модель, до сучасного його сприйняття як складного поліаспектного об'єкта філософської, етичної та правової рефлексії. Встановлено, що сучасний розвиток міжнародних і національних підходів до визначення штучного інтелекту супроводжується переходом від техніко-технологічного розуміння відповідних систем до їх правового осмислення через юридично значущі характеристики – автономність, адаптивність, функціональне призначення та потенційний вплив на права людини і суспільні

відносини.

2. Визначено та систематизовано юридично значущі характеристики штучного інтелекту, які зумовлюють специфіку його правового регулювання та відмежовують його від суміжних цифрових технологій, зокрема Інтернету речей (IoT). До таких характеристик віднесено здатність до аналізу й обробки інформації, самонавчання, прогнозування та формування алгоритмічних рішень, високий рівень автономності, адаптивність, а також здатність впливати на права людини і суспільні відносини.

3. На основі системно-структурного аналізу з'ясовано принципову відмінність між штучним інтелектом як системою, здатною до аналізу інформації, адаптивного навчання та формування алгоритмічних рішень, і Інтернетом речей (IoT) як технологічним середовищем збирання, передавання та обробки даних. Встановлено, що IoT виконує переважно інфраструктурну функцію забезпечення інформаційної взаємодії, тоді як системи штучного інтелекту здійснюють інтелектуальну обробку даних та формують результати, здатні впливати на права людини і суспільні відносини.

4. Виявлено правову проблему відсутності уніфікованого понятійно-категоріального апарату у сфері регулювання штучного інтелекту, що проявляється у неузгодженості його визначення у правових системах США, ЄС, Японії, Південної Кореї та Великої Британії й негативно впливає на ефективність сучасних регуляторних моделей. Встановлено, що ухвалення Регламенту ЄС про штучний інтелект (EU AI Act) не усунуло цієї проблеми, оскільки закріплений у ньому ризикоорієнтований підхід має переважно функціональний характер і не вирішує питання фундаментального правового визначення сутності штучного інтелекту. У зв'язку з цим обґрунтовано необхідність формування уніфікованої правової дефініції штучного інтелекту, яка враховуватиме його юридично значущі характеристики та забезпечуватиме чітке відмежування від суміжних цифрових технологій, зокрема Інтернету речей (IoT).

5. На підставі компаративного аналізу технічних підходів,

філософських концепцій та правових доктрин провідних міжнародних інституцій сформульовано авторську правову дефініцію штучного інтелекту. Штучний інтелект *запропоновано визначати не як будь-які «розумні» чи алгоритмізовані системи, а як автономні інтелектуальні системи, які поєднують автономність функціонування, здатність до адаптації або самонавчання та спроможність впливати на юридично значущі сфери суспільних відносин.* Обґрунтовано, що визначальною ознакою таких систем є не лише здатність імітувати окремі когнітивні процеси, а й потенційна здатність створювати ризики для прав людини, демократії, національної безпеки та публічного порядку.

6. Встановлено, що непередбачуваність подальшого розвитку автономних алгоритмів штучного інтелекту зумовлює зростання суспільних пересторог щодо втрати контролю над цифровими системами. Доведено, що зазначена проблема посилюється внаслідок існування регуляторного розриву (regulatory gap), за якого темпи технологічного розвитку випереджають процеси формування механізмів правового регулювання ШІ. За результатами проведеного емпіричного дослідження підтверджено, що такий розрив спричиняє зростання соціальної напруги, зниження рівня суспільної довіри та виникнення нових ризиків для прав людини і безпеки. У зв'язку з цим доведено необхідність формування людиноцентричної моделі правового регулювання штучного інтелекту, орієнтованої на мінімізацію ризиків і забезпечення захисту фундаментальних прав людини.

7. Розкрито зміст аксіологічного виміру функціонування штучного інтелекту, який полягає у концептуальному протиставленні гуманістичної та трансгуманістичної парадигм. Аргументовано, що радикальні трансгуманістичні концепції посилюють суспільні побоювання щодо втрати людського контролю над автономними системами, нівелювання морально-етичних орієнтирів та обмеження автономії особи. Доведено, що в умовах розвитку високоавтономних технологій гуманістична парадигма зберігає значення фундаментальної ціннісної основи правового регулювання штучного

інтелекту, а право виступає ключовим механізмом встановлення меж його допустимого використання з метою забезпечення людської гідності, автономії волі та захисту прав людини.

8. Обґрунтовано, що емпіричним підґрунтям аксіолого-правового аналізу ризиків використання штучного інтелекту є соціолого-правове дослідження. Встановлено наявність стійкого суспільного запиту на використання ШІ для підвищення ефективності окремих сфер діяльності, автоматизації рутинних процесів і мінімізації корупційних ризиків, а також підтверджено існування суспільних побоювань щодо структурного безробіття, цифрового контролю та використання ШІ у високоризикових сферах, пов'язаних із реалізацією фундаментальних прав людини. Доведено, що отримані емпіричні дані становлять інформаційну основу для формування державної правової політики та вдосконалення нормативно-правового регулювання у сфері штучного інтелекту.

9. Встановлено, що соціодемографічні характеристики респондентів впливають на особливості сприйняття окремих ризиків використання штучного інтелекту, проте ключові пріоритети суспільних очікувань та ієрархія основних побоювань залишаються сталими для різних груп. Доведено, що виявлені відмінності конкретизують особливості суспільного сприйняття ризиків, тоді як визначальним критерієм формування ризикоорієнтованої моделі правового регулювання є сфера застосування систем штучного інтелекту та характер потенційних ризиків для прав людини.

10. Визначено та систематизовано найбільш аксіологічно чутливі сфери суспільних відносин, які потребують першочергового встановлення правових обмежень та спеціальних механізмів контролю використання ШІ. Встановлено, що найвищий рівень суспільних побоювань концентрується у військовій сфері, охороні здоров'я, правоохоронній діяльності, правосудді та освіті. Доведено, що специфічний безпековий контекст України суттєво трансформував суспільне сприйняття автономних систем озброєння (Lethal Autonomous Weapons Systems – LAWS), які із футурологічної концепції

перетворилися на реальний фактор сучасної воєнної дійсності.

11. Узагальнено, що зафіксовані суспільні побоювання щодо використання штучного інтелекту виконують функцію правового індикатора потенційних ризиків та можуть розглядатися як механізм раннього виявлення латентних загроз, пов'язаних із використанням автономних систем. Доведено, що суспільне сприйняття технологічних ризиків має враховуватися як один із визначальних чинників формування державної правової політики та нормативно-правового регулювання у сфері штучного інтелекту, а також ризикоорієнтованої моделі його правового регулювання в Україні. У зв'язку з цим обґрунтовано, що формування державної правової політики та нормативно-правового регулювання у сфері штучного інтелекту має здійснюватися на засадах ризикоорієнтованого, людиноцентричного та секторально диференційованого підходів, які забезпечують баланс між технологічним розвитком, суспільною безпекою та захистом фундаментальних прав людини.

РОЗДІЛ 2. МІЖНАРОДНІ ТА НАЦІОНАЛЬНІ ПРАВОВІ ЗАСАДИ ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Сучасний етап технологічного розвитку, ознаменований експансією ШІ, вимагає трансформації класичних підходів до формування механізмів його правового регулювання. Специфіка ШІ, пов'язана із підвищеними ризиками для фундаментальних прав і свобод людини, безпеки та публічного порядку, актуалізує необхідність переосмислення сутності та структури самого інструментарію юридичного впливу.

Зазначене корелює із класичною позицією О. В. Скакун, яка розглядає механізм правового регулювання як процес переходу нормативності права в реальну впорядкованість суспільних відносин, що здійснюється за допомогою відповідного правового інструментарію з метою досягнення соціально значущого результату [234, с. 262].

Х. П. Ярмачі своєю чергою зазначає, що механізм правового регулювання не можна зводити лише до норм права. Він являє собою цілісну систему взаємопов'язаних юридичних засобів, які забезпечують впорядкування суспільних відносин і досягнення визначеної правової мети. При цьому кожен елемент механізму виконує самостійну функцію, але лише їх взаємодія забезпечує ефективність правового регулювання. норми права є лише одним із елементів механізму. До механізму входять також: правовідносини; юридичні факти; акти реалізації права; акти застосування права; способи правового регулювання; юридична відповідальність; гарантії реалізації права [344]. Водночас він підкреслює, що перелік може змінюватися залежно від предмета регулювання.

У науковій літературі існують й дещо інші підходи до визначення сутності механізму адміністративно-правового регулювання. Так, І. П. Голосніченко характеризує його як сукупність адміністративно-правових засобів, за допомогою яких здійснюється регулюючий вплив на суспільні

відносини, що складаються у процесі виконавчо-розпорядчої діяльності держави [53, с. 231]. Розвиваючи зазначений підхід, В. В. Галуцько розглядає механізм адміністративно-правового регулювання як систему юридичних засобів, функціонування яких спрямоване на забезпечення реалізації прав і свобод людини, охорону публічних законних інтересів фізичних і юридичних осіб, а також ефективне функціонування держави та громадянського суспільства [44, с. 8].

О.М. Куракін визначає механізм правового регулювання як нормативно-організований, послідовний комплексний процес, спрямований на результативне втілення правових норм у життя, на впорядкування, закріплення, розвиток і вдосконалення суспільних відносин за допомогою адекватних правових засобів з метою реалізації інтересів суспільства та держави [138, с.7]

Вчений, аналізуючи співвідношення категорій «правове регулювання» та «правовий вплив», виокремлює ознаки, що характеризують правове регулювання як самостійне правове явище. До них належать: наявність визначеного предмета у вигляді суспільних відносин, які підлягають правовому врегулюванню; використання спеціальних юридичних засобів і методів впливу; спрямованість на нормативне закріплення, упорядкування та розвиток суспільних відносин, а також усунення негативних соціальних явищ; реалізація через систему правовідносин із чітким розмежуванням прав та обов'язків їх учасників; забезпечення досягнення юридично значущих соціальних результатів [137, с. 32].

Розвиваючи концепцію структури механізму адміністративно-правового регулювання, Т.О. Коломоєць та П.С. Лютіков пропонують розмежовувати його органічні та функціональні складові. До першої групи вони відносять норми права, правовідносини та акти реалізації норм права, які утворюють нормативну основу механізму. До другої – юридичні факти, правосвідомість суб'єктів, законність, а також акти тлумачення і застосування правових норм, що забезпечують його практичне функціонування та ефективність [120, с.13].

Запропонований підхід має важливе методологічне значення для дослідження механізму правового регулювання використання штучного інтелекту, оскільки демонструє, що ефективність правового регулювання забезпечується не лише сукупністю нормативно-правових приписів, а й функціонуванням інших взаємопов'язаних елементів. Водночас розвиток технологій штучного інтелекту зумовлює необхідність розширення класичної моделі механізму правового регулювання шляхом включення до його структури таких елементів, як управління ризиками, оцінка відповідності, алгоритмічна прозорість, незалежний аудит, сертифікація та державний нагляд, які нині є невід'ємними складовими сучасної моделі регулювання штучного інтелекту.

О. А. Моргунов зауважує, що механізм адміністративно-правового регулювання є інтегрованою системою, у межах якої органічні елементи (норми права, акти їх реалізації, форми, методи та правовідносини) взаємодіють із функціональними компонентами (юридичними фактами, правосвідомістю, актами тлумачення та застосування норм права), забезпечуючи практичну реалізацію адміністративно-правового впливу. Завдяки такій взаємодії нормативні приписи трансформуються у правомірну поведінку учасників адміністративних правовідносин, що проявляється у дотриманні, виконанні та застосуванні відповідних правових норм [157, с. 277].

Наведений підхід свідчить, що ефективність механізму правового регулювання визначається не лише наявністю відповідних нормативно-правових приписів, а насамперед узгодженим функціонуванням усіх його структурних елементів. Саме тому дослідження механізму правового регулювання використання штучного інтелекту доцільно здійснювати крізь призму взаємодії міжнародних стандартів, суб'єктного складу, правових інструментів регулювання та національних механізмів їх реалізації.

Слід акцентувати увагу на пропонованій М. В. Карчевським трирівневій моделі правового регулювання ШІ, яка включає мета-рівень, стратегічний рівень, тактичний рівень, у якій «стратегічний рівень окреслює довгострокові

вектори розвитку ІІІ, а тактичний забезпечує нормативне реагування на поточні ризики, то мета-рівень відповідає за осмислення цілей, соціального призначення та відповідності ІІІ-систем людським цінностям» [124 с. 19].

З огляду на комплексний характер суспільних відносин, що виникають у зв'язку зі створенням, впровадженням та використанням систем ІІІ, дослідження міжнародних і національних засад їх правового регулювання, на нашу думку, доцільно здійснювати із застосуванням методологічного підходу, заснованого на категорії механізму правового регулювання. Такий підхід дозволяє розглядати правове регулювання не як сукупність окремих нормативно-правових актів чи ізольованих правових інститутів, а як цілісну систему взаємопов'язаних елементів, функціонування яких спрямоване на досягнення єдиної мети – забезпечення безпечного, відповідального та людиноцентричного використання систем штучного інтелекту.

У межах цього розділу механізм правового регулювання використання штучного інтелекту розглядається як багаторівнева система взаємопов'язаних нормативних, організаційних та процедурних компонентів, взаємодія яких забезпечує досягнення основної мети правового регулювання – законного використання систем штучного інтелекту, мінімізацію ризиків їх застосування, належний захист прав і свобод людини, а також створення ефективної системи державного контролю у відповідній сфері.

Виходячи із зазначеного методологічного підходу, структура цього розділу побудована відповідно до логіки функціонування самого механізму правового регулювання.

Першим структурним компонентом механізму виступають міжнародно-правові стандарти, які формують його концептуальну та ціннісну основу, визначають фундаментальні принципи безпечного й відповідального використання штучного інтелекту, а також встановлюють міжнародні стандарти захисту прав людини, демократії та верховенства права.

Другий структурний компонент становить суб'єктний склад правовідносин, який охоплює всіх учасників процесу створення, впровадження,

використання та державного регулювання систем штучного інтелекту. Саме визначення їхнього правового статусу, компетенції, прав, обов'язків і меж юридичної відповідальності забезпечує практичну реалізацію нормативних приписів.

Третім структурним компонентом є система правових засобів та інструментів регулювання, що найбільш повно реалізована у сучасній європейській моделі правового регулювання, закріпленій насамперед у AI Act. До неї належать ризико-орієнтований підхід, нормативні обмеження використання окремих систем штучного інтелекту, класифікація рівнів ризику, процедури оцінки відповідності, управління ризиками, вимоги щодо прозорості, сертифікація, державний нагляд та інші правові інструменти забезпечення безпечного функціонування систем штучного інтелекту.

Четвертий структурний компонент представлений національною моделлю правового регулювання, яка забезпечує імплементацію міжнародних і європейських стандартів у законодавство України, формування відповідної інституційної системи державного управління та адаптацію європейських підходів до особливостей української правової системи.

Таким чином, у цьому розділі застосовується методологічний підхід, відповідно до якого міжнародні та національні засади правового регулювання використання штучного інтелекту досліджуються не ізольовано, а як структурні компоненти єдиного механізму правового регулювання. Саме така логіка дослідження дозволяє послідовно розкрити взаємозв'язок між міжнародними стандартами, суб'єктами правовідносин, правовими інструментами регулювання та особливостями їх реалізації у національному законодавстві.

2.1. Міжнародно-правові стандарти безпечного та відповідального використання штучного інтелекту

Трансформація міжнародних стандартів у національну площину потребує переосмислення «класичного» механізму правового регулювання. Спираючись

на концепцію В. І. Осадчого, який визначає цей механізм як засіб забезпечення не лише приватних, а й «публічних законних інтересів та належного функціонування держави» [165], доцільно розглядати міжнародні стандарти ІІІ як фундамент для формування нових адміністративно-правових режимів безпеки. Це корелює з поглядами О. В. Стукаленка щодо функціональної єдності правових засобів, де міжнародні норми виступають первинним імпульсом для впорядкування алгоритмізованих суспільних відносин» [241, с. 23]. Традиційно у вітчизняній доктрині цей феномен трактується як архітектоніка правових засобів (дозволів, заборон, зобов'язань), що забезпечують нормативний вплив на поведінку суб'єктів та суспільні відносини.

Водночас, зважаючи на автономність та недетермінованість систем ІІІ, антропоцентричний вектор регулювання набуває вирішального значення. У цьому контексті доцільно спиратися на концепцію В. І. Осадчого, який визначає досліджуваний механізм як засіб «функціонування єдиної системи правового регулювання в сучасному українському суспільстві з метою забезпечення прав, свобод і публічних законних інтересів фізичних та юридичних осіб, а також належного функціонування громадянського суспільства і держави» [165, с. 336–340].

Практична реалізація людиноцентричної спрямованості правового регулювання у цифрову епоху стикається із суттєвими доктринальними викликами. Як слушно зазначає О. Костенко, на сучасному етапі правове регулювання у сфері ІІІ переважно обмежується розробленням технічних стандартів та сертифікацією технологій, тоді як проблема формування комплексного системного законодавчого підходу до регулювання ІІІ й надалі залишається відкритою та дискусійною [126, с. 62]. Отже, гнучкі інструменти «м'якого права» наразі випереджають класичні імперативні механізми, що зумовлює необхідність розробки принципово нових підходів до вітчизняного законодавства.

Г. К. Тетерятник справедливо зазначає: «Механізм правового регулювання для різних сфер правовідносин буде відрізнятися, що обумовлює спрямованість різних видів правового регулювання на досягнення, у першу чергу, результату суб'єктами правовідносин. Правовий режим за об'єктом правового регулювання є більш широким поняттям, він включає у себе механізм правового регулювання, може поєднувати різні методи такого регулювання» [257, с. 37].

Ураховуючи специфіку штучного інтелекту як комплексного міжгалузевого об'єкта правового регулювання, механізм його правового регулювання не може бути побудований виключно на класичній моделі адміністративно-правового чи інформаційно-правового впливу. Він має інтегрувати елементи конституційного, адміністративного, цивільного, інформаційного, кримінального права, а також міжнародно-правових стандартів та технічного регулювання.

Питання безпеки впровадження ШІ розглядаються на міжнародному рівні та є предметом уваги як міждержавних організацій, так і науково-експертних спільнот. Починаючи з 2015 року, проблематика ШІ активно обговорюється на провідних міжнародних майданчиках – від Всесвітнього економічного форуму [298] до спеціалізованих конференцій [264] та дослідницьких ініціатив.

Водночас у глобальному дискурсі простежується подвійна тенденція: з одного боку, зростає занепокоєння щодо потенційних ризиків, пов'язаних із перевищенням штучним інтелектом окремих когнітивних можливостей людини, з іншого – визнається неминучість і доцільність його подальшого впровадження з огляду на значні технологічні переваги.

За таких умов показовою є позиція щодо недопустимості надмірного обмеження інновацій, яка знаходить відображення у відповідних міжнародних документах. Зокрема, у Резолюції Європейського парламенту від 16 лютого 2017 року з рекомендаціями Європейській Комісії щодо норм цивільного права у сфері робототехніки (2015/2103(INL)) у пункті С підкреслюється необхідність правового регулювання ШІ з урахуванням його потенційного розвитку, а також

потреба у формуванні гнучких дефініцій, що не перешкоджатимуть інноваціям [355].

На момент прийняття відповідного акта основні напрями застосування ІІІ прогнозувалися насамперед у сферах транспорту, оборони, медицини, освіти та управління персоналом (пп. D-M) [355], а принцип гнучкості правового регулювання розглядався як універсальний і такий, що мав поширюватися на інші галузі.

Вказані підходи формувалися не ізольовано, а на основі попередніх міжнародних документів, спрямованих на розвиток інформаційно-комунікаційних технологій та становлення інформаційного суспільства. Серед них ключове значення мали «Окінавська хартія глобального інформаційного суспільства» [458] (далі – Окінавська хартія) та «Декларація тисячоліття» ООН [196], які заклали підґрунтя для подальшого формування інформаційно-правової політики на глобальному рівні.

Прийнята країнами «Великої вісімки» Окінавська хартія глобального інформаційного суспільства визначила засади формування нової ери розвитку, у межах якої інформаційно-комунікаційні технології розглядаються як ключовий чинник соціально-економічних трансформацій. У пункті 2 цього документа наголошується на необхідності використання інформаційних технологій для досягнення стійкого економічного зростання, підвищення добробуту, зміцнення демократії, забезпечення прав людини та підтримання міжнародної стабільності [458].

Попри свій рекомендаційний характер, Окінавська хартія заклала підґрунтя для формування сучасної інформаційно-правової політики, визначивши технології як невід’ємний елемент глобалізаційних процесів та подальшого розвитку міжнародного правового регулювання.

Невдовзі після цього Генеральною Асамблеєю ООН було схвалено Декларацію тисячоліття, яка, спираючись на ідеї інформаційного суспільства та потенціал ІКТ, розвинула положення Загальної декларації прав людини [194], і

Декларації ООН про право на розвиток 197] у контексті забезпечення сталого розвитку із використанням сучасних технологій.

Декларація тисячоліття ООН закріпила як фундаментальні цінності суспільства XXI століття свободу, рівність, солідарність, терпимість, повагу до природи та колективну відповідальність, пов'язавши їх реалізацію з можливостями застосування інформаційно-комунікаційних технологій.

У цьому контексті положення Статуту ООН та цілі «Порядку денного на XXI століття» (1992 р.) [199] були переосмислені крізь призму розвитку інформаційного суспільства та потенціалу ІКТ як інструменту їх досягнення. Зокрема, у Декларації наголошено на необхідності забезпечення доступу до нових технологій, насамперед інформаційних і комунікаційних, для всіх [196].

Отже, Декларація тисячоліття заклала підґрунтя для формування нових механізмів досягнення глобальних цілей, у яких технологічний розвиток розглядається як ключовий фактор соціального та економічного прогресу.

Подальший розвиток цих підходів відбувся під час Всесвітнього саміту з питань інформаційного суспільства, де у 2003 році в Женеві було прийнято Декларацію принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» (далі – Женевська декларація) [195].

У зазначеному документі підкреслюється необхідність використання потенціалу ІКТ для реалізації цілей Декларації тисячоліття, а також забезпечення універсального доступу до інформаційного суспільства без дискримінації (абз. 2 п. 4) [195]. Водночас поряд із визначенням цілей та інструментів їх досягнення, Женевська декларація сформулировала підходи до розуміння безпеки використання ІКТ у новому тисячолітті [195, с. 57], що згодом набули розвитку у спеціалізованому правовому регулюванні цифрових технологій, зокрема з позицій: інформаційної безпеки та безпеки мереж (абз. 1 п. 35); кібербезпеки (абз. 2 п. 35); свободи доступу до ІКТ (п. 36); протидії небажаним інформаційним впливам, зокрема спаму (п. 37).

Це дає підстави стверджувати, що Женевська декларація, будучи одним із ключових документів міжнародної інформаційно-правової політики, не містить

спеціалізованих положень щодо безпеки використання ІІІ. Основна увага в ній зосереджена на загальних питаннях безпеки інформаційних технологій та доступу до них, тоді як потенційні ризики пов'язані передусім із інформаційними загрозами, кіберзагрозами та захистом інформаційних прав людини.

Подальший розвиток міжнародних підходів до регулювання цифрових технологій відображено у Порядку денному ООН у сфері сталого розвитку до 2030 року, ухваленому у 2015 році. У пункті 53 цього документа підкреслюється відповідальність сучасного покоління за забезпечення сталого розвитку та передачу його результатів майбутнім поколінням [200].

Формування спеціалізованих механізмів обмеження використання ІІІ стало наступним етапом розвитку міжнародного правового регулювання цифрових технологій, що зумовлено появою нових ризиків, не охоплених попередніми підходами.

Дослідження змісту документів ООН щодо досягнення статутних цілей та їх інтерпретації в умовах розвитку інформаційного суспільства дає підстави стверджувати, що станом на відповідний період Організація Об'єднаних Націй не виокремлює використання ІІІ як самостійний сегмент правового регулювання, розглядаючи його в межах ширшого сектору інформаційно-комунікаційних технологій. Відповідно, у зазначених документах відсутні спеціалізовані механізми забезпечення безпечного впровадження та використання ІІІ.

Натомість інша тенденція простежується на рівні європейського права та правової політики Європейського Союзу, де питання розвитку та безпечного використання ІІІ набувають самостійного значення та стають предметом спеціалізованого правового регулювання.

Починаючи з початку ХХІ століття, в Європейському Союзі було прийнято значну кількість нормативних актів, спрямованих на розвиток інформаційних технологій та забезпечення їх безпечного функціонування.

У 2017 році Рада Європи наголосила на необхідності своєчасного

реагування на нові технологічні виклики, включаючи штучний інтелект, із одночасним забезпеченням високого рівня захисту персональних даних, цифрових прав і дотримання етичних стандартів [362].

У грудні 2018 року Європейська комісія з питань ефективності правосуддя прийняла «Етичну хартію про використання штучного інтелекту в судових системах та їх середовищі» (European Ethical Charter on the Use of AI in Judicial Systems and their Environment) [349]. Цей документ став одним із перших системних кроків до формування засад відповідального впровадження ШІ у судові системи європейських держав відповідно до цінностей Ради Європи.

У 2019 році у Висновках Ради Європейського Союзу щодо Скоординованого плану з розвитку ШІ (Coordinated Plan on Artificial Intelligence, 2019) [347] підкреслювалася необхідність повного дотримання прав громадян, а також містився заклик до перегляду чинного законодавства з метою його адаптації до нових можливостей і викликів, пов'язаних із впровадженням ШІ.

Подальший розвиток зазначених підходів знайшов своє відображення у формуванні комплексної системи правового регулювання ШІ в Європейському Союзі, ключовим елементом якої стали формування довіри до ШІ [39; 43] та ризик-орієнтований підхід до класифікації та обмеження використання відповідних технологій.

У цьому контексті важливим інституційним кроком стало створення 19 вересня 2019 року Комітету експертів з питань штучного інтелекту (САНІІ – Ad hoc Committee on Artificial Intelligence Комітетом Міністрів Ради Європи, якому було доручено вивчити доцільність та можливі елементи правової основи для розроблення, проєктування і застосування ШІ з урахуванням стандартів Ради Європи у сферах прав людини, демократії та верховенства права.

На відміну від класичної моделі правотворення, коли спочатку формуються юридично обов'язкові норми, а згодом практика їх застосування, у сфері ШІ розвиток механізму правового регулювання відбувався у зворотній

послідовності. Первинно міжнародною експертною спільнотою були вироблені етичні стандарти використання алгоритмічних технологій, які надалі трансформувалися у юридично обов'язкові вимоги, закріплені насамперед у AI Act, Рамковій конвенції Ради Європи про штучний інтелект, права людини, демократію та верховенство права, а також інших актах права Європейського Союзу. Таким чином, етичні принципи стали своєрідною нормативною матрицею, на основі якої сформувалися сучасні адміністративно-правові режими регулювання штучного інтелекту.

Рекомендації з етики для надійного ШІ (Ethics Guidelines for Trustworthy AI), розроблені у 2019 році, визначають сім ключових вимог до систем ШІ: людський контроль та нагляд; технічна надійність і безпека; конфіденційність і управління даними; прозорість; різноманітність, недискримінація та справедливість; суспільне та екологічне благополуччя; підзвітність [358].

У цьому контексті сім вимог до надійного штучного інтелекту доцільно розглядати не лише як систему етичних рекомендацій, а як ціннісно-нормативний компонент механізму правового регулювання використання штучного інтелекту, що визначає допустимі межі функціонування алгоритмічних систем та зміст майбутніх юридичних обов'язків їх розробників, постачальників і користувачів. Фактично вони виконують регулятивну функцію, оскільки встановлюють критерії, відповідно до яких держава надалі вибудовує систему адміністративно-правових засобів впливу на суспільні відносини у сфері штучного інтелекту.

Так, вимога щодо забезпечення людського контролю заклала основу гарантійного елементу механізму правового регулювання, відповідно до якого прийняття юридично значущих рішень не може бути повністю передано алгоритмічним системам без можливості втручання людини [368]. Прозорість функціонування систем ШІ охоплює як безпеку оброблення даних, так і зрозумілість їх роботи. Зокрема, передбачається впровадження механізмів відстеження дій системи, які мають бути доступними та зрозумілими для зацікавлених сторін, включаючи користувачів. При цьому підкреслюється, що

особи повинні бути поінформовані про факт взаємодії із системою ШІ, а також про її можливості та обмеження: «Люди повинні знати, що вони взаємодіють із системою штучного інтелекту, і повинні бути поінформовані про можливості та обмеження системи» [358].

Вимоги технічної надійності та безпечності трансформувалися у правові механізми оцінки відповідності, сертифікації, управління ризиками та державного нагляду за високоризиковими системами штучного інтелекту. Принципи конфіденційності, належного управління даними та прозорості стали підґрунтям для формування інформаційно-правових та процедурних елементів механізму, що забезпечують пояснюваність алгоритмічних рішень, законність обробки даних і можливість здійснення ефективного контролю за функціонуванням систем штучного інтелекту. Водночас вимоги недискримінації, справедливості, суспільного благополуччя та підзвітності сформували правозахисний і контрольно-наглядовий компоненти механізму правового регулювання, які знайшли своє відображення у процедурах аудиту, оцінки впливу на фундаментальні права, незалежного контролю, ведення технічної документації та запровадження юридичної відповідальності за порушення вимог щодо використання систем штучного інтелекту.

Отже, значення *Ethics Guidelines for Trustworthy AI* полягає не лише у формулюванні універсальних етичних принципів використання штучного інтелекту. Вони стали методологічною основою формування сучасного механізму правового регулювання, визначивши його аксіологічний зміст, напрями подальшої нормотворчості та систему правових інструментів, що забезпечують безпечне, підконтрольне й людиноцентричне використання алгоритмічних технологій. Саме тому зазначені Рекомендації слід розглядати як вихідну точку переходу від добровільного етичного саморегулювання до комплексного юридично обов'язкового регулювання штучного інтелекту, яке сьогодні реалізується через адміністративно-правові механізми, закріплені в законодавстві Європейського Союзу.

На нашу думку, ці сім вимог мають бути враховані при прийнятті спеціального закону про ШІ в Україні, гармонізованого з європейським стандартом. Як справедливо зазначає М. Карчевський, перехід до юридично зобов'язального регулювання має базуватися на трирівневій моделі, де метарівень (аксіологічний фундамент) формується саме на основі цих етичних стандартів для захисту гідності та свободи особи в умовах алгоритмізації [125, с. 20].

У механізмі правового регулювання ці сім вимог трансформувалися з етичних принципів у юридичні обов'язки розробників та операторів, порушення яких тягне за собою суворі адміністративні санкції за AI Act. Це і є перехід від Digital State до Agentic State – держави, де законність автоматизованих дій гарантується техніко-юридичними фільтрами.

Порушуючи проблему нормативного закріплення етики використання ШІ, Ів Пулет, президент IFAP (WG Info-Ethics) поставив під сумнів самі підходи до можливості її правового унормування, вказуючи: «По-перше, це сама природа запропонованого регулювання. Чи достатньо стверджувати етичні принципи, чи етика в кінцевому підсумку стосується претензії правової бази? Окрім цього, чи відноситься регуляторна модель до саморегулювання, співрегулювання чи державного регулювання?» [502].

Подальший розвиток механізмів забезпечення безпечного використання ШІ пов'язаний із усвідомленням його як джерела підвищених ризиків, що зумовило необхідність вироблення відповідних управлінських і правових рішень на європейському рівні.

Під час спеціальної зустрічі Європейської Ради (1-2 жовтня 2020 р.) застосування ШІ було віднесено до сфер підвищеного ризику [363], у зв'язку з чим Європейська Рада запропонувала Європейській Комісії такі напрями дій: запропонувати шляхи збільшення європейських і національних державних і приватних інвестицій у дослідження, інновації та впровадження штучного інтелекту; забезпечити кращу координацію, розвиток мереж і синергії між

європейськими дослідницькими центрами; надати чітке та об'єктивне визначення систем штучного інтелекту з високим рівнем ризику [363].

Водночас, у 2020 році Комітетом Міністрів Ради Європи була прийнята Рекомендація CM/Rec (2020)1 щодо впливу алгоритмічних систем на права людини, преамбула якої відображає ключові положення, що свідчать про формування підходу, за якого алгоритмічні системи розглядаються як об'єкт підвищеного правового контролю у зв'язку з їхнім впливом на права людини, демократичні цінності та принцип верховенства права: зобов'язання держав забезпечувати права і свободи людини поширюється на умови технологічного розвитку та цифрової трансформації суспільства; алгоритмічні системи, включаючи системи ШІ, можуть мати як позитивний, так і негативний вплив на реалізацію прав і свобод людини; динамічний розвиток цифрових технологій зумовлює необхідність постійного моніторингу та адаптації механізмів управління з метою ефективного захисту прав людини [348].

Рекомендація CM/Rec(2020)1 фактично пропонує комплексну модель механізму адміністративно-правового регулювання, яка ґрунтується на поєднанні нормативних, інституційних, процедурних, контрольних і гарантійних засобів впливу. Аналіз змісту Рекомендації та її Додатка («Керівництво щодо реагування на вплив алгоритмічних систем на права людини») дає підстави стверджувати, що запропонований Радою Європи механізм включає декілька взаємопов'язаних складових.

Нормативний елемент, що передбачає обов'язок держав здійснювати перегляд національного законодавства, адміністративних процедур і державної політики з урахуванням ризиків застосування алгоритмічних систем та необхідності забезпечення фундаментальних прав людини.

Інституційний елемент, який проявляється у вимозі створення або належного забезпечення діяльності компетентних органів державного нагляду, контролю, оцінки ризиків і правозастосування, наділених достатніми повноваженнями для здійснення моніторингу, перевірок, координації діяльності та реагування на порушення прав людини.

Процедурний елемент, що охоплює оцінку ризиків, оцінку впливу алгоритмічних систем на права людини, моніторинг їх функціонування протягом усього життєвого циклу, забезпечення прозорості, підзвітності, можливості перегляду автоматизованих рішень і застосування превентивних запобіжних заходів. Саме ця складова демонструє перехід від реактивного адміністративного контролю до моделі превентивного управління ризиками.

Контрольно-гарантійний елемент, який полягає у функціонуванні систем державного нагляду, регулярного звітування, незалежного аудиту, участі громадськості, забезпеченні ефективних засобів правового захисту, а також постійному перегляді правової політики відповідно до розвитку цифрових технологій. Характерною особливістю цього підходу є поєднання державного контролю із механізмами демократичного врядування та суспільної участі.

Таким чином, аналіз положень Рекомендації CM/Rec(2020)1 дозволяє зробити висновок, що цей документ фактично започатковує нову модель механізму адміністративно-правового регулювання використання штучного інтелекту, у якій визначальне значення мають не лише нормативні приписи, а й адміністративні процедури оцінювання ризиків, інституційне забезпечення державного нагляду, механізми прозорості, підзвітності, участі громадськості та гарантії захисту прав людини. Саме такий підхід став основою подальшого розвитку європейської моделі правового регулювання штучного інтелекту та отримав нормативне закріплення у Регламенті (ЄС) 2024/1689 (Artificial Intelligence Act), який вперше встановив комплексну систему обов'язкових вимог до високоризикових систем штучного інтелекту, людського нагляду, оцінки відповідності, постринкового моніторингу, державного нагляду та відповідальності суб'єктів, що розробляють або використовують такі системи.

Додаток до Рекомендації Ради Європи – «Керівництво щодо реагування на вплив алгоритмічних систем на права людини» – є її невід'ємною складовою та містить системний перелік загальних і спеціальних поступових заходів, спрямованих на соціально прийнятне, безпечне та кероване впровадження ШІ та інших алгоритмічних систем у суспільні відносини.

У період 2020 – 2021 років Європейський парламент ухвалив низку резолюцій, які заклали підґрунтя для подальшої деталізації правового регулювання у ключових сферах взаємодії з технологіями штучного інтелекту.

Зокрема, у резолюціях 2020 року було визначено основні напрями правового впливу на сферу ІІІ, що охоплюють:

- етичні засади розроблення та використання штучного інтелекту і пов'язаних технологій (Резолюція від 20 жовтня 2020 р., 2020/2012 (INL)) [364];

- формування режиму цивільно-правової відповідальності за шкоду, заподіяну системами штучного інтелекту (Резолюція від 20 жовтня 2020 р., 2020/2014 (INL)) [365];

- визначення підходів до захисту прав інтелектуальної власності у сфері розроблення технологій штучного інтелекту (Резолюція від 20 жовтня 2020 р., 2020/2015 (INI)) [366].

Слід погодитися з думкою І. М. Городиського, що хоча Резолюції Європарламенту не відносяться в системі джерел права ЄС до загальнообов'язкових актів, її приписи дають уявлення щодо очікувань у процесі правового регулювання сфери ІІІ, а також містять «дороговкази, на які будуть орієнтуватися при розробці відповідних обов'язкових стандартів» [57].

У 2021 році розвиток підходів до правового регулювання штучного інтелекту в Європейському Союзі набув подальшої конкретизації через галузеву та стратегічну деталізацію відповідних механізмів.

Зокрема, у проєктах звітів Європейського парламенту було окреслено специфіку застосування ІІІ у ключових сферах суспільних відносин, що дозволило сформулювати диференційований підхід до його правового регулювання. Йдеться, зокрема, про сферу кримінальної юстиції, включаючи використання ІІІ поліцією та судовими органами (2020/2016 (INI)) [367], а також про освітню, культурну та аудіовізуальну сфери (2020/2017 (INI)) [369].

Паралельно Європейська Комісія 9 березня 2021 року оприлюднила стратегічний документ «Цифровий компас 2030: європейський шлях для цифрового десятиліття» [359], який визначив довгострокові орієнтири цифрової

трансформації, включаючи розвиток і безпечне впровадження технологій штучного інтелекту.

Ключовим етапом стало започаткування 21 квітня 2021 року процесу розроблення спеціального нормативного акта – майбутнього Регламенту Європейського Союзу про штучний інтелект (AI Act) – шляхом подання відповідної пропозиції Європейської Комісії щодо встановлення гармонізованих правил у цій сфері та внесення змін до низки актів Союзу [354].

Подальший розвиток цього процесу відбувся 14 червня 2023 року, коли Європейський парламент схвалив проєкт зазначеного акта, спрямованого на комплексне врегулювання використання штучного інтелекту в Європейському Союзі.

Зазначений акт спрямований на забезпечення контролю людини за функціонуванням систем ШІ, а також на гарантування їх безпеки, прозорості, відстежуваності, недискримінаційності та екологічної безпечності.

Передбачалося, що документ встановить єдине технологічно нейтральне визначення штучного інтелекту, придатне для застосування в умовах подальшого розвитку технологій, а також забезпечить реалізацію ключових цілей правової політики Європейського Союзу у цій сфері. До таких цілей належать:

- гарантування того, що системи ШІ, які розміщуються на ринку ЄС та використовуються в ньому, є безпечними та відповідають законодавству про основні права і цінності ЄС;
- забезпечення правової визначеності з метою сприяння інвестиціям та інноваціям у сфері ШІ;
- удосконалення механізмів управління та ефективного застосування чинного законодавства щодо основних прав і вимог безпеки до систем ШІ;
- сприяння розвитку єдиного ринку безпечного та надійного ШІ і запобігання фрагментації внутрішнього ринку [354].

Важливою особливістю запропонованого підходу є його ризик-орієнтований характер, відповідно до якого обсяг правових зобов'язань прямо

залежить від рівня потенційного ризику для прав і свобод людини, а також її життя і здоров'я.

Так, зокрема, у грудні 2018 року Європейська комісія з питань ефективності правосуддя прийняла «Етичну хартію про використання штучного інтелекту в судових системах та їх середовищі» (European Ethical Charter on the Use of AI in Judicial Systems and their Environment) [349]. Цей документ став одним із перших системних кроків до формування засад відповідального впровадження ШІ у судові системи європейських держав відповідно до цінностей Ради Європи.

Наступним кроком формування сучасної міжнародної моделі правового регулювання штучного інтелекту стало ухвалення Генеральною Асамблеєю ООН 21 березня 2024 року Резолюції A/RES/78/265 «Використання можливостей безпечних, захищених і надійних систем штучного інтелекту для сталого розвитку», прийнятої консенсусом усіх держав-членів ООН. Незважаючи на рекомендаційний характер, зазначений документ має принципове значення для розвитку міжнародної правової політики, оскільки вперше на універсальному рівні визначає базові стандарти державного управління використанням штучного інтелекту та окреслює напрями формування глобальної системи його врядування [490].

На відміну від Рекомендації Ради Європи CM/Rec(2020)1, яка переважно визначає адміністративно-правові механізми забезпечення прав людини під час використання алгоритмічних систем, Резолюція Генеральної Асамблеї ООН формує глобальну концепцію публічного управління штучним інтелектом, поєднуючи питання безпеки, сталого розвитку, цифрової рівності, міжнародного співробітництва та захисту фундаментальних прав людини. Саме тому її значення виходить за межі правозахисної проблематики й охоплює загальні засади формування майбутнього міжнародного адміністративно-правового порядку у сфері використання штучного інтелекту.

Проведений аналіз дає підстави стверджувати, що Резолюція фактично закріплює ризик-орієнтовану модель державного регулювання. Якщо попередні

міжнародні акти у сфері цифрового розвитку були переважно спрямовані на забезпечення доступності інформаційно-комунікаційних технологій, то Резолюція зміщує акцент на забезпечення безпечності, захищеності та надійності систем штучного інтелекту протягом усього їх життєвого циклу. Відповідно, адміністративно-правове регулювання поступово трансформується від моделі загального державного контролю до системи превентивного управління ризиками, що охоплює розроблення, впровадження, використання та постійний моніторинг систем штучного інтелекту. Резолюція формує аксіологічну основу адміністративно-правового механізму, визначаючи людиноцентризм, повагу до прав людини, верховенство права, безпечність, прозорість, відповідальність та міжнародне співробітництво як фундаментальні принципи майбутнього правового регулювання. На відміну від галузевих регламентів, документ не встановлює конкретних адміністративних процедур, однак визначає систему цінностей, яка має бути покладена в основу національного законодавства та діяльності органів публічної влади.

Документ започатковує інституційний вимір міжнародного адміністративного співробітництва, процес юридизації етичних принципів використання штучного інтелекту. Документ закликає держави забезпечити, щоб розроблення та використання систем штучного інтелекту здійснювалися відповідно до міжнародного права, міжнародних стандартів у сфері прав людини та принципів безпеки. Унаслідок цього етичні вимоги щодо недискримінації, прозорості, людського контролю, підзвітності та справедливості поступово трансформуються у критерії оцінки правомірності діяльності суб'єктів публічного адміністрування, що набуває особливого значення для адміністративних процедур, у яких застосовуються автоматизовані системи прийняття рішень.

І. М. Берназюк підкреслює, що зазначений нормативний акт на відміну від інших міжнародних договорів у сфері прав людини, не встановлює нових фундаментальних прав, а конкретизує механізми реалізації вже закріплених міжнародними актами гарантій у контексті автоматизованого прийняття

рішень. Для України з метою подальшої імплементації положень Конвенції про штучний інтелект до національного законодавства доцільним є застосування комплексного підходу, який передбачає: нормативне закріплення принципів використання штучного інтелекту у ключових сферах публічного управління; запровадження обов'язкових процедур оцінки впливу високоризикових систем ШІ на права людини, демократію та верховенство права до їх впровадження і протягом усього життєвого циклу; інституційне посилення механізмів державного контролю шляхом визначення компетентного органу, уповноваженого здійснювати оцінку, нагляд і моніторинг використання таких систем; нормативне закріплення вимог щодо прозорості, пояснюваності та забезпечення людського контролю під час використання ШІ суб'єктами владних повноважень; а також удосконалення процесуального законодавства для забезпечення ефективного адміністративного і судового оскарження рішень, прийнятих із застосуванням алгоритмічних систем [20, с. 28].

У наукових дослідженнях, присвячених геополітиці розвитку штучного інтелекту, нині чітко окреслюються декілька напрямів: лідерство США та Китаю [35, с. 68] у сфері розроблення ШІ, а також провідна роль Європейського Союзу у його правовому регулюванні з урахуванням європейських цінностей і вимог безпеки впровадження. У межах останнього науковці виокремлюють такі чотири основні принципи наднаціонального управління:

1) «мультилатералізм» як залучення держав до участі в міжнародних організаціях і формування правових підходів до впровадження ШІ незалежно від рівня їхнього розвитку, що, зокрема, сприяє виявленню прихованих розробок і забезпеченню їх належної оцінки та контролю;

2) «мультисекторальність» як транснаціональна взаємодія із залученням стейкхолдерів та інших зацікавлених сторін;

3) «мережевий формат управління» у процесі вироблення рішень і координації дій, який пов'язується з глобалізацією управління ШІ та може запобігати концентрації технологічної влади;

4) «наднаціональна інтеграція» через формування спільних

міжнародних норм, обов'язкових для всіх учасників ринку ШІ [35, с. 68].

Зокрема, слід згадати Блетчлійську декларацію, ухвалена за результатами AI Safety Summit (1–2 листопада 2023 р.), є політичним документом, що започаткував міжнародну координацію держав у сфері безпечного розвитку передових систем штучного інтелекту. Хоча Декларація не має юридично обов'язкового характеру, її значення полягає у формуванні єдиних підходів до державного управління ризиками, пов'язаними з використанням сучасних моделей ШІ.

Концептуально документ ґрунтується на визнанні того, що найбільш потужні системи штучного інтелекту можуть створювати не лише значні соціально-економічні переваги, а й ризики глобального масштабу, які потребують скоординованого міжнародного реагування. У зв'язку з цим держави-учасниці наголошують на необхідності розвитку механізмів оцінки ризиків, наукового співробітництва, інформаційного обміну, спільного вироблення стандартів безпеки та формування інституційних механізмів міжнародного нагляду.

У контексті адміністративно-правового регулювання використання штучного інтелекту Блетчлійську декларацію, яка закріплює підхід, відповідно до якого об'єктом державного управління стає не лише процес використання ШІ, а й ризики, що виникають на всіх етапах його життєвого циклу. Саме тому ключовими елементами адміністративно-правового механізму визначаються постійний моніторинг, міждержавна координація, обмін інформацією, експертне оцінювання та превентивне реагування на потенційні загрози.

Таким чином, Блетчлійська декларація започатковує міжнародну концепцію ризик-орієнтованого адміністративного управління штучним інтелектом, яка згодом отримала подальший розвиток у Рамковій конвенції Ради Європи про штучний інтелект та Регламенті (ЄС) 2024/1689 (AI Act) [470].

Науковці, аналізуючи досвід США у сфері регулювання використання ШІ зазначають, що він свідчить про істотну відмінність від європейської моделі. На відміну від ЄС, у США відсутній єдиний комплексний нормативно-правовий

акт у цій сфері, а регулювання характеризується: по-перше, відсутністю уніфікованого законодавчого визначення штучного інтелекту навіть на федеральному рівні, що зумовлює правову невизначеність; по-друге, децентралізованою моделлю регулювання, яка поєднує федеральні ініціативи, акти адміністративного «м'якого права» та законодавство окремих штатів, що формують власні підходи до регулювання ШІ; по-третє, посиленням ризик-орієнтованого підходу, який покладає на суб'єктів, що розробляють і використовують системи штучного інтелекту, обов'язок забезпечувати належне управління пов'язаними ризиками [127, с. 26].

Китаєм у сфері правового регулювання використання ШІ протягом останнього десятиріччя здійснено суттєві кроки. Зокрема, у 2017 році було прийнято Національний план розвитку новітніх галузей, який визначив курс на світове лідерство, у 2020 році опубліковано «Посібник зі стандартів ШІ», що містив рекомендації щодо безпеки та етики [121, с. 210]. У 2021 році було прийнято Personal Information Protection Law of the People's Republic of China, який хоча і не є спеціальним законом про ШІ, однак формує правову основу його використання у частині обробки персональних даних та автоматизованого прийняття рішень. Закон закріплює принципи законності, прозорості, мінімізації даних і недискримінації, а також встановлює вимоги до використання алгоритмів, надаючи особам право на отримання пояснень щодо автоматизованих рішень і захист від їх дискримінаційного впливу. Водночас документ покладає на державні органи повноваження щодо здійснення нагляду, проведення перевірок та застосування адміністративних санкцій за порушення законодавства у сфері захисту персональної інформації. У контексті дослідження він становить інтерес як складова китайської моделі адміністративно-правового регулювання використання штучного інтелекту, оскільки визначає нормативні, процедурні та контрольні засади використання даних, необхідних для функціонування систем ШІ [482].

У грудні 2025 року Наприкінці 2025 року Адміністрація кіберпростору Китаю (САС) оприлюднила проєкт «Тимчасових заходів щодо адміністрування

інтерактивних послуг штучного інтелекту, подібних до людських», який став першою комплексною спробою спеціального правового регулювання систем ШІ, здатних імітувати людську особистість та емоційну взаємодію. На відміну від загального регулювання генеративного ШІ, документ поширюється виключно на сервіси, що формують емоційний контакт із користувачем (віртуальні співрозмовники, цифрові компаньйони, емоційні чат-боти).

Проект запроваджує превентивну модель адміністративно-правового регулювання, покладаючи на постачальників послуг обов'язки щодо забезпечення прозорості використання ШІ, постійного інформування користувачів про взаємодію з алгоритмічною системою, моніторингу ознак психологічної залежності, захисту неповнолітніх і вразливих категорій осіб, недопущення емоційних маніпуляцій, а також спеціального режиму захисту емоційних даних користувачів.

Особливістю документа є поширення державного контролю на весь життєвий цикл відповідних систем штучного інтелекту – від розроблення алгоритмів до їх експлуатації та модифікації. Постачальники зобов'язані повідомляти регулятора про істотні зміни функціонування систем, а також забезпечувати відповідність встановленим вимогам безпеки та суспільної стабільності.

Таким чином, зазначений проєкт демонструє подальшу еволюцію китайської моделі адміністративно-правового регулювання ШІ від загального контролю за алгоритмічними системами до спеціалізованого регулювання окремих видів ШІ залежно від характеру ризиків. На відміну від європейського ризик-орієнтованого підходу, китайська модель поєднує превентивний державний нагляд із централізованим адміністративним контролем, поширюючи його не лише на технічну безпеку, а й на психологічний вплив алгоритмічних систем на користувачів. По суті, зазначений проєкт демонструє тенденцію правового регулювання використання ШІ у Китаї з використанням не просто ризик-орієнтованої моделі, а пріоритизації національної безпеки над технологічною автономією.

Водночас, якщо у ст. 5 AI Act істотно обмежує використання систем розпізнавання емоцій, забороняючи їх застосування в окремих сферах високого ризику, насамперед у трудових відносинах та освіті, то відмінністю китайської моделі для державної системи є здатність алгоритмів мати прямий доступ до баз даних державних органів, що дозволяє емоційному ШІ (наприклад, асистентам у судах) ефективніше виконувати функції верифікації осіб та виявлення логічних невідповідностей у їхніх свідченнях. Це створює модель «розумного врядування», де емоційна взаємодія є не лише сервісом, а й інструментом забезпечення публічного порядку. Якщо європейська модель захищає людину від втручання ШІ в її емоційну сферу через заборони, то китайська модель намагається керувати цим втручанням, роблячи його інструментом державної політики та соціальної стабільності.

Повертаючись до правового регулювання використання ШІ в ЄС, підсумуємо, що багаторічна робота експертних груп над відповідними документами дала змогу сформулювати підхід, відображений в AI Act, як у базовому акті, що узагальнено закріплює «збалансований і пропорційний горизонтальний регуляторний підхід до штучного інтелекту, який обмежується мінімально необхідними вимогами для усунення ризиків і проблем, пов'язаних із штучним інтелектом, без надмірного обмеження чи перешкод технологічному розвитку або непропорційного збільшення вартості розміщення рішень ШІ на ринку» (згідно з пояснювальною запискою до AI Act) [353].

AI Act має комплексну структуру, що охоплює регулювання використання ШІ залежно від рівня ризику, встановлення заборонених практик, визначення вимог до систем високого ризику, забезпечення прозорості окремих систем, а також механізми управління, нагляду за ринком і постринкового контролю. Окрему увагу приділено підтримці інновацій, формуванню кодексів поведінки та запровадженню відповідальності за порушення встановлених вимог. Така структура відображає ризик-орієнтований підхід Європейського Союзу до регулювання ШІ, у межах якого обсяг правових вимог прямо

залежить від потенційного впливу відповідних систем на права людини та безпеку.

Вихідною точкою до концептуалізації цього акту як найвищого етапу еволюції механізму правового регулювання ІІІ в ЄС, що трансформує етичні настанови у імперативні адміністративно-правові режими стала спроба правової регламентації суміжних із штучним інтелектом правовідносин у сфері робототехніки. Серед нормативних джерел зазначеного періоду базове значення має Резолюція Європейського парламенту від 16 лютого 2017 року з рекомендаціями Комісії щодо норм цивільного права у сфері робототехніки [355] (далі – Резолюція 2017 року). Цей акт став першим системним кроком до визначення цивільно-правових засад функціонування автономних агентів, охоплюючи, зокрема, такі ключові аспекти: автономні транспортні засоби (п.п. 24-29); дрони (п. 30); роботизовані системи догляду (п.п. 31, 32); медичні роботи (п.п. 33-35); роботи для відновлення та покращення людського організму (п.п. 36-40).

Другим етапом формування європейської моделі обмеження використання ІІІ став розвиток правового регулювання інтернету речей, якому вже було приділено увагу в попередніх розділах цього дослідження. Базовими документами Європейського Союзу у цій сфері стали Європейський кодекс електронних комунікацій (European Electronic Communications Code (Directive (EU) 2018/1972) [370] та Регламент про BEREC (Regulation (EU) 2018/1971) [469], відповідно до яких сутність обмежень використання ІоТ, по суті, зводилась до забезпечення кібербезпеки, захисту персональних даних, гармонізації стандартів зв'язку та запобігання антиконкурентним практикам на ринку електронних комунікацій.

Третій, завершальний, етап формування сучасної системи правового регулювання ІІІ був започаткований результатом десятирічної роботи експертних груп та прийняттям Європейським парламентом AI Act – Законодавчої резолюції Європейського Парламенту від 13 березня 2024 року щодо пропозиції щодо регламенту Європейського Парламенту та Ради про

встановлення гармонізованих правил щодо штучного інтелекту (Закон про штучний інтелект) та внесення змін до окремих законодавчих актів Союзу [352].

Регламент (ЄС) 2024/1689 (AI Act) формує ризик-орієнтовану модель правового регулювання штучного інтелекту, відповідно до якої інтенсивність адміністративно-правового впливу визначається рівнем потенційного ризику, який конкретна система ШІ може створювати для прав людини, безпеки, демократії та інших суспільних інтересів. На відміну від традиційного галузевого регулювання, AI Act не встановлює однакових вимог до всіх систем штучного інтелекту, а запроваджує диференційований підхід, за якого обсяг правових обов'язків суб'єктів залежить від категорії ризику відповідної системи.

З цією метою AI Act класифікує системи штучного інтелекту на чотири групи: системи з неприпустимим ризиком, використання яких за загальним правилом забороняється; системи високого ризику, для яких встановлено комплекс обов'язкових вимог щодо управління ризиками, якості даних, технічної документації, людського контролю, прозорості, оцінки відповідності та постринкового моніторингу; системи обмеженого ризику, використання яких допускається за умови виконання окремих вимог щодо прозорості та інформування користувачів; а також системи мінімального ризику, для яких спеціальні регуляторні вимоги практично не застосовуються, хоча заохочується дотримання добровільних кодексів поведінки [353].

Таким чином, класифікація ризиків, закріплена в AI Act, є не лише способом систематизації систем штучного інтелекту, а й основою побудови сучасного механізму адміністративно-правового регулювання, у межах якого рівень державного контролю, адміністративних процедур і юридичних обов'язків прямо залежить від ступеня ризику, пов'язаного з використанням відповідної системи ШІ. Саме ризик-орієнтований підхід визначає зміст правового статусу суб'єктів, межі державного нагляду та обсяг адміністративно-правових засобів, що застосовуються до різних категорій

систем штучного інтелекту. Класифікація ризиків в AI Act є не самостійним елементом механізму, а критерієм диференціації адміністративно-правового регулювання, який визначає зміст процедур, інтенсивність державного нагляду, обсяг обов'язків суб'єктів та характер юридичної відповідальності.

Як зазначає М. Я. Янишівський: «Вплив Акту про ШІ виходить за межі ЄС, формуючи глобальні стандарти регулювання, аналогічно до Загального регламенту про захист даних (GDPR) (European Parliament and Council, 2016), який став світовим еталоном захисту персональних даних. Єврокомісія чітко позиціонує Акт про ШІ як майбутній глобальний стандарт регулювання у цій сфері» [341, с. 110].

Аналізуючи проєкт Закону Європейського Союзу про штучний інтелект, В. Г. Пилипчук, О. А. Баранов та О. С. Гиляка зазначають, що правове регулювання у цій сфері спрямоване на досягнення чотирьох взаємопов'язаних цілей: забезпечення безпечного використання систем штучного інтелекту з дотриманням основоположних прав і цінностей Європейського Союзу; створення правової визначеності для стимулювання інновацій та інвестицій; підвищення ефективності механізмів управління й застосування законодавства щодо захисту прав людини та безпеки під час використання систем ШІ; а також формування єдиного внутрішнього ринку безпечних, надійних і правомірних технологій штучного інтелекту та запобігання його фрагментації [177].

Сам AI Act визначає систему ШІ як програмне забезпечення, яке розроблено з використанням одного або кількох методів і підходів, і може для заданого набору визначених людиною цілей генерувати результати, такі як вміст, прогнози, рекомендації, або рішення, що впливають на середовище, з яким вони взаємодіють [353].

Крім того, пп. б ч. 2 ст. 5 встановлює, що використання правоохоронними органами систем ШІ для біометричної ідентифікації має відповідати принципам необхідності та пропорційності, які повинні бути закріплені у національному законодавстві держав-членів. Водночас такі системи, за загальним правилом, підлягатимуть преєстрації у відповідних базах даних систем ШІ згідно з ст. 49

AI Act починаючи з 2 серпня 2026 р.¹. Разом з тим положення ст. 49 AI Act передбачають окремі випадки допуску до експлуатації певних систем ШІ без попередньої реєстрації або під час процедури такої реєстрації, що видається обґрунтованим з огляду на необхідність врахування невідкладних випадків застосування таких систем, зокрема у правоохоронній діяльності.

Щодо високоризикових систем ШІ, AI Act встановлює критерії їх оцінки та висуває спеціальні вимоги до контролюваного використання.

AI Act визначає загальні критерії віднесення систем ШІ до високоризикових у ст. 6, відповідно до якої такими визнаються системи, що створюють значну загрозу здоров'ю, безпеці або основоположним правам людини (ризик дискримінації, свавільного втручання в приватність, позбавлення волі тощо). Саме це обґрунтовує встановлення підвищених вимог до якості даних, прозорості, людського контролю й управління ризиками.

Зазначені критерії застосовуються до систем ШІ, перелічених у Додатку III AI Act, з урахуванням потенційної шкоди для здоров'я, безпеки чи фундаментальних прав.

Ризик-орієнтований підхід AI Act полягає не лише у встановленні прямих заборон щодо окремих практик використання ШІ, а й у формуванні спеціального правового режиму для високоризикових систем ШІ.

Центральне місце в ризик-орієнтованій моделі AI Act займають високоризикові системи штучного інтелекту, правовий режим яких визначено ст. 6 Регламенту. До них належать, по-перше, системи ШІ, що є компонентами безпеки продукції, яка підлягає обов'язковій оцінці відповідності відповідно до законодавства ЄС, а по-друге, системи, призначені для використання у сферах, визначених Додатком III, зокрема у біометричній ідентифікації, критичній інфраструктурі, освіті, трудових відносинах, правоохоронній діяльності, правосудді та демократичних процесах. Крім того, компетентні органи держав-членів можуть віднести до високоризикових й інші системи, якщо їх

¹ Ст. 49 «Реєстрація» AI Act, в свою чергу, набирає чинності 2 серпня 2026 р.

використання створює значний ризик для життя, здоров'я чи фундаментальних прав людини [353].

Юридичне значення цієї класифікації полягає в тому, що саме вона визначає обсяг адміністративно-правових вимог, які застосовуються до відповідної системи III. На відміну від заборонених практик, для високоризикових систем Регламент встановлює спеціальний режим правового регулювання, який охоплює весь життєвий цикл системи – від її проєктування до післяринкового моніторингу.

Механізм такого регулювання базується на сукупності взаємопов'язаних адміністративно-правових інструментів. Його процедурний елемент охоплює систему управління ризиками, оцінку відповідності, постринковий моніторинг та безперервний людський нагляд (human oversight). Останній є однією з ключових гарантій законного використання високоризикових систем, оскільки передбачає обов'язок розробників забезпечити можливість своєчасного втручання людини у функціонування системи, виправлення або скасування її рішень, а також мінімізацію ризику безкритичного покладання на автоматизовані рішення (automation bias). Таким чином, AI Act закріплює принцип, за яким остаточний контроль у сферах, що можуть впливати на права людини, повинен залишатися за людиною.

Інформаційно-документаційний елемент механізму включає вимоги до управління даними, ведення технічної документації, логування роботи системи та забезпечення прозорості її функціонування. Ці інструменти створюють можливість простежуваності алгоритмічних рішень, здійснення державного контролю та подальшої юридичної оцінки правомірності використання системи III.

Окреме місце займає безпековий елемент механізму, який передбачає встановлення мінімальних вимог до точності, надійності, стійкості до помилок і кіберзагроз, а також обов'язкове тестування систем у різних сценаріях їх функціонування. У такий спосіб AI Act імплементує принцип «безпечності за замовчуванням» (security/safety by design), перетворюючи технічні вимоги на

юридично обов'язкові критерії допуску високоризикових систем до експлуатації.

Водночас ключовим адміністративно-правовим інструментом виступає оцінка відповідності (conformity assessment), яка здійснюється до введення високоризикової системи в обіг. Залежно від категорії системи вона проводиться шляхом внутрішньої оцінки або із залученням нотифікованого органу, що забезпечує незалежну перевірку відповідності системи встановленим вимогам. Саме процедура оцінки відповідності є юридичним механізмом допуску систем штучного інтелекту до ринку Європейського Союзу та одночасно одним із основних інструментів превентивного адміністративного контролю.

Таким чином, правовий режим високоризикових систем III є ключовим елементом механізму адміністративно-правового регулювання, оскільки саме через нього реалізується ризик-орієнтований підхід AI Act. Класифікація систем за рівнем ризику визначає інтенсивність державного нагляду, зміст адміністративних процедур, обсяг обов'язків суб'єктів та систему юридичних гарантій, спрямованих на забезпечення безпечного, прозорого й правомірного використання штучного інтелекту.

Ризик-орієнтована модель AI Act передбачає, що правовий статус суб'єктів створення та використання високоризикових систем штучного інтелекту визначається не лише їх роллю у життєвому циклі системи, а й обсягом покладених на них адміністративно-правових обов'язків. Основними суб'єктами такого регулювання виступають постачальники (providers), розгортачі (deployers), нотифіковані органи (notified bodies), компетентні національні органи та Офіс ЄС з питань штучного інтелекту (AI Office), кожен з яких виконує визначені функції у механізмі забезпечення законного та безпечного використання систем штучного інтелекту (ст. 3, ст.ст. 28–39, 64–78 AI Act).

Центральне місце у цьому механізмі займає постачальник високоризикової системи III, на якого покладається обов'язок забезпечити

відповідність системи вимогам Регламенту до її введення в експлуатацію (ст.ст. 16–21 AI Act). Реалізація цього обов'язку здійснюється через процедуру оцінки відповідності (conformity assessment), яка проводиться відповідно до ст.ст. 43–48 AI Act. За результатами такої процедури складається Декларація про відповідність ЄС (EU Declaration of Conformity) (ст. 47) та наноситься СЕ-маркування (ст. 48), що підтверджує відповідність системи встановленим вимогам і є юридичною підставою для її допуску на ринок Європейського Союзу. Таким чином, оцінка відповідності виступає ключовим процедурним елементом механізму адміністративно-правового регулювання, який забезпечує превентивний контроль безпечності систем штучного інтелекту.

Важливим елементом цього механізму є також реєстрація високоризикових систем ШІ в базі даних ЄС, що здійснюється відповідно до ст.ст. 49–50 AI Act. Така реєстрація забезпечує ідентифікацію систем, їх простежуваність та інформаційну відкритість, створюючи умови для здійснення державного нагляду, ринкового контролю та громадського моніторингу.

Адміністративно-правові обов'язки постачальників не припиняються після введення системи в обіг. Відповідно до ст.ст. 72–73 AI Act вони зобов'язані забезпечувати післяринковий моніторинг (post-market monitoring), здійснювати аналіз функціонування системи, оновлювати технічну документацію та повідомляти компетентні органи й AI Office про серйозні інциденти або порушення вимог Регламенту. Такий підхід свідчить про перехід від одноразової процедури сертифікації до моделі безперервного адміністративного нагляду протягом усього життєвого циклу системи ШІ.

Окремим елементом механізму правового регулювання є оцінка впливу на фундаментальні права (Fundamental Rights Impact Assessment, FRIA), проведення якої передбачено ст. 27 AI Act для окремих категорій розгортачів високоризикових систем штучного інтелекту, насамперед у сферах правосуддя, правоохоронної діяльності, міграції, освіти, працевлаштування та соціального забезпечення. Проведення такої оцінки забезпечує інтеграцію стандартів захисту прав людини у процес прийняття адміністративних рішень щодо

використання систем штучного інтелекту та є однією з ключових гарантій людиноцентричного підходу, закладеного в AI Act.

Поряд із постачальниками самостійний адміністративно-правовий статус мають розгортачі (deployers) високоризикових систем ШІ. На відміну від традиційної моделі, де користувач виступає лише споживачем технології, AI Act покладає на нього комплекс самостійних обов'язків щодо безпечної експлуатації системи (ст. 26, ст. 29). До них належать забезпечення використання системи відповідно до її призначення, здійснення людського нагляду (human oversight), моніторинг функціонування системи, ведення журналів (logs), повідомлення про серйозні інциденти, взаємодія з постачальником та дотримання вимог законодавства про захист персональних даних. Таким чином, розгортач стає повноцінним учасником механізму адміністративно-правового регулювання та несе самостійну відповідальність за правомірність використання системи ШІ.

Особливий правовий режим встановлено для органів публічної влади, які використовують високоризикові системи штучного інтелекту. Відповідно до ст. 27 та ст. 30 AI Act вони зобов'язані проводити оцінку впливу на фундаментальні права до впровадження таких систем, забезпечувати прозорість їх використання, а у визначених випадках — організовувати консультації із заінтересованими сторонами. Це свідчить про те, що застосування штучного інтелекту у публічному управлінні розглядається Регламентом як об'єкт підвищеного адміністративного та суспільного контролю.

Таким чином, AI Act формує комплексний механізм адміністративно-правового регулювання високоризикових систем штучного інтелекту, у якому правовий статус суб'єктів безпосередньо пов'язаний із їх функціями на різних етапах життєвого циклу системи. Постачальники забезпечують відповідність і безпечність систем (ст.ст. 16–21), розгортачі — їх правомірне використання (ст.ст. 26–29), компетентні органи та AI Office здійснюють державний нагляд (ст.ст. 64–78), а процедури оцінки відповідності (ст.ст. 43–48), реєстрації (ст.ст. 49–50), післяринкового моніторингу (ст.ст. 72–73) та оцінки впливу на

фундаментальні права (ст. 27) утворюють взаємопов'язану систему адміністративно-правових засобів, спрямованих на мінімізацію ризиків і забезпечення захисту прав людини [353].

AI Act формує нову систему суб'єктів організаційно-правового забезпечення, до якої входять: Офіс Штучного Інтелекту (AI Office); Європейська рада зі штучного інтелекту; Національні компетентні органи нагляду. Для України імплементація цієї моделі означає потребу у створенні аналогічного національного органу нагляду за ШІ, який би забезпечував незалежний моніторинг і аудит алгоритмів

Ю. І. Тюрє водночас логічно звертає увагу на одне із дискусійних питань аналізованого нормативного документа щодо його екстериторіальності. Однією з ключових проблем сучасного правового регулювання використання штучного інтелекту є визначення меж територіальної юрисдикції відповідних нормативних актів. Стрімкий розвиток цифрових технологій зумовлює ситуацію, за якої розробники, постачальники та користувачі систем ШІ можуть перебувати у різних державах, тоді як наслідки їх функціонування виникають на території іншої юрисдикції [259, с. 253-254].

За таких умов надмірно вузький територіальний підхід істотно знижує ефективність правового регулювання, створює можливості для обходу встановлених вимог та ускладнює захист прав осіб, на яких впливає використання систем штучного інтелекту. Водночас надмірне поширення юрисдикції на іноземних суб'єктів може породжувати колізії із принципом державного суверенітету та міжнародної юрисдикції. У зв'язку з цим визначення територіальної сфери дії законодавства набуває значення одного з ключових елементів механізму адміністративно-правового регулювання, оскільки саме від нього залежить коло суб'єктів, на яких поширюються адміністративно-правові обов'язки, контрольні повноваження компетентних органів та механізми юридичної відповідальності. Саме тому AI Act застосовує екстериторіальний підхід, поширюючи окремі вимоги не лише на суб'єктів, зареєстрованих у державах-членах ЄС, а й на постачальників і розгортачів

систем штучного інтелекту з третіх країн, якщо результати функціонування таких систем використовуються на території Європейського Союзу.

Підсумовуючи викладене, слід зауважити, що AI Act фактично сформував нову модель адміністративно-правового механізму регулювання ШІ, яка складається з:

- ризик-орієнтованого елемента (класифікація систем);
- процедурного (оцінка ризиків, оцінка відповідності, людський нагляд);
- контрольно-наглядового (державний нагляд, аудит, постринковий моніторинг);
- інформаційного (технічна документація, логування, прозорість);
- гарантійного (захист прав людини, можливість людського втручання, відповідальність).

Таким чином, європейська парадигма правового регулювання ШІ еволюціонувала від фрагментарних підходів до робототехніки та Інтернету речей до комплексної моделі заборон і обмежень, закріпленої в AI Act як акті «керованого ризику» для систем ШІ. У системі правового регулювання AI Act визначається як ключовий інструмент переходу від інструментів «м'якого права» (soft law) до імперативних законодавчих механізмів («жорсткого права»). Крім того, на відміну від міжнародних декларацій (наприклад, Резолюції ГА ООН A/78/L.49, що є лише «політичним сигналом»), AI Act є Регламентом, який має пряму дію та є обов'язковим для виконання у всіх державах-членах ЄС. Він виступає першим у світі комплексним нормативним актом щодо ШІ.

Послідовне формування режимів відповідальності, людського й технічного контролю, вимог до страхування, інклюзії, кібербезпеки, якості даних, прозорості, людського нагляду та післяринкового моніторингу перетворює високоризикові системи ШІ з експериментальної технології на особливий об'єкт правового регулювання, допуск якого на ринок жорстко пов'язується з гарантіями безпеки людини, суспільства та довкілля.

У такій логіці особливої актуальності набуває подальше дослідження

обмежень використання ІІІ насамперед у найбільш чутливих сферах: автономної зброї, медицини, правоохоронної діяльності, правосуддя та освіти, адже саме у них поєднуються максимальний потенціал користі з найбільш руйнівними ризиками.

Спектр ризиків у зазначених сферах коливається від загроз існуванню людства та окремої людини до підриву довіри до правосуддя й масового порушення фундаментальних прав людини. Тому європейський підхід, який послідовно вибудовує модель «заборон – високого ризику – керованої автономії», потребує подальшого поглибленого аналізу з метою окреслення чітких і науково обґрунтованих меж допустимості використання ІІІ у кожній із таких сфер.

Для України ці підходи мають щонайменше чотири ключові виміри, оскільки вони:

1) надають концептуальну матрицю для побудови власної політики обмеження використання ІІІ – від виокремлення неприйнятних практик до створення спеціальних режимів для високоризикових систем і запровадження процедур оцінки впливу на права людини;

2) встановлюють регуляторні «маячки», без урахування яких інтеграція України до європейського цифрового ринку буде істотно ускладнена. Зокрема, це стосується необхідності адаптації законодавства у сферах медицини, освіти, правосуддя, правоохоронної діяльності, фінансових послуг і критичної інфраструктури до вимог AI Act;

3) дають змогу уникнути спокуси формувати політику у сфері ІІІ виключно навколо технологічних і економічних параметрів, без урахування аксіологічного і правозахисного вимірів, які, як було показано в розділі 1, є визначальними для легітимності будь-яких рішень у цій сфері.

4) виступають методологічним орієнтиром: Національна стратегія (згідно з «Білою книгою») передбачає спочатку «м'який» підхід (bottom-up), щоб підготувати бізнес, із подальшим ухваленням закону-аналога європейського AI Act до кінця 2026 року.

У межах нормативної інфраструктури Європейського Союзу, з якою кореспондує AI Act, особливе значення мають акти, що регулюють функціонування інформаційних систем у сферах міграції, прикордонного контролю, безпеки та правоохоронної діяльності. Їх розвиток відбувався поступово та супроводжувався ухваленням як базових регламентів, так і подальших змін до них, спрямованих на підвищення ефективності обробки даних і взаємодії між системами.

Так, у сфері функціонування Візової інформаційної системи (VIS) важливим етапом стало внесення змін до базового Регламенту (ЄС) № 767/2008, а також пов'язаних з ним актів – Регламенту (ЄС) № 810/2009 (Візовий кодекс), Регламенту (ЄС) 2017/2226 (EES) та Регламенту (ЄС) 2016/399 (Шенгенський кодекс про кордони). У цьому контексті значення має Пропозиція Регламенту Європейського Парламенту і Ради COM(2018) 302 final, яка передбачала модернізацію VIS, розширення обсягу даних, що обробляються, а також посилення зв'язків із іншими інформаційними системами ЄС.

Окремий напрям становить розвиток системи Eurodac, створеної для порівняння біометричних даних осіб, які подають заяви про надання притулку або незаконно перебувають на території ЄС. У цьому контексті важливою є змінена пропозиція щодо Регламенту Європейського Парламенту і Ради про створення оновленої системи Eurodac, яка передбачає розширення її функціоналу [470; 471], зокрема використання даних не лише для цілей надання притулку, але й для ідентифікації осіб та забезпечення правоохоронної діяльності, включаючи доступ до даних для Європолу та компетентних органів держав-членів.

У сфері прикордонного контролю ключовим актом є Регламент (ЄС) 2017/2226 Європейського Парламенту і Ради від 30 листопада 2017 року, який запровадив систему в'їзду/виїзду (EES). Ця система передбачає електронну реєстрацію даних про в'їзд і виїзд громадян третіх країн, а також фіксацію випадків відмови у в'їзді, що дозволяє підвищити ефективність контролю за

дотриманням правил перебування на території ЄС і посилити безпекову складову прикордонної політики.

Важливим елементом цифрової інфраструктури ЄС є Європейська система інформації та авторизації подорожей (ETIAS), створена відповідно до Регламентів (ЄС) 2018/1240 та 2018/1241 Європейського Парламенту і Ради від 12 вересня 2018 року. Її функціонування спрямоване на попередню перевірку осіб, які подорожують до ЄС без віз, із метою виявлення потенційних ризиків для безпеки, міграційної політики та громадського порядку.

У сфері кримінально-правового співробітництва значну роль відіграє Регламент (ЄС) 2019/816 Європейського Парламенту і Ради від 17 квітня 2019 року, який передбачає створення системи ECRIS-TCN для централізованого обліку інформації про судимості громадян третіх країн. Ця система забезпечує швидкий доступ до інформації про кримінальне минуле осіб і сприяє підвищенню ефективності судової та правоохоронної взаємодії між державами-членами.

Важливим напрямком розвитку цифрової архітектури ЄС стало також ухвалення Регламентів (ЄС) 2019/817 та 2019/818 Європейського Парламенту і Ради від 20 травня 2019 року, які заклали основу для взаємодії (інтероперабельності) інформаційних систем ЄС у сферах кордонів, віз, міграції, а також поліцейської та судової співпраці. Запровадження інтероперабельності дозволяє забезпечити обмін даними між різними системами, підвищуючи їх ефективність і знижуючи ризики фрагментації інформаційного простору.

Таким чином, зазначені акти формують цілісну нормативну основу функціонування інформаційних систем Європейського Союзу, у межах якої AI Act виступає як інструмент інтеграції штучного інтелекту у вже існуючу цифрову та правову інфраструктуру. Це свідчить про міжсекторальний характер регулювання ШІ та його органічне включення у систему безпеки, міграційної політики та управління даними в ЄС.

Проаналізовані міжнародні акти ООН демонструють, що глобальна інформаційно-правова політика тривалий час розглядала ІКТ як універсальний інструмент досягнення цілей сталого розвитку, фокусуючись на подоланні цифрової нерівності, забезпеченні доступу до технологій та класичних інформаційних загроз, але не виокремлюючи штучний інтелект як самостійний об'єкт безпекового регулювання. Це зумовило ситуацію, за якої ШІ фактично «розчинився» в загальному секторі ІКТ, а механізми його безпечного впровадження на універсальному рівні залишилися нерозробленими, попри очевидне визнання переваг ШІ над когнітивними можливостями людини та пов'язаних із цим ризиків.

На відміну від універсального рівня, правова політика Ради Європи та Європейського Союзу вже сьогодні формує системну, ціннісно орієнтовану модель упереджувального регулювання алгоритмічних систем і штучного інтелекту, в центрі якої перебувають права людини, демократія, верховенство права та етика відповідального впровадження технологій. Рекомендації з етики для надійного ШІ, Рекомендація CM/Rec(2020)1 щодо впливу алгоритмічних систем на права людини, а також подальші акти Європейського Союзу (від етичних резолюцій до AI Act) закріплюють поетапний підхід: від формування принципів і настанов – до встановлення конкретних зобов'язань для держав, суб'єктів приватного сектору, інституцій нагляду та розвитку постійного суспільного діалогу щодо ризиків і наслідків застосування ШІ.

В умовах євроінтеграційних процесів України саме європейська модель правового регулювання безпечного ШІ має виступати орієнтиром для розвитку національного законодавства, з огляду на необхідність гармонізації підходів до етики, безпеки та захисту прав людини. При визначенні моделі правовідносин між виробниками, провайдерами, користувачами та державою ключового значення набуває чітке закріплення правосуб'єктності учасників, окреслення меж допустимого та недопустимого застосування ШІ, а також імплементація принципів ризик-орієнтованого регулювання як основи формування узгодженої з правом Європейського Союзу національної правової політики.

У цьому контексті особливої уваги потребує визначення структури відповідних правовідносин, у межах яких об'єктом виступають системи штучного інтелекту, а зміст охоплює права та обов'язки суб'єктів щодо їх розроблення, впровадження та використання. Водночас необхідним є нормативне визначення сфер застосування ІІІ з урахуванням тих із них, у яких його використання є недопустимим або підлягає спеціальним обмеженням.

Важливо, що європейський підхід не зводиться до загального заклику щодо етичного використання ІІІ, а передбачає нормативне узгодження трьох ключових площин: визначення видів застосування ІІІ, які суперечать базовим правам людини та підлягають прямій забороні; формування детального регуляторного режиму для систем високого ризику із встановленням вимог до управління ризиками, якості даних, технічної та організаційної безпеки, прозорості, нагляду та відповідальності; застосування більш гнучкого підходу до систем, ризик яких для прав людини є обмеженим або мінімальним.

2.2. Правовий статус суб'єктів створення, впровадження та використання штучного інтелекту

Проблема правосуб'єктності у правовідносинах, пов'язаних із використанням ІІІ, є однією з найбільш дискусійних та концептуально складних у сучасній юридичній науці. Її актуалізація зумовлена не лише стрімким розвитком цифрових технологій, а й трансформацією моделей взаємодії між людиною, державою та високоавтономними цифровими системами, які дедалі частіше виконують функції, що традиційно були властиві класичним суб'єктам права.

Систематизуючи доктринальні підходи до розуміння правосуб'єктності [68], А. В. Денисова пропонує оцінювати цю категорію крізь призму двох ключових методологічних напрямів: структурно-логічного, який ґрунтується на аналізі її елементів, та діалектичного, що розглядає правосуб'єктність як динамічне правове явище, пов'язане зі здатністю суб'єкта набувати прав,

реалізовувати їх і нести юридичну відповідальність [69, с. 146]. Такий підхід має важливе методологічне значення для дослідження правового статусу суб'єктів створення, впровадження та використання систем штучного інтелекту.

У юридичній науці категорія «правовий статус» розглядається як універсальна характеристика суб'єкта правовідносин, що визначає його місце у системі суспільних відносин, міру юридично можливої поведінки, а також обсяг прав, обов'язків і повноважень [158, с. 8]. Відмінності правового статусу окремих суб'єктів зумовлюються їх функціональним призначенням і роллю у відповідній системі правовідносин, що визначає межі реалізації наданих їм законом можливостей.

На думку О. В. Зайчука та Н. М. Оніщенко, правовий статус є законодавчо визначеною та гарантованою державою системою прав, свобод, законних інтересів і обов'язків суб'єкта суспільних відносин. Його характерними ознаками є універсальність, індивідуалізація, системність і взаємозв'язок з іншими елементами правового регулювання. Залежно від характеру та кола суб'єктів правовий статус поділяється на загальний, галузевий, спеціальний та індивідуальний [99, с. 366]. Такий підхід є методологічною основою для визначення правового статусу суб'єктів створення, впровадження та використання систем штучного інтелекту, який, поряд із загальними ознаками, характеризується спеціальними правами, обов'язками та гарантіями, обумовленими особливостями механізму адміністративно-правового регулювання цієї сфери.

При цьому, вчені додають, що відповідно до класифікації за характером правового статусу, загальний правовий статус визначає сукупність основних юридичних властивостей, спільних для всіх суб'єктів права. Галузевий правовий статус конкретизує ці загальні характеристики з урахуванням особливостей окремої сфери правового регулювання та відповідних правовідносин, у зв'язку з чим його нерідко розглядають як різновид спеціального правового статусу. Подальша конкретизація здійснюється на рівні

спеціального та індивідуального статусів, які відображають особливості правового становища окремого суб'єкта. При цьому кожен наступний рівень зберігає ознаки загального та галузевого статусів, водночас доповнюючи їх специфічними правами, обов'язками й повноваженнями, що визначають унікальне правове становище конкретного суб'єкта [55, с. 33].

А. О. Москаленко зауважує: «Як і стосовно правового статусу, поширеною думкою серед науковців є визначення адміністративно-правового статусу як сукупності конкретно визначених суб'єктивних прав і обов'язків, яких закріплено за відповідним суб'єктом нормами адміністративного права» [158, с. 185]. Х. П. Ярмачі обґрунтовує, що структура правового статусу будь-якого державного органу охоплює його завдання, функції, повноваження (права та обов'язки), а також юридичну відповідальність, які у сукупності визначають місце та роль відповідного органу в механізмі державного управління [343, с. 315]. Для визначення правового статусу суб'єктів публічного адміністрування у сфері використання штучного інтелекту, оскільки їх місце у механізмі адміністративно-правового регулювання визначається не лише сукупністю повноважень, а й спеціальними функціями щодо управління ризиками, здійснення нагляду, контролю та забезпечення дотримання прав людини під час створення, впровадження й використання систем штучного інтелекту.

У зв'язку з цим правовий статус відповідних суб'єктів визначається не лише їх місцем у системі правовідносин, а й функціональною роллю на етапах створення, впровадження, використання, контролю та припинення експлуатації систем ШІ. З огляду на це правовий статус суб'єктів створення, впровадження та використання систем штучного інтелекту доцільно розглядати як спеціальний галузевий правовий статус, що поєднує загальні елементи адміністративно-правового статусу із спеціальними правами, обов'язками та гарантіями, обумовленими ризик-орієнтованою моделлю правового регулювання використання штучного інтелекту.

Сучасні підходи до визначення правового статусу ШІ є плюралістичними та безпосередньо зумовлюються домінуючими уявленнями про природу,

онтологічний статус, функціональне призначення й еволюційні перспективи цього феномену. На доктринальному рівні його розуміння формується переважно у межах двох фундаментальних аспектів:

- як операційної спроможності, «що надається алгоритмами оптимального або неоптимального вибору з широкого простору можливостей, для досягнення цілей шляхом застосування стратегій, які можуть спиратися на навчання або адаптацію до навколишнього середовища»;

- як штучно сконструйованих систем, що «діють у фізичному або цифровому світі, враховують складну мету і обирають найкращі дії (відповідно до заздалегідь визначених параметрів), які необхідно виконати для досягнення поставленої мети на основі сприйняття свого середовища, інтерпретації зібраних структурованих або неструктурованих даних та обґрунтування знань, отриманих з цих даних» [238].

Концептуалізація ІІІ як високотехнологічної системи, здатної на основі моделювання когнітивної архітектури людського мислення генерувати та реалізовувати релевантні рішення, відкриває нові теоретико-методологічні можливості для оцінки його сутнісної ролі у правовідносинах. Зокрема, це створює підґрунтя для дискусії щодо потенційної інтеграції ІІІ у юридичну реальність у статусі нетипового (квазісуб'єктного) учасника правових зв'язків.

У загальній теорії права правосуб'єктність традиційно дефініюється як юридична здатність особи виступати повноправним учасником правовідносин [8, с. 578]. Зазначена категорія є інтегративною юридичною властивістю суб'єкта, що поєднує правоздатність, дієздатність та деліктоздатність. Водночас специфічні онтологічні характеристики ІІІ унеможливають механічне перенесення цього класичного тринітарного підходу. Правосуб'єктність інтелектуальних агентів не є і не може бути тотожною правосуб'єктності фізичних чи юридичних осіб, сформованій у межах класичної правової доктрини [29 с. 85]. Така відмінність зумовлена як відсутністю у ІІІ автономної правової волі та здатності до самостійного цілепокладання, так і його технічною природою як створеної людиною технічної системи.

З іншого боку, абсолютизація інструментального підходу, який зводить ІІ до статусу звичайної «машини» чи пасивного технічного об'єкта, вступає у суперечність із сутнісною природою інтелектуальних систем. Здатність ІІ до автономного ухвалення рішень та здійснення дій, що мають юридично значущі наслідки, актуалізує доктринальну потребу у формуванні специфічних моделей його правосуб'єктності.

У такий спосіб проблема юридичного статусу ІІ безпосередньо пов'язується з розподілом деліктної відповідальності між його розробниками, постачальниками та кінцевими користувачами. Автономність функціонування таких систем, попри їх високу прагматичну ефективність, породжує ризики як локального, так і глобального характеру. Найбільш виразно це проявляється у випадках автономного ухвалення алгоритмічних рішень, які прямо або опосередковано вступають у суперечність із вимогами безпеки людини, суспільними інтересами чи загальним правопорядком.

Вагоме доктринальне значення для рефлексії юридичної природи ІІ має концепція О. А. Баранова, який обґрунтовує необхідність визнання роботів із ІІ суб'єктами права на основі їхньої здатності здійснювати дії, подібні до людських, що породжують юридично значущі наслідки [14]. Дослідник аргументує необхідність парадигмального переходу від класичного «об'єктного» статусу технологій до «суб'єктного» або гібридного виміру щодо окремих категорій інтелектуальних робототехнічних комплексів

Зазначена вітчизняна доктринальна позиція узгоджується з домінуючими тенденціями глобального наукового дискурсу, у межах якого активно розробляється концепція «гібридного інтелекту» (Hybrid Intelligence). Зокрема, представники нідерландської наукової школи (З. Аката, Ф. ван Хармелен та ін.) акцентують на синергетичній когнітивній взаємодії людини та ІІ [269, с. 18]. Такий міждисциплінарний підхід дає вагомі підстави інтерпретувати правосуб'єктність інтелектуальних агентів не як ізольовану онтологічну властивість алгоритмічної системи, а як динамічний елемент моделі розподіленої відповідальності.

У цьому ж дослідницькому напрямі перебуває методологічно значуща концепція «відповідального штучного інтелекту», обґрунтована В. Дігнам (Virginia Dignum). Дослідниця акцентує на необхідності впровадження принципів підзвітності, прозорості та етичності на всіх етапах життєвого циклу інтелектуальних систем [357, р. 45]. Зазначений деонтологічний підхід дозволяє інтерпретувати *правосуб'єктність III не як статичну абстрактну категорію, а як динамічний прагматичний механізм мінімізації технологічних ризиків та превенції шкоди шляхом чіткого нормативного закріплення обов'язків за всіма суб'єктами, які взаємодіють із технологією.*

Зазначені доктринальні підходи дістали відображення й на міжнародному нормативно-правовому рівні. Показовим прикладом є Резолюція Європейського парламенту від 16 лютого 2017 року з рекомендаціями Комісії щодо цивільно-правових норм у сфері робототехніки (2015/2103(INL)) [355] (далі – Резолюція про цивільно-правові норми в робототехніці). У цьому акті безпосередньо констатується, що «автономність робота можна визначити як здатність ухвалювати рішення і реалізовувати їх у зовнішньому середовищі незалежно від зовнішнього контролю або впливу» (п. АА) [355]. Водночас у документі акцентується, що «така автономія має суто технологічний характер, а її ступінь залежить від того, наскільки складною є взаємодія робота з навколишнім середовищем» [355].

У теоретико-правовому вимірі це означає, що автономність III виступає виключно його функціонально-операційною характеристикою, параметри якої закладаються на етапі архітектурного проєктування. Відповідно, різні моделі інтелектуальних систем характеризуються різним рівнем операційної самостійності – від часткової (інструментальної) до високої. Відтак формулювання «незалежність від зовнішнього контролю або впливу» слід інтерпретувати не як прояв суверенної правової волі, а як техніко-технологічну здатність цифрової системи, межі функціонування якої визначаються її розробником та/або оператором.

Аналізуючи сучасні підходи до визначення правового статусу штучного

інтелекту, Б. С. Щербина та В. В. Ткаченко доходять висновку про концептуальну аморфність його правосуб'єктності у межах сучасної юридичної доктрини, де інтелектуальні системи переважно кваліфікуються як традиційні об'єкти права. Зіставляючи потенційні модуси правосуб'єктності ШІ з класичними моделями фізичних та юридичних осіб, автори констатують, що домінуючі доктринальні підходи фактично редукують інтелектуальних агентів до об'єктного статусу у правовідносинах [246, с. 143-145].

Водночас, з метою подолання лінійної об'єктивізації технологій та забезпечення послідовного теоретичного аналізу, зазначені дослідники пропонують диференційовану класифікацію ШІ, виокремлюючи: новостворений штучний інтелект; несамотійний штучний інтелект; незалежний штучний інтелект [246, с. 144].

Побудова цієї тріадичної моделі здійснюється дослідниками за допомогою методологічної аналогії з еволюційними етапами розвитку цивільної дієздатності фізичної особи (від малолітніх до повнолітніх суб'єктів). З огляду на іманентну здатність сучасних систем ШІ до машинного самонавчання, кумулятивного накопичення емпіричного досвіду та автономної генерації моделей ухвалення рішень, запропонована класифікаційна матриця має значний теоретико-прикладний потенціал і потребує подальшого правового осмислення.

Динамічні етапи генезису та функціонального розгортання штучного інтелекту, незалежно від хронологічної тривалості його когнітивної підготовки та попередньо визначеного рівня готовності до повноцінного функціонування, можуть бути системно типізовані таким чином: архітектурне моделювання (створення); активація та верифікація (введення в експлуатацію); первинне машинне навчання; цільове функціонування (включаючи рекурсивне самонавчання та алгоритмічну оптимізацію); деактивація та виведення з експлуатації.

Водночас, на наше переконання, процес навчання та накопичення емпіричного досвіду ШІ виступає його іманентною функціональною

характеристикою, яка об'єктивується безпосередньо з моменту його активації. З огляду на це, вбачається доктринально обґрунтованим розмежовувати операційно-функціональну самостійність системи та градієнт її фактичної автономності у процесах ухвалення рішень.

У зв'язку з цим вважаємо за доцільне дефініювати штучний інтелект, який перебуває на стадії інституційного навчання та підготовки до автономного функціонування, як неавтономний ШІ, тобто такий, *що функціонує виключно під телеологічним контролем з боку людини, і який виключає його самостійну правосуб'єктність*.

Отже, стадія інституційного навчання не детермінує іманентну автономність ШІ, а лише формує когнітивні предумови для її подальшої функціональної реалізації.

Етап допуску інтелектуального агента до цільового функціонування (який метафорично зіставляється з «повноліттям» фізичної особи) зазначені дослідники маркують як фазу «незалежного» ШІ, беруть за методологічну основу модель повної цивільної дієздатності фізичної особи. Проте стосовно ШІ така конструкція не може бути механічно перенесена в юридичну площину, оскільки абсолютне «незалежне» функціонування цифрових систем – тобто таке, що здійснюється поза будь-яким контролем з боку людини, – є апріорі неприйнятним з огляду на імперативи національної та глобальної безпеки. Водночас інтелектуальний агент, перебуваючи під стратегічним наглядом людини, вже володіє верифікованим масивом знань і здатний здійснювати автономне операційне функціонування.

З огляду на викладене, розглядаємо ШІ як автономну інтелектуальну систему, здатну виконувати поставлені завдання під системним наглядом людини, але без її безпосереднього покрокового керування.

За умови впровадження запропонованого авторського розмежування на неавтономний та автономний ШІ теоретико-правові параметри його потенційного статусу набувають вищого рівня доктринальної визначеності. Це, своєю чергою, забезпечує чітке окреслення меж розподіленої відповідальності

за проєктування, експлуатацію та негативні наслідки функціонування ШІ, зокрема у випадках заподіяння деліктної шкоди.

Проте означена специфікація функціональної автономності жодним чином не свідчить про доктринальну можливість інтерпретувати ШІ як повноцінного суверенного суб'єкта права. Навпаки, навіть найвищий рівень операційної автономності ШІ не є тотожним його правовій самостійності. Безперервний людський нагляд і можливість втручання (*human oversight*) виступають імперативним критерієм легітимності та допуску інтелектуальних систем до ринку у межах сучасної людиноцентричної європейської правової парадигми [359; 349; 354; 369].

Вчені зазначають, що концепція наділення систем штучного інтелекту правоздатністю як складовою правосуб'єктності потребуватиме докорінної трансформації існуючої правової парадигми та перегляду положень базових галузей права, які історично сформовані з урахуванням природи людини, її свідомості, волі та здатності нести юридичну відповідальність. У зв'язку з цим більш обґрунтованим видається не прирівнювання систем штучного інтелекту до людини у правовому статусі, а формування спеціального правового режиму, який передбачатиме лише той обсяг прав та обов'язків, що відповідає їх функціональному призначенню та технологічній природі.

Т. П. Попович, продовжуючи цю думку, зауважує, що Наділення систем штучного інтелекту правосуб'єктністю є недоцільним, оскільки право має залишатися антропоцентричним і спрямованим на забезпечення прав та інтересів людини, а не технологій. Пріоритетом сучасного етапу розвитку є формування ефективного механізму правового регулювання використання штучного інтелекту як об'єкта права, заснованого на принципах захисту прав людини, прозорості, відповідальності, недискримінації та людського контролю, що відповідає європейському підходу до регулювання ШІ [180 с. 149].

Теоретико-правові параметри правосуб'єктності штучного інтелекту перебувають у прямій залежності від рівня його операційної автономності та характеру взаємодії між інтелектуальним і вольовим компонентами його

двоєдиної природи. Лише за умови узгодженої взаємодії цих складових інтелектуальний агент може претендувати на статус самостійного суб'єкта права; за такого сценарію деліктний ризик заподіяння шкоди, ініційованої автономним функціонуванням ІІІ, покладається на його розробника (провайдера).

Навпаки, ІІІ, наділений виключно когнітивно-інтелектуальною функцією без автономного волевиявлення, не може визнаватися суверенним суб'єктом права, оскільки оцінка та реалізація результатів його алгоритмічної діяльності залежать від людського суб'єкта – оператора. У межах такого підходу деліктна відповідальність за наслідки експлуатації ІІІ підлягає диференційованому розподілу залежно від причин виникнення шкоди. Зокрема, якщо негативні наслідки зумовлені прихованими дефектами чи архітектурними особливостями алгоритмів ІІІ, відповідальність покладається на розробника; якщо ж шкода виникла внаслідок неправомірного або неналежного використання результатів його функціонування – вона покладається на оператора [41, с. 61].

Інтелектуально-вольовий аспект правосуб'єктності ІІІ передбачає, що в умовах неавтономного (інструментального) функціонування вольовий (цілепокладаючий) компонент опосередковується людиною – оператором або власником, тоді як за цифровою системою зберігається виключно когнітивна функція, що полягає у моделюванні та генерації оптимальних рішень. За таких умов, *доки інтелектуальний агент функціонує в межах безпосереднього контролю з боку людини, він не може визнаватися самостійним суб'єктом правовідносин.*

Правосуб'єктність перебуває у безпосередньому взаємозв'язку з деліктоздатністю суб'єкта. У доктринальному вимірі учасником правовідносин може визнаватися виключно той суб'єкт, який не лише усвідомлює характер власних дій і свідомо керує ними, а й спроможний нести за них юридичну відповідальність. Відтак визначальною ознакою правосуб'єктності виступає здатність інтелектуально оцінювати соціокультурну та правову значущість

своїєї поведінки та її наслідків, зокрема наявність психоемоційного компонента – здатності відчувати вину за вчинене правопорушення.

Згідно з концепцією П. М. Рабіновича, юридична відповідальність виступає специфічною формою соціальної відповідальності, закріпленою у позитивному праві та гарантованою державою як юридичний обов'язок правопорушника зазнати встановлених законом несприятливих наслідків карального чи компенсаційного характеру [220, с. 133]. Соціальна відповідальність визначається як «обов'язок особи оцінити власні наміри та здійснювати вибір поведінки відповідно до норм, що відображають інтереси суспільного розвитку, а у випадку порушення їх – обов'язок звітувати перед суспільством і нести покарання» [117, с.15].

Наведені дефінітивні конструкції характеризуються високим рівнем теоретичної абстракції, оскільки фокусуються передусім на внутрішній оцінці власних намірів індивіда та здійсненні ним свідомого поведінкового вибору. Зазначений вибір реалізується у системі соціальних регуляторів (права, етики, моралі), а порушення правових імперативів зумовлює застосування до правопорушника легітимних санкцій.

З огляду на викладене постає фундаментальне теоретико-правове питання: чи існують на сучасному етапі технологічного розвитку доктринальні підстави поширювати на системи III ознаки самотійного суб'єкта, здатного до внутрішньої аксіологічної оцінки власних інтенцій з позицій суспільних інтересів та до свідомого поведінкового вибору під впливом соціокультурних настанов.

Досліджуючи розмежування та змістове наповнення категорій «цифрова людина», «цифрова особа» та «цифрова особистість», О. І. Харитонova та Є. О. Харитонов розкривають специфіку співвідношення між цифровою особою та цифровою особистістю, зазначаючи, що «електронна особа [в розумінні «цифрова особа», В. В.] – це пристрої (роботи тощо) із високорозвиненим штучним інтелектом, здатні ухвалювати самотійні рішення і незалежно від розробника взаємодіяти з іншими особами» [261, с. 10].

Аналізуючи правову природу та місце цього феномену у системі правовідносин, у сучасному науковому дискурсі, на відміну від позиції О. А. Баранова щодо перспектив визнання правосуб'єктності ШІ як антропоморфного «еквівалента фізичної особи» [13], обґрунтовується пропозиція розглядати роботів із високоавтономним штучним інтелектом («електронних осіб») через конструкцію квазіюридичної особи [261, с. 8].

Вирішення питання щодо доктринальної спроможності та доцільності поширення зазначених підходів на системи ШІ перебуває у прямому зв'язку з аналізом його когнітивно-вольового потенціалу, а відтак виступає визначальним критерієм для встановлення меж його деліктоздатності та інтеграції у систему правовідносин у статусі самостійного суб'єкта.

У цьому контексті *методологічно виправданим вбачається застосування міждисциплінарної аналогії з критеріями юридичної оцінки осудності суб'єкта правопорушення. У межах зазначеного класичного інституту інтелектуальний (здатність усвідомлювати фактичний характер і суспільну небезпеку своїх дій) та вольовий (здатність керувати ними) компоненти у їх нерозривній двоєдності виступають визначальними критеріями встановлення деліктоздатності особи, що підтверджує неможливість визнання суб'єктом права сутності, позбавленої такої психічної та аксіологічної основи.*

Водночас у межах чинного правового регулювання як юридичні особи, так і суверенні держави визнаються повноправними суб'єктами різних галузей права, включно з міжнародним правопорядком. Проте їхня юридична правосуб'єктність у своїй основі базується на людському субстраті – корпоративному чи політичному об'єднанні фізичних осіб.

Штучний інтелект за своєю природою таким об'єднанням не є: він не уособлює ані людину, ані юридичну особу, ані державу чи міждержавне утворення. ШІ є похідним продуктом інтелектуальної діяльності людини і, відповідно, належить до простору штучно створених об'єктів.

З цих методологічних позицій базові характеристики ШІ корелюють з ознаками речі у її класичному цивільно-правовому розумінні, оскільки ця

категорія традиційно охоплює будь-які технологічні артефакти. Відповідно до статті 179 Цивільного кодексу України [187], річчю є предмет матеріального світу, щодо якого можуть виникати цивільні права та обов'язки.

Разом з тим ІІІ є специфічною «інтелектуалізованою річчю», наділеною операційними можливостями аналізу та ухвалення рішень. Однак зазначена здатність повністю визначається математичними алгоритмами, закладеними у систему в процесі її архітектурного проектування людиною. Експлуатація ІІІ також незмінно перебуває у полі безперервного людського нагляду: навіть найвищий рівень операційної автономності не нівелює вимог стратегічного нагляду, що підтверджує відсутність у технології повної правової самостійності.

На цьому тлі постає ключова доктринальна дилема: чи здатна «мисляча річ» (у технологічному вимірі), навіть за умов опосередкованого управління чи стратегічного нагляду з боку людини, володіти атрибутами деліктоздатності?

Відповідь на це питання вимагає ґрунтовного аналізу інтелектуально-вольового критерію деліктоздатності (осудності). Оскільки в основі юридичного інституту осудності лежить здатність суб'єкта усвідомлювати суспільну значущість своїх діянь та вольовим зусиллям керувати ними, редукція волі ІІІ до закладеного програмного коду фактично виключає наявність у нього суб'єктивної сторони правопорушення (вини), перетворюючи будь-яку заподіяну ним шкоду на категорію технічного випадку або делікту його оператора чи розробника.

Відповідно до фундаментальних засад загальної теорії права, вина суб'єкта визначається як нерозривна єдність інтелектуального та вольового моментів, що відображають внутрішнє психічне ставлення особи до вчинюваного нею правопорушення та його наслідків.

Умисна форма вини класично передбачає усвідомлення суб'єктом суспільно небезпечного (протиправного) характеру свого діяння та передбачення можливості або неминучості настання його суспільно небезпечних наслідків (інтелектуальний елемент), поєднані з бажанням чи

свідомим допущенням їх настання (вольовий елемент).

Натомість необережна форма вини (у вигляді злочинної самовпевненості або недбалості) характеризується або передбаченням можливості настання суспільно шкідливих наслідків при легковажному розрахунку на їх відвернення, або непередбаченням такої можливості за наявності обов'язку та можливості їх передбачити.

Екстраполяція зазначеної класичної моделі на сферу високих технологій дозволяє констатувати, що у більшості випадків операційної діяльності ІІІ присутній когнітивний компонент. Це дає підстави для теоретичного припущення, що високоавтономна цифрова система здатна генерувати прогностичні моделі та алгоритмічні рішення, які за своїми функціональними ознаками можуть імітувати інтелектуальний аспект вини.

Водночас штучний інтелект апріорі позбавлений вольового моменту у його доктринально-юридичному розумінні. Зазначений сутнісний компонент не може бути замінений або компенсований алгоритмічно зумовленим «оптимальним рішенням». Юридичні категорії «бажання», «наміру» чи «усвідомленого допущення» нерозривно пов'язані з психоемоційною сферою, рефлексією, інстинктом самозбереження та особистісними потребами біологічного суб'єкта, які за своєю природою не притаманні безтілесним математичним кодам та обчислювальній архітектурі.

Відсутність у систем штучного інтелекту свідомості, волі та здатності до аксіологічного осмислення власної поведінки свідчить про відсутність необхідних передумов для покладення на них самостійної юридичної відповідальності. Алгоритмічні системи не здатні усвідомлювати юридичне значення власних дій, оцінювати їх наслідки та формувати вольове ставлення до них, що є необхідною передумовою деліктоздатності. Саме тому на сучасному етапі розвитку науки й техніки відсутні підстави для визнання штучного інтелекту самостійним суб'єктом юридичної відповідальності.

Якщо архітектура алгоритмічної системи імперативно передбачає заборону певних протиправних дій, штучний інтелект не здатний до їх

інтенційного вчинення. Якщо ж програмний код або функціональне призначення системи цілеспрямовано орієнтовані на протиправну поведінку чи заподіяння шкоди, такий штучний інтелект виступає виключно як інтелектуалізований засіб або високотехнологічне знаряддя вчинення правопорушення, тоді як юридична відповідальність покладається на особу, яка визначила параметри його функціонування, — розробника, оператора чи іншого належного суб'єкта.

Аналогічно, у випадку маніпулятивного використання операційних можливостей ІІІ людиною цифрова система в жодному разі не набуває статусу самостійного суб'єкта делікту; навпаки, внаслідок повної іманентної відсутності суверенної правової волі вона виступає як інструментальний об'єкт правопорушення, що підтверджує її абсолютну неделіктоздатність.

Значно більш відповідним доктринальному розумінню соціальної та юридичної відповідальності у разі заподіяння шкоди охоронюваним законом правам та інтересам є імперативне покладення деліктних зобов'язань на осіб, діяльністю яких така шкода була безпосередньо спричинена. Зазначений підхід покладає відповідальність на розробників (виробників) — у разі допущення архітектурних чи програмних помилок на етапі проєктування та створення ІІІ, а також на власників (операторів) — у випадках некоректного, помилкового або протиправного використання технології, що спричинило шкідливі наслідки.

У цьому контексті показовою є позиція Н. Ткаченка, згідно з якою «соціальна відповідальність бізнесу — є відповідальність компанії (фірми) перед усіма фізичними та юридичними особами, з якими вона має справу в процесі діяльності, і перед суспільством загалом» [255, с.128].

При дослідженні юридичної природи інтелектуальних систем слід акцентувати увагу на тому, що високоавтономний ІІІ за своєю природою здатний виступати потенційним джерелом підвищеної небезпеки. Незалежно від конкретних сфер прагматичного застосування, латентні ризики його функціонування варіюються від незначних технічних ексцесів до масштабного порушення прав і свобод людини, суспільних чи державних інтересів.

У цьому зв'язку доцільним є залучення прогностичного застереження філософа і футуролога Станіслава Лема (Stanisław Lem) про те, що «будь-яка цивілізація включає і те, до чого суспільство прагнуло, і те, чого ніхто не замишляв». Дана теза наочно ілюструє, що прогнозування та моделювання параметрів керованості складних здатних до самонавчання технологічних систем часто мають умовний і відносний характер.

Насамперед модель відповідальності за шкоду, заподіяну джерелом підвищеної небезпеки, ґрунтується на засадах об'єктивного (безвинного) покладення деліктних зобов'язань, де ключовою виступає презумпція протиправності заподіювача. На відміну від презумпції невинуватості, яка становить фундаментальний принцип правового статусу індивіда, зазначений приватно-правовий інститут передбачає покладення правової відповідальності на власника небезпечного об'єкта, доки ним не будуть доведені легітимні підстави звільнення від неї (обставини непереборної сили або умисел потерпілого).

У сучасних юридичних реаліях штучний інтелект кваліфікується як об'єкт права власності, принаймні до моменту потенційного нормативного конструювання його альтернативного правового статусу у майбутньому. Доки системи ШІ перебувають у цивільному обороті як майно, домінуючим залишається засадничий конституційний та цивілістичний принцип «власність зобов'язує». Оскільки високоавтономний ШІ кваліфікується як джерело підвищеної небезпеки, загальний тягар ризиків його експлуатації поширює на його титульного або фактичного володільця дію презумпції відповідальності за негативні наслідки його функціонування.

Базові параметри цивільно-правової відповідальності у цій сфері, абстраговані від філософського аналізу онтологічної правосуб'єктності ШІ, вперше сформульовані на рівні Резолюції Європейського парламенту про цивільно-правові норми в робототехніці (пп. 49–58) [355]. Цей акт у пункті 59 також окреслює стратегічні орієнтири для подальшої законотворчої діяльності Європейської комісії щодо уніфікації регуляторного середовища використання

III

Зокрема, у розділі «Зобов'язання» зазначена Резолюція як ключовий принцип закріплює відповідальність за шкоду, спричинену робототехнічними комплексами. Ця проблематика розглядається як фундаментальна на рівні правопорядку Європейського Союзу, у зв'язку з чим наголошується на формуванні єдиних стандартів «ефективності, прозорості та послідовності в реалізації правової визначеності» на всьому просторі Співтовариства.

У контексті визначення юридичної природи III значущим є доктринальний акцент документа на тому, що покладення відповідальності вимагає доведення самого факту заподіяння шкоди та встановлення безпосереднього причинно-наслідкового зв'язку між автономним функціонуванням робота і шкідливими наслідками для потерпілої сторони. Така модель доказування є додатковим аргументом на користь доктринального підпорядкування систем штучного інтелекту правовому режиму джерел підвищеної небезпеки.

Модель деліктної відповідальності в аналізованому акті розкривається крізь призму ризико-орієнтованого підходу. Такий підхід зміщує регуляторний акцент із суб'єкта, який безпосередньо діяв з необережності, на суб'єкта, що володіє здатністю мінімізувати технологічні ризики та превентивно запобігати негативним наслідкам. Юридична відповідальність має розподілятися пропорційно ступеню програмного контролю над роботом та рівню його операційної автономності. Відповідно, чим вищою є здатність інтелектуального агента до рекурсивного самонавчання та автономного функціонування, тим більшим є обсяг деліктних зобов'язань його розробника або оператора.

У Резолюції (зокрема у загальній логіці оцінки III) простежується принциповий антропоцентричний акцент: на сучасному етапі технологічної еволюції юридична відповідальність за експлуатацію III має покладатися виключно на людського суб'єкта, а не на інтелектуальну систему як технологічний об'єкт.

Як фундаментальні гарантії відшкодування шкоди, заподіяної

інтелектуальними системами, документ передбачає диференційовані моделі обов'язкового страхування, покликані забезпечити покриття потенційних деліктних ризиків у межах усього ланцюга постачання – від розробника до власника чи кінцевого оператора. З цією метою Європейській комісії доручається (п. 59 Резолюції про цивільно-правові норми в робототехніці [355]) забезпечити реалізацію таких нормативних заходів: інституціоналізацію імперативного деліктного страхування для специфічних категорій робототехнічних комплексів за аналогією з правовим режимом страхування володільців наземних транспортних засобів та інших джерел підвищеної небезпеки (пп. «а»); формування та нормативно-правове забезпечення діяльності ефективного компенсаційного фонду (пп. «b»); нормативне закріплення інституту обмеженої відповідальності розробника, програміста, власника або оператора за умови здійснення ними регулярних фінансових внесків до зазначеного компенсаційного фонду або в межах механізмів кооперованого страхування (пп. «с»); доктринальне та прагматичне вирішення питання щодо доцільності заснування уніфікованого компенсаційного фонду для всіх типів інтелектуальних автономних роботів або диференційованих фондів для кожної окремої категорії технологій (пп. «d»); забезпечення прямої каузальної індексації індивідуально визначеного робота з конкретним фондом шляхом створення Загальноєвропейського реєстру роботів з метою повноцінного інформування контрагентів та третіх осіб про правову природу фонду й ліміти його деліктної відповідальності (пп. «e»); формування конструкції спеціального правового статусу для автономних робототехнічних систем у довгостроковій перспективі, включаючи можливість надання найбільш складним автономним системам статусу «електронної особи» у випадках автономного ухвалення алгоритмічних рішень та самостійної взаємодії з третіми особами (пп. «f»).

Особливу увагу у контексті визначення правосуб'єктності ШІ слід приділити концептуальним положенням Резолюції Європейського парламенту від 20 жовтня 2020 року про режим цивільної відповідальності за штучний

інтелект (2020/2014(INL)) [365]. У пункті 5 преамбули цього акта акцентується, що глобальна конкуренція у сфері штучного інтелекту вже триває, і Союз повинен відігравати у ній лідируючу роль, реалізуючи свій науково-технологічний потенціал. Водночас рішуче наголошується, що розвиток технологій не має послаблювати чи підривати рівень захисту користувачів від шкоди, яка може бути заподіяна системами ШІ, що зумовлює необхідність просування уніфікованих європейських стандартів цивільної відповідальності на міжнародному рівні [365].

Згідно з пунктом 7 аналізованого документа, фізичні або віртуальні дії, пристрої чи процеси, які зумовлюються системами штучного інтелекту, технічно можуть виступати прямою або опосередкованою причиною заподіяння шкоди чи збитків, проте майже завжди є результатом того, що конкретний людський суб'єкт створює, розгортає або втручається у роботу цих систем [365].

Зазначена констатація формує підґрунтя для висновку про відсутність доктринальних підстав для надання системам штучного інтелекту самостійної правосуб'єктності, попри збереження дискусійності цього питання у сучасному європейському правовому дискурсі.

Обґрунтування такої консервативної позиції пов'язується з тим, що властивості непрозорості («чорної скриньки»), взаємопов'язаності та автономності систем штучного інтелекту здатні на практиці суттєво ускладнити або навіть унеможливити встановлення конкретних алгоритмічних рішень, що спричинили шкоду, а також встановлення причинного зв'язку між ними та конкретним людським втручанням або рішеннями, ухваленими на етапі архітектурного проєктування [365].

З метою нівелювання та превенції зазначених потенційних ризиків аналізований акт закріплює такі концептуальні підходи: безальтернативне покладення деліктних зобов'язань на оператора системи (пп. 11–13); диференціація правил цивільно-правової відповідальності залежно від градації ризику (ризико-орієнтований вектор) (пп. 14–22); інституціоналізація

спеціальних механізмів страхування в ландшафті експлуатації систем штучного інтелекту (пп. 23–25).

Отже, Резолюція Європейського парламенту від 20 жовтня 2020 року про режим цивільної відповідальності за штучний інтелект (2020/2014(INL)) фактично ставить під сумнів можливість визнання правосуб'єктності ШІ на сучасному етапі цивілізаційного розвитку. Така позиція обґрунтовується високим рівнем ризику відчуження або повної втрати людського контролю над автономним функціонуванням інтелектуальних систем, зокрема на стадії архітектурного проєктування та розробки коду.

Ключовим для системного осмислення можливості визнання правосуб'єктності ШІ виступає фундаментальне розуміння сутності права як соціокультурного феномену та сукупності загальнообов'язкових норм, покликаних регулювати виключно суспільні відносини – передусім соціальні зв'язки між людьми.

Відтак ШІ не може володіти правосвідомістю як специфічною формою усвідомлення правової реальності, а отже – у жодному з можливих сценаріїв не здатний виступати носієм фундаментальних прав і свобод..

Отже, у межах класичної антропоцентричної парадигми права штучний інтелект не може визнаватися самостійним суб'єктом правовідносин. Виключно людина виступає визначальним елементом правового регулювання незалежно від специфіки юридичних конструкцій, через які реалізується її правова воля: безпосередньо як фізична особа, опосередковано через корпоративні інституції (юридичні особи) та спеціальні правові статуси або на рівні публічно-владних утворень (держав та їх кооперованих союзів).

У цьому контексті вагоме значення для критичного переосмислення техноутопічних уявлень мають напрацювання David Mindell, який у межах дослідження еволюційних перспектив ШІ виокремив три фундаментальні «міфи» технологічного поступу [Mindell, p. 72]

1) міф про лінійний прогрес – помилкове припущення про те, що еволюція технологій рухається лінійною траєкторією: від жорсткого

покрокового керування людиною до абсолютно автономних кіберфізичних систем;

2) міф про заміщення – радикальна ідея про те, що інтелектуальні машини спроможні поступово та беззастережно витіснити людину з усіх сфер професійної та соціокультурної діяльності, повністю перебравши на себе її функції;

3) міф про повну автономність – утопічна концепція, згідно з якою робототехнічні комплекси здатні до абсолютно ізольованого, суверенного функціонування поза межами будь-якої антропологічної системи нагляду [123, с. 117].

Водночас, попри високий рівень дискусійності означених футурологічних сценаріїв, було б методологічною помилкою повністю виключати ймовірність того, що в міру експоненційного розвитку ІТ-архітектур, алгоритми яких моделюються на основі когнітивної матриці людини, у довгостроковій перспективі – за умови безальтернативного доведення їхньої операційної надійності, етичної комплієнтності та керованості – у фокусі правової науки знову актуалізується питання про обмежене визнання за ШІ специфічної правосуб'єктності. Такий цивілізаційний транзит потенційно здатний радикально трансформувати архітектоніку майбутньої глобальної правової системи.

На сучасному етапі цивілізаційного та технологічного поступу подібні футурологічні предикції мають суто гіпотетичний характер. Для того, щоб штучний інтелект теоретично міг претендувати на статус самостійного (суверенного) суб'єкта права, він має бути імманентно наділений не просто калькулятивною функцією, а цілісним комплексом етико-моральних якостей, які забезпечують належний рівень соціальної деліктоздатності, а також спроможністю до рефлексивного осмислення базових аксіологічних цінностей, нерозривно пов'язаних із гуманізмом, моральністю та персональною відповідальністю.

На рівні позитивного права Європейського Союзу наріжним комплексним

актом, який де-факто кодифікує та нормативно закріплює об'єктну природу й відсутність правосуб'єктності інтелектуальних агентів, є Європейський акт про штучний інтелект (EU AI Act), ухвалений Європейським парламентом 13 березня 2024 року та планомірно імплементований протягом 2025–2026 років [352]. Відповідно до архітектури цього Регламенту, деліктна відповідальність за функціонування та ризики систем ШІ імперативно покладається на його розробників (providers), розгортачів (deployers) та суб'єктів ринкового нагляду, тоді як юридична відповідальність самого штучного інтелекту як автономної сутності нормативно не передбачається.

Водночас, у довгостроковій еволюційній перспективі – у міру масштабування конвергентно-гібридної взаємодії людини з цифровими агентами та ускладнення операційної автономії кіберфізичних систем – європейський та глобальний правопорядки можуть зазнати парадигмальних трансформацій щодо можливості визнання за ШІ специфічного юридичного статусу. За такого сценарію вектор самого права неминуче зміститься від класичного регулювання суто інтерсуб'єктивних (міжлюдських) відносин до нормативного впорядкування відносин у триаді «людина – ШІ – людина», а також між автономними системами безпосередньо.

Хоча сучасне законодавство не визнає роботів суб'єктами права, тенденція до їх нормативної індивідуалізації свідчить про еволюцію правового регулювання, яка в майбутньому може актуалізувати дискусію щодо перегляду окремих елементів їх правового статусу, але не змінює сучасної концепції покладення юридичної відповідальності на людину [83].

Резюмуючи, слід констатувати, що правосуб'єктність ШІ на сучасному етапі розвитку юридичної науки та законотворчості не може ототожнюватися ані з правосуб'єктністю фізичних, ані юридичних осіб. Штучний інтелект за своєю онтологічною природою залишається нетиповим об'єктом цивільних прав – специфічною «мислячою річчю» (*res cogitans* у технологічному вимірі), яка виступає дериватом людської діяльності, функціонує виключно в межах префіксованих математичних алгоритмів та перебуває під імперативним

стратегічним наглядом людини.

Навіть за умов граничної операційної автономності функціонування штучного інтелекту не виходить за межі суто технічної реалізації заданих моделей поведінки. Екзистенційна відсутність у нього суверенної волі, правосвідомості та здатності до соціальної відповідальності апріорі унеможливорює наділення інтелектуальних агентів деліктоздатністю, а відтак – нівелює підстави для визнання за ними повноцінного статусу суб'єкта права в межах класичної правової парадигми.

Невизначення ІІІ самостійним суб'єктом перебуває у прямому каузальному зв'язку з проблематикою розподілу відповідальності за шкоду, спричену його використанням. Це зумовлює необхідність закріплення в позитивному праві презумпції відповідальності його розробника, власника та оператора як осіб, які здійснюють проєктування, навчання, стратегічний нагляд та використання відповідної цифрової системи. У межах цієї концептуальної конструкції ІІІ розглядається як джерело підвищеної небезпеки або інтелектуалізоване знаряддя правопорушення, а не як самостійний деліктоздатний суб'єкт. Відповідно, обов'язок доведення підстав звільнення від цивільно-правової відповідальності покладається на людських суб'єктів, у володінні або під контролем яких перебуває така система, що загалом корелює з європейськими підходами до суворої відповідальності за наслідки функціонування роботизованих систем.

Перспектива визнання ІІІ самостійним суб'єктом права, включно з концепцією «електронної особи», на сучасному етапі розвитку правознавства має виключно гіпотетичний характер. Реалізація такого сценарію вимагала б зміни самої сутності права – від нормативного впорядкування виключно інтерсуб'єктивних (міжлюдських) зв'язків до регулювання відносин у конвергентній тріаді «людина – ІІІ – людина», а також між автономними цифровими агентами безпосередньо. Ключовою антропологічною передумовою подібної трансформації мало б стати наділення ІІІ не просто когнітивною архітектурою, а емоційно-сенсорною та етико-моральною сферами, які здатні

забезпечити рефлексію соціальної відповідальності й усвідомлення вини. До моменту, поки вказані ментальні константи відсутні, а європейський регуляторний стандарт (зокрема, EU AI Act) імперативно фіксує об'єктну природу ШІ та покладає деліктні зобов'язання на людей, штучний інтелект має інтерпретуватися суто як об'єкт цивільних прав, наділений специфічною, інтелектуально-функціональною природою.

Дискусія навколо потенційної правосуб'єктності ШІ позбавлена суто теоретичної абстрагованості, оскільки вона безпосередньо безпосередньо пов'язана з питанням розподілу деліктних зобов'язань за шкоду, заподіяну застосуванням інтелектуальних систем, а відтак – визначає ефективність правових механізмів судового захисту. Концепція «електронної особи», яка на початку 2010-х років активно обговорювалася на рівні Європейського парламенту [355], видавалася привабливою в технократичному дискурсі, проте зазнала нищівної критики з боку міжнародної правозахисної та академічної спільноти. Обґрунтовано наголошувалося, що штучне конструювання фіктивного автономного суб'єкта правовідносин створює високий ризик його перетворення на інструмент розмивання та уникнення юридичної відповідальності з боку реальних учасників – розробників, постачальників, власників та операторів систем ШІ, що є надзвичайно актуальним і для сучасного правового простору України.

Антропоцентрична модель, яка наразі домінує в європейському та міжнародному праві, апріорі виходить із того, що штучний інтелект, незалежно від рівня його функціонально-технічної автономності, незмінно залишається артефактом людської діяльності. Будь-яка система ШІ виступає похідною формою людських рішень щодо цілепокладання, формування релевантних масивів даних, архітектури алгоритмів, критеріїв оцінювання та моделей управління ризиками. З огляду на це, наділення такої системи самостійною правосуб'єктністю є не лише методологічно деструктивним, а й екзистенційно небезпечним у вимірі захисту прав людини. Створення подібного прецеденту легітимізує можливість перекладання деліктних зобов'язань із реальних

правопорушників на системи ШІ, позбавлені як самостійної майнової основи для повноцінної компенсації шкоди, так і здатності до моральної відповідальності перед суспільством.

Відповідно, у межах сучасних регуляторних підходів дедалі виразніше утверджується імперативний принцип, згідно з яким виключно людина – фізична або юридична особа – має залишатися суб'єктом нормативних приписів, обов'язків та санкцій, пов'язаних із розробленням, впровадженням і застосуванням ШІ. Відтак правосуб'єктність у відносинах, опосередкованих використанням інтелектуальних систем, інтерпретується не як внутрішня онтологічна властивість самих алгоритмів, а як сукупність юридичних статусів, прав та обов'язків осіб, які здійснюють їх конструювання, впровадження, контроль і експлуатацію.

Зазначений підхід узгоджується як із логікою Європейського акту про штучний інтелект (EU AI Act), так і з імперативами Рамкової конвенції Ради Європи про штучний інтелект, права людини, демократію та верховенство права. В обох міжнародно-правових актах законодавець послідовно виходить із того, що ШІ виступає виключно об'єктом правового регулювання, тоді як повноцінними суб'єктами правовідносин залишаються людина та створені нею інституції. У зв'язку з цим на рівні позитивного права закріплюються жорсткі вимоги щодо забезпечення реального людського контролю, безперервного людського нагляду, а також прозорих процедур оскарження рішень, у яких застосовуються алгоритмічні системи.

Для України це має фундаментальне практичне значення, оскільки будь-які спроби імплементувати в національне законодавство концепцію «електронної особи» або прирівняти високоавтономні системи ШІ до самостійних суб'єктів права матимуть не стільки модернізаційний, скільки регресивний ефект. Створення подібних правових аномалій створить потенційно широкий і неконтрольований простір для уникнення деліктної відповідальності за незаконне, девіантне або суспільно небезпечне використання ШІ.

Натомість стратегічне завдання вітчизняного законодавця полягає в оптимізації, конкретизації та деталізації правового статусу людських та інституційних учасників відповідних суспільних відносин – включаючи розробників, суб'єктів упровадження, кінцевих користувачів, операторів систем та уповноважені державні органи, – а також у встановленні для них чітких режимів юридичної відповідальності.

Таким чином, гармонізація вітчизняного законодавства з європейським регуляторним стандартом має ґрунтуватися не на штучному розширенні кола суб'єктів права за рахунок алгоритмічних систем, а на поглибленні та деталізації інституту персональної деліктної відповідальності людини за наслідки експлуатації штучного інтелекту.

У частині суб'єктів, які безпосередньо беруть участь у життєвому циклі ШІ, слід зазначити, що аналіз чинних нормативно-правових документів дозволяє надати їхню відповідну класифікацію. Правовий статус суб'єктів у сфері використання ШІ доцільно визначати через їх роль у життєвому циклі системи ШІ: створення – введення в обіг – впровадження – використання – моніторинг, а не лише через формальний перелік прав та обов'язків. При цьому на підставі раніше розглянутих ризико-орієнтованих параметрів систем ШІ і обсяг прав, обов'язків та відповідальності таких суб'єктів будуть відрізнятися.

На відміну від класичних суб'єктів публічного адміністрування, вони є учасниками регульованих правовідносин, на яких законодавством покладається комплекс юридичних обов'язків щодо забезпечення безпечного, прозорого та правомірного функціонування систем ШІ. Їхній правовий статус визначається не лише обсягом прав та обов'язків, а й місцем у життєвому циклі системи штучного інтелекту та характером юридичної відповідальності за ризики її функціонування.

Однією з особливостей сучасної моделі адміністративно-правового регулювання використання штучного інтелекту є істотне розширення кола суб'єктів, на яких покладаються юридичні обов'язки щодо забезпечення безпечного, прозорого та правомірного функціонування систем штучного

інтелекту. На відміну від традиційної моделі правового регулювання інформаційних технологій, де основним суб'єктом відповідальності виступав виробник або власник програмного продукту, AI Act запроваджує багаторівневу систему розподілу прав, обов'язків і юридичної відповідальності між усіма учасниками життєвого циклу системи штучного інтелекту [455]. При цьому обсяг їх адміністративно-правового статусу визначається не формальною участю у створенні чи використанні системи, а виконуваними функціями та рівнем фактичного контролю над її функціонуванням.

У зв'язку із цим доцільно розмежовувати технічних учасників процесу створення систем штучного інтелекту та юридичних суб'єктів, адміністративно-правовий статус яких безпосередньо визначений AI Act.

До технічних учасників належить розробник (Developer) — особа або організація, яка здійснює створення програмного забезпечення, алгоритмів чи моделей штучного інтелекту. Водночас розробник не є самостійною юридичною категорією AI Act. Його діяльність набуває самостійного юридичного значення лише тоді, коли він одночасно виконує функції постачальника (Provider) або іншого суб'єкта, визначеного Регламентом.

Центральне місце серед регульованих суб'єктів займає постачальник (Provider), який є основним носієм юридичної відповідальності за відповідність системи вимогам законодавства. Відповідно до AI Act постачальником є фізична або юридична особа, орган державної влади чи інша організація, яка розробляє систему штучного інтелекту або замовляє її розроблення та вводить систему в обіг чи експлуатацію під власним найменуванням або торговельною маркою. Саме на нього покладаються обов'язки щодо впровадження системи управління ризиками, забезпечення якості даних, проведення оцінки відповідності, формування технічної документації, організації змістовного людського контролю (meaningful human oversight) та післяринкового моніторингу [353].

Особливістю адміністративно-правового статусу постачальника є його функціональний характер. Правовий статус визначається не фактом технічної

розробки, а здійсненню юридично значущих дій щодо введення системи в обіг або експлуатацію. Саме тому навіть у разі передачі розроблення системи на аутсорсинг суб'єкт, який розміщує її на ринку під власною торговельною маркою, набуває статусу Provider та несе повний обсяг встановлених законом обов'язків. Крім того, AI Act передбачає можливість трансформації адміністративно-правового статусу, коли оператор, імпортер, дистриб'ютор або інший суб'єкт набуває статусу постачальника внаслідок істотної модифікації системи, зміни її цільового призначення або введення її в обіг під власним найменуванням. Це свідчить про динамічний характер адміністративно-правового статусу суб'єктів у сфері використання штучного інтелекту [353].

Особливе місце у системі суб'єктів займає оператор (Deployer) — фізична або юридична особа, орган державної влади чи інша організація, яка використовує систему штучного інтелекту під власним контролем у межах професійної діяльності. Саме оператор забезпечує практичну реалізацію принципу *meaningful human oversight*, здійснює оцінку ризиків у конкретному контексті використання системи, контролює її функціонування, приймає остаточні рішення щодо використання результатів роботи системи та забезпечує можливість людського втручання. Як справедливо зазначається у сучасних дослідженнях, людський контроль не є виключно технічною характеристикою системи, а реалізується через діяльність конкретних суб'єктів, які здійснюють оцінку, перевірку та, за необхідності, коригування результатів функціонування штучного інтелекту.

Його адміністративно-правовий статус охоплює обов'язок здійснювати оцінку ризиків з урахуванням конкретного контексту використання, забезпечувати постійний моніторинг функціонування системи, організовувати належний людський контроль за прийняттям рішень та вживати заходів у разі виявлення порушень чи інцидентів. Саме на рівні оператора реалізується принцип *meaningful human oversight*, що виключає можливість повністю автономного прийняття юридично значущих рішень штучним інтелектом [395].

Користувач також набуває самостійного адміністративно-правового статусу. На відміну від традиційної моделі пасивного споживача цифрових технологій, сучасне європейське законодавство покладає на нього активні юридичні обов'язки щодо дотримання правил використання систем штучного інтелекту, виконання інструкцій виробника, належної експлуатації системи та повідомлення про виявлені інциденти чи порушення її функціонування. Таким чином, користувач стає повноцінним учасником механізму забезпечення безпечного використання штучного інтелекту.

Отже, адміністративно-правовий статус зазначених суб'єктів визначається не лише сукупністю їхніх прав та обов'язків, а й функціональною роллю на різних етапах життєвого циклу системи штучного інтелекту в частині забезпечення людського контролю. Вони формують цілісний механізм розподілу юридичної відповідальності, у межах якого обов'язки щодо забезпечення безпеки, прозорості, підзвітності та людського контролю розподіляються між усіма учасниками створення, введення в обіг та використання систем штучного інтелекту. Саме така модель відповідає сучасній європейській концепції ризик-орієнтованого управління, за якої відповідальність покладається не на систему штучного інтелекту, а на суб'єктів, які здійснюють контроль над її створенням, впровадженням та експлуатацією.

С. Іващенко зазначає, що сучасне українське законодавство перебуває на етапі формування спеціального правового регулювання, спрямованого на визначення правового статусу та юридичної відповідальності у сфері використання систем штучного інтелекту. У зв'язку з цим автор обґрунтовує доцільність застосування моделі розподіленої відповідальності, відповідно до якої обсяг юридичних обов'язків розробника, користувача та інших учасників правовідносин визначається залежно від ступеня автономності системи штучного інтелекту. Такий підхід дозволяє адаптувати механізми юридичної відповідальності до особливостей функціонування систем штучного інтелекту без відходу від антропоцентричної концепції права [103, с. 29].

З позицій правової доктрини більш обґрунтованим є функціональний підхід до класифікації суб'єктів, відповідно до якого визначальним критерієм виступає місце суб'єкта у механізмі адміністративно-правового регулювання використання штучного інтелекту. Такий підхід дозволяє розглядати кожного учасника не ізольовано, а як складову єдиної системи адміністративно-правового впливу, в межах якої забезпечується формування державної політики, встановлення регуляторних вимог, підтвердження відповідності систем штучного інтелекту, їх експлуатація, захист прав людини та здійснення державного контролю.

На відміну від AI Act, який класифікує суб'єктів залежно від їх ролі у життєвому циклі системи штучного інтелекту, запропонований підхід ґрунтується на їх функціональному призначенні у механізмі адміністративно-правового регулювання, що дозволяє інтегрувати положення європейського законодавства із системою суб'єктів публічного адміністрування України.

Першу групу становлять суб'єкти формування державної політики та нормативно-правового регулювання. До них належать Верховна Рада України, Президент України, Кабінет Міністрів України, Міністерство цифрової трансформації України, інші центральні органи виконавчої влади, які в межах своєї компетенції формують державну політику, розробляють нормативно-правові акти, визначають стратегічні напрями розвитку технологій штучного інтелекту та забезпечують адаптацію національного законодавства до права Європейського Союзу. У європейській моделі аналогічні функції виконують Європейська Комісія, AI Office та European Artificial Intelligence Board, які здійснюють координацію реалізації AI Act та забезпечують формування єдиної регуляторної політики.

Другу групу складають суб'єкти забезпечення відповідності систем штучного інтелекту, діяльність яких спрямована на підтвердження відповідності систем установленим технічним, організаційним та правовим вимогам до моменту їх введення в обіг. До цієї групи належать розробники (Developer), постачальники (Provider), імпортери (Importer), дистриб'ютори

(Distributor), уповноважені представники (Authorised Representative), а також органи оцінки відповідності й акредитовані установи. Саме вони забезпечують виконання вимог щодо управління ризиками, оцінки відповідності, технічної документації, кібербезпеки та впровадження механізмів змістовного людського контролю ще до початку використання системи.

Третю групу утворюють суб'єкти впровадження та експлуатації систем штучного інтелекту, центральне місце серед яких посідає оператор. До цієї групи також належать органи державної влади, органи місцевого самоврядування, державні підприємства, установи, приватні юридичні особи та фізичні особи-підприємці, які використовують системи штучного інтелекту у своїй професійній діяльності. Саме вони реалізують практичне застосування технологій штучного інтелекту, здійснюють оцінку ризиків у конкретних умовах експлуатації, забезпечують реалізацію принципу людського контролю, контролюють результати функціонування системи та приймають остаточні рішення щодо їх використання.

Четверту групу становлять суб'єкти реалізації та захисту прав у сфері використання штучного інтелекту. До них належать користувачі систем штучного інтелекту, фізичні та юридичні особи, права, свободи чи законні інтереси яких можуть бути порушені або обмежені внаслідок застосування відповідних технологій. На відміну від AI Act, який переважно концентрується на суб'єктах, що створюють або використовують системи штучного інтелекту, запропонований підхід передбачає виділення цієї групи як самостійного елемента механізму адміністративно-правового регулювання. Саме ці особи є носіями права на інформацію про використання штучного інтелекту, права на пояснення автоматизованого рішення, права на його перегляд людиною, права на оскарження та інших адміністративно-правових гарантій захисту.

П'яту групу складають суб'єкти державного контролю та адміністративного нагляду, до яких доцільно віднести Міністерство цифрової трансформації України (після наділення його відповідними повноваженнями), Уповноваженого Верховної Ради України з прав людини, Державну службу

спеціального зв'язку та захисту інформації України, Національний банк України – у межах регулювання фінансового сектору, Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку, інші галузеві регулятори, а також суди, які забезпечують судовий контроль за законністю використання систем штучного інтелекту. Аналогічні функції в Європейському Союзі виконують Competent Authorities, Market Surveillance Authorities, Notifying Authorities та Notified Bodies.

Запропонована класифікація демонструє, що адміністративно-правовий статус суб'єктів визначається не лише їх організаційно-правовим становищем або участю у певному етапі життєвого циклу системи штучного інтелекту, а насамперед функцією, яку вони виконують у механізмі адміністративно-правового регулювання. Це дозволяє комплексно визначити їх компетенцію, адміністративно-правові повноваження, юридичні обов'язки, межі відповідальності та характер взаємодії між суб'єктами публічного адміністрування і приватними учасниками правовідносин.

2.3. Стан адміністративно-правового та інформаційно-правового регулювання використання штучного інтелекту в Україні

Становлення правового регулювання штучного інтелекту в Україні відбувається в умовах, коли технологічні рішення вже інтегруються у публічне управління, інформаційну безпеку, правоохоронну діяльність, охорону здоров'я, освіту, оборону та економічні процеси, однак спеціальний закон, який би комплексно визначав межі допустимого використання систем ШІ, досі не прийнято. Тому оцінювання національної моделі не може зводитися до констатації наявності або відсутності профільного нормативно-правового акта. Необхідно дослідити сукупність конституційних положень, базових законів інформаційної та адміністративної спрямованості, стратегічних документів, галузевих актів і позанормативних інструментів, які разом утворюють

фрагментарне, але вже фактично діюче правове середовище використання ІІІ. Такий підхід відповідає висновку про недостатність чинної системи норм та потребу у визначенні поняття ІІІ, класифікації ризиків, диференційованих вимог, процедур оцінки відповідності й експериментального регулювання [100].

Для наукової спеціальності 12.00.07 принципове значення має розмежування двох взаємопов'язаних площин. В інформаційно-правовій площині, яку в контексті розвитку новітніх технологій активно досліджують І. В. Арістова [10;12], Л. П. Коваленко [105], О. А. Костенко [125; 133], А. І. Марущак [145], К. Р. Слюсаренко [237] та інших вчених, системи ІІІ виступають інструментами збирання, генерування, аналізу, передачі та використання інформації, а тому їх функціонування пов'язане з правовими режимами даних, персональної інформації, публічних електронних реєстрів, інформаційної та кібербезпеки. В адміністративно-правовій площині, окремі аспекти якої висвітлено у працях В. Л. Грохольського [62], А. В. Денисової [67; 68; 69], О. А. Задахайла [82], Т. О. Губанової [63], А. Ю. Нашинець-Наумової [162], Ю. І. Тюрі [252; 253], Т. І. Шинкар [271] та інших вчених, використання ІІІ органами публічної влади впливає на підготовку і прийняття адміністративних актів, надання адміністративних послуг, реалізацію дискреційних повноважень, державний контроль і нагляд, а також на можливості особи бути вислуханою, отримати мотивоване рішення та оскаржити його. Отже, предметом аналізу має бути не лише «законодавство про ІІІ», а формування адміністративно-правового й інформаційно-правового механізму обмеження його використання.

Методологічно доцільно оцінювати цей механізм за такими критеріями: 1) визначеність об'єкта регулювання та кола адресатів правових приписів; 2) наявність класифікації систем за рівнем ризику; 3) законодавче закріплення заборонених практик і спеціальних вимог до високоризикових систем; 4) визначеність компетенції органів публічного адміністрування; 5) існування процедур оцінки ризиків, впливу на права людини, відповідності, реєстрації,

аудиту й постринкового моніторингу; 6) забезпечення прозорості, людського контролю, права на пояснення та оскарження; 7) наявність юридичної відповідальності за порушення встановленого режиму. Саме за цими параметрами можна встановити, чи перейшла Україна від програмно-декларативного стимулювання технологій до юридично обов'язкового режиму їх безпечного використання.

У 2021 році Європейська Комісія представила проєкт Регламенту про штучний інтелект, який 13 березня 2024 року був схвалений Європейським Парламентом. Документ закріплює ризик-орієнтований підхід до правового регулювання штучного інтелекту, за якого обсяг нормативних вимог визначається з урахуванням рівня потенційної небезпеки, пов'язаної із розробленням, введенням в обіг та використанням відповідної системи ШІ.

Аналізуючи проєкт відповідного нормативно-правового акту, В. Г. Пилипчук, О. А. Баранов та О. С. Гиляка зазначають, що Європейською Комісією було визначено такі основні цілі правового регулювання у сфері штучного інтелекту:

- забезпечення безпечності систем штучного інтелекту, які вводяться в обіг і використовуються на території Європейського Союзу, а також їх відповідності законодавству ЄС у сфері основоположних прав і спільних європейських цінностей;
- формування належного рівня правової визначеності з метою стимулювання інвестицій, наукових досліджень та інновацій у сфері штучного інтелекту;
- удосконалення механізмів управління та забезпечення ефективного застосування законодавства про основоположні права і вимог безпеки, що поширюються на системи штучного інтелекту;
- сприяння розвитку єдиного європейського ринку законних, безпечних і надійних систем штучного інтелекту, а також запобігання фрагментації правового регулювання у цій сфері [177].

Конституційні засади правового регулювання.

Первинним нормативним рівнем є Конституція України. Її статті 3, 8, 19, 32, 34 і 55 формують вихідну систему вимог до використання ІІІ державою: людина, її гідність і безпека визнаються найвищою соціальною цінністю; діяльність органів публічної влади має здійснюватися виключно на підставі, у межах повноважень та у спосіб, передбачені законом; втручання у приватне життя й обробка конфіденційної інформації допускаються лише на законній підставі; особі гарантуються право на інформацію та судовий захист [115]. Звідси випливає, що використання алгоритмічної системи не може саме по собі створювати нову компетенцію органу влади, усувати обов'язок мотивувати рішення або звужувати обсяг процесуальних гарантій. Технологія є засобом реалізації повноваження, а не самостійним джерелом владної волі.

Конституційний підхід дозволяє сформулювати важливий для адміністративного права принцип: чим істотнішим є вплив алгоритмічного результату на права, свободи чи законні інтереси особи, тим вищими мають бути вимоги до законодавчої визначеності, людського контролю, фіксації операцій і можливості перевірки. Відтак автоматизація технічної операції та алгоритмічна підтримка аналітичної роботи не можуть прирівнюватися до автоматизованого остаточного владного рішення. Останнє потребує спеціальної законодавчої підстави, чітко визначених меж застосування, відповідального посадового суб'єкта і дієвого механізму адміністративного та судового оскарження.

Базове інформаційно-правове регулювання.

До ухвалення спеціального закону відносини у сфері ІІІ регулюються загальними нормами інформаційного законодавства. Д. Д. Позова обґрунтовано поділяє джерела регулювання інформаційно-технологічних відносин на акти, безпосередньо присвячені інформатизації та інформаційним системам, і акти, що містять окремі норми, застосовні до функціонування інформаційних технологій [181]. Така класифікація зберігає значення й для ІІІ, однак сучасний стан вимагає її доповнення третім елементом - стратегічними та експериментальними інструментами, які не встановлюють повного набору

юридичних обов'язків, але визначають майбутню модель регулювання та практику підготовки суб'єктів до неї.

Закон України «Про інформацію» визначає базові принципи інформаційних відносин, види інформації та гарантії права на інформацію [203]. Проте він не містить спеціальних положень щодо алгоритмічного виведення нових відомостей, побудови профілів, використання синтетичних даних або автоматизованого формування рекомендацій і рішень. Для систем ІІІ ця прогалина є суттєвою: юридично значущий висновок може бути отриманий не лише з інформації, яку особа безпосередньо надала, а й шляхом статистичного виведення з великого масиву даних. Відсутність спеціального режиму таких висновків ускладнює визначення обсягу інформаційних прав особи, вимог до достовірності, права на виправлення та меж використання похідних даних.

Ключовим актом є Закон України «Про захист персональних даних», дія якого поширюється на обробку даних із застосуванням автоматизованих засобів [202]. У поєднанні з Конвенцією Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних він формує правову основу законності, цільової визначеності, пропорційності та безпеки обробки [113]. Однак чинний Закон не встановлює розгорнутого спеціального режиму рішень, що приймаються виключно або переважно на основі алгоритмічного профілювання, не визначає окремого права на змістовне пояснення логіки високоризикової системи та не закріплює обов'язкової оцінки впливу на права людини перед її використанням органом влади. Тому формальна відповідність правилам обробки даних ще не гарантує правомірності всього життєвого циклу системи ІІІ.

Значення Закону України «Про доступ до публічної інформації» полягає в тому, що алгоритмічні системи, придбані або розгорнуті органами влади, не повинні перетворюватися на непроникну «чорну скриньку» лише з посиланням на комерційну таємницю постачальника [204]. Водночас відкритість не може бути абсолютною, оскільки технічна документація може містити відомості з

обмеженим доступом, дані про уразливість або об'єкти інтелектуальної власності. Потрібен спеціальний баланс: загальнодоступними мають бути відомості про призначення системи, правову підставу її використання, категорії даних, основні ризики, результати оцінки впливу, відповідального суб'єкта та порядок оскарження, тоді як технічні деталі можуть розкриватися контролюючому органу або суду в режимі захищеного доступу.

Закони України «Про захист інформації в інформаційно-комунікаційних системах» [201] і «Про основні засади забезпечення кібербезпеки України» [207] поширюють на системи ІІІ загальні вимоги до захисту інформації, стійкості інфраструктури та реагування на кіберінциденти. Разом із тим специфічні ризики моделей машинного навчання - отруєння навчальних даних, підміна моделі, adversarial-атаки, витік параметрів, маніпулювання запитами та неконтрольоване оновлення - прямо не врегульовані. Тому інформаційно-правовий режим ІІІ потребує не лише охорони інформаційної системи як технічного об'єкта, а й перевірки цілісності наборів даних, моделі та результатів упродовж усього життєвого циклу.

Особливе значення має Закон України «Про публічні електронні реєстри», оскільки державні реєстри є одним із головних джерел даних для майбутніх аналітичних систем публічної влади [205].

В той же час застосування до систем ІІІ норм, створених для попереднього етапу технологічного розвитку, не завжди забезпечує ефективне регулювання нових суспільних відносин. О. В. Костенко характеризує відповідну нормативну основу як сукупність «архаїчних нормативно-правових актів» та «законодавства аналогової епохи», яке може бути лише «реанімовано» для розв'язання сучасних проблем електронного середовища. Ця позиція підтверджує необхідність не фрагментарного пристосування чинних норм, а створення спеціальних правил щодо високоризикових систем ІІІ, алгоритмічного прийняття рішень, аудиту, прозорості та відповідальності [52].

Особливої уваги потребує застосування ІІІ у цифровій інфраструктурі територіальних громад і системах «розумного міста». О. А. Заярний вважає, що

необхідно ухвалити Закон України «Про цифрові операційні платформи “розумних” міст», у якому слід визначити «принципи, умови та процедури формування інформаційної екосистеми “розумного” міста, вимоги до процедур публічних закупівель у цій сфері, порядок залучення інвестицій, гарантії забезпечення інформаційних прав жителів цих міст». Такий підхід є актуальним і для регулювання систем ІІІ, які використовують дані публічних реєстрів, камер відеоспостереження, транспортних систем та інших елементів міської цифрової інфраструктури [68].

Інтеграція ІІІ з реєстрами може підвищити якість верифікації, виявлення помилок і шахрайства, але одночасно посилює ризик функціонального розширення: дані, зібрані для однієї адміністративної мети, можуть використовуватися для прогнозування поведінки, оцінювання ризику або профілювання особи. Чинне регулювання реєстрів не замінює спеціальних правил щодо допустимості такого вторинного використання, якості даних, меж міжвідомчого обміну та фіксації алгоритмічних операцій.

Закони України «Про електронні комунікації» [206] та «Про електронну ідентифікацію та електронні довірчі послуги» [208] створюють інфраструктурне підґрунтя для цифрової взаємодії, ідентифікації користувачів та підтвердження цілісності електронних даних. Проте достовірна ідентифікація особи не є тотожною правомірності алгоритмічного висновку щодо неї. Саме тому у сфері ІІІ необхідно розрізняти достовірність вхідних даних, технічну точність моделі, юридичну допустимість її мети та справедливості конкретного рішення. Наявність кваліфікованої електронної ідентифікації не усуває ризик дискримінації або помилкового профілювання.

Адміністративно-правові гарантії використання ІІІ.

Найбільш перспективною основою для оцінювання алгоритмічних рішень органів влади є Закон України «Про адміністративну процедуру» [186]. Він не містить окремої глави про ІІІ й прямо не визначає автоматизоване адміністративне рішення, однак закріплені ним принципи законності, обґрунтованості, пропорційності, добросовісності, розсудливості, участі особи

та права на оскарження мають поширюватися на адміністративну діяльність незалежно від того, чи використовувався посадовою особою алгоритмічний інструмент. Це означає, що орган не може виправдовувати непрозорість рішення складністю моделі або посиланням на зовнішнього постачальника.

У контексті III Закон «Про адміністративну процедуру» потребує системного тлумачення. По-перше, алгоритмічна рекомендація не може звільняти адміністративний орган від обов'язку всебічно встановити обставини справи. По-друге, мотивування адміністративного акта має містити не лише посилання на результат системи, а пояснення фактичних і правових підстав, які дозволяють перевірити рішення. По-третє, особі має бути повідомлено про суттєве використання III, якщо його результат вплинув на зміст акта. По-четверте, адміністративне оскарження має передбачати реальний перегляд людиною, а не повторне автоматичне обчислення тим самим алгоритмом.

Закон України «Про адміністративні послуги» та законодавство про електронні публічні послуги створюють правову основу для цифровізації сервісної діяльності держави [185]. Використання III є найменш проблемним у технічних операціях: маршрутизації звернень, перевірці комплектності документів, пошуку суперечностей, консультуванні та прогнозуванні навантаження. Натомість автоматичне вирішення справи, яке безпосередньо визначає право особи на послугу, виплату, дозвіл чи статус, потребує спеціальної законодавчої підстави. За її відсутності рішення має залишатися персоніфікованим актом компетентного органу або посадової особи.

Наукові дослідження 2025 року також фіксують, що використання III у публічному управлінні відкриває можливості для підвищення ефективності, але водночас створює ризики алгоритмічної дискримінації, порушення приватності та кібербезпеки [194]. У межах адміністративно-правового підходу ці ризики мають трансформуватися у конкретні юридичні обов'язки: попередню оцінку впливу, визначення відповідального розгортувача, документування цільового призначення, контроль якості даних, ведення журналів операцій, періодичний аудит і повідомлення про серйозні інциденти.

Стратегічний рівень державної політики.

Першим профільним стратегічним документом стала Концепція розвитку штучного інтелекту в Україні, схвалена Кабінетом Міністрів України у 2020 році [197]. Її значення полягає в офіційному визнанні ШІ пріоритетом державної політики, визначенні базового поняття та переліку сфер застосування. Водночас Концепція має програмно-стратегічну, а не безпосередньо регулятивну природу: вона не встановлює юридично обов'язкової класифікації ризиків, не визначає процедури допуску високоризикових систем, компетентний наглядовий орган, санкції або індивідуальні засоби правового захисту.

Початкова Концепція переважно орієнтована на стимулювання розвитку технологій у сферах освіти, науки, економіки, кібербезпеки, інформаційної безпеки, оборони, публічного управління, правового регулювання та правосуддя. Її позитивною рисою є визнання необхідності дотримання міжнародних стандартів і прав людини. Проте ця вимога не перетворена на систему адміністративних процедур. У документі відсутні критерії неприйнятності ризику, обов'язкова оцінка впливу на основоположні права, правила людського контролю, алгоритмічного аудиту, реєстрації та постринкового моніторингу. Відтак Концепція заклала напрям розвитку, але не створила завершеного механізму обмеження.

Критична оцінка Концепції не повинна підмінятися твердженням про її «неефективність» лише через відсутність санкцій. Стратегічний документ за своєю природою не має виконувати функцію спеціального закону. Проблема полягає в іншому: після визначення загального політичного напрямку держава тривалий час не забезпечувала його послідовного нормативного розгортання. План заходів на 2021-2024 роки конкретизував окремі завдання, однак також не сформував юридично обов'язкового ризикоорієнтованого режиму [198].

Вітчизняна доктрина послідовно характеризує українське регулювання як фрагментарне і таке, що потребує уніфікованого правового підходу [146]. У дослідженнях адміністративно-правової спрямованості акцентується

відсутність єдиного визначення, комплексної законодавчої бази, інституційної підтримки, правил відповідальності, прозорості та захисту персональних даних [103]. Подібна конвергенція висновків різних авторів свідчить, що проблема має не випадковий, а системний характер.

Новий етап формування державної політики пов'язаний із Дорожньою картою та Білою книгою з регулювання ШІ, оприлюдненими Міністерством цифрової трансформації України [196; 195]. Запропонований bottom-up підхід передбачає дві послідовні стадії. На першій формуються добровільні кодекси поведінки, методичні рекомендації, оцінювання ризиків, регуляторний Sandbox і спроможність майбутнього регулятора. На другій має бути прийнято закон-аналог AI Act. Цей підхід знижує ризик різкого регуляторного навантаження на індустрію та дозволяє апробувати майбутні процедури.

Наявність зазначених стратегічних і програмних документів свідчить про поступове формування державної політики у сфері штучного інтелекту, однак не усуває потреби в її подальшій законодавчій інституціоналізації. Біла книга, дорожні карти, методичні рекомендації, кодекси поведінки та експериментальні регуляторні середовища можуть забезпечувати апробацію майбутніх моделей регулювання, але за своєю юридичною природою не здатні встановити загальнообов'язкові заборони, вимоги до високоризикових систем, компетенцію наглядових органів, процедури оцінки відповідності та юридичну відповідальність.

Декларативність сучасного регулювання ШІ не є ізольованим недоліком, а відображає більш загальну проблему українського інформаційного законодавства. Ю. Є. Максименко зазначає: «Характерною рисою національного інформаційного законодавства є декларативність значного масиву норм без указівок на шляхи їх реалізації, внаслідок чого спостерігається низький рівень правореалізації норм права, що регулюють суспільні відносини у сфері забезпечення інформаційної безпеки» [148]. Цей висновок повною мірою стосується стратегічних документів у сфері ШІ, положення яких нерідко

не конкретизовані через компетенцію органів, адміністративні процедури, механізми контролю та юридичну відповідальність.

Непослідовність формування законодавства про ІІІ також відповідає загальним закономірностям розвитку джерел інформаційного права. Ю. В. Корейба характеризує сучасний етап як період, у межах якого «відбувається поспішне утворення й подеколи непослідовність розвитку джерел інформаційного права України». Стосовно ІІІ це проявляється у прийнятті окремих стратегічних і секторальних норм без їх об'єднання в цілісний ризикоорієнтований адміністративно-правовий та інформаційно-правовий механізм [126].

Відтак перехід від програмно-декларативного до нормативно зобов'язувального етапу державної політики потребує формування взаємопов'язаної системи законодавчих і підзаконних актів.

Разом із тим добровільне саморегулювання має обмежену юридичну спроможність. Воно є прийнятним для низькоризикових застосувань і підготовки бізнесу до майбутніх вимог, але не може бути достатньою підставою для використання високоризикових систем органами публічної влади. Добровільний кодекс не замінює законодавчої підстави втручання у права, не забезпечує незалежного контролю, не встановлює санкцій і не гарантує особі засобу оскарження. Тому bottom-up модель повинна розглядатися як перехідна, а не остаточна форма правового регулювання.

Важливим практичним інструментом став експериментальний Sandbox для AI- та блокчейн-рішень, фактичний запуск якого відбувся у 2025 році. У його межах передбачено юридичний аудит, перевірку персональних даних, оцінку відповідності AI Act, експертизу за методологією HUDERIA та аудит кіберзахисту [199]. Значення пісочниці для адміністративного права полягає у формуванні регуляторного знання до прийняття спеціального закону. Водночас результати експерименту не повинні створювати індивідуальні привілеї або сприйматися як дозвіл на відступ від чинних законів; рекомендації Sandbox

мають консультативний характер, якщо інше прямо не встановлено нормативним актом.

План заходів з реалізації Концепції на 2025-2026 роки демонструє поступовий перехід від загальних декларацій до конкретних регуляторних завдань. Він передбачає розроблення законопроекту щодо правового врегулювання сфери ШІ до IV кварталу 2026 року, рекомендацій з кібербезпеки, оцінювання захищеності систем, методичних рекомендацій для вищої освіти, використання ШІ у публічних закупівлях і державному управлінні, а також прийняття міжнародних стандартів як національних [200]. Однак сам план не визначає зміст майбутнього закону та не вирішує питання про інституційну модель нагляду, тому його слід оцінювати як організаційно-програмну передумову, а не завершене нормативне регулювання.

Показовим є й короткий період дії Концепції державної цільової науково-технічної програми з використання ШІ у пріоритетних галузях економіки, схваленої у 2024 році та визнаної такою, що втратила чинність у січні 2026 року. [213; 189]Ця обставина свідчить не про відмову держави від розвитку ШІ, а про нестабільність окремих програмних інструментів і потребу узгоджувати їх із загальною регуляторною архітектурою. Для правової визначеності важливо, щоб стратегічні акти мали взаємопов'язані цілі, чіткі індикатори, відповідальних виконавців і механізм наступності у разі скасування або заміни.

Секторальне регулювання та його межі.

Поряд зі стратегічними документами в Україні виникають окремі секторальні положення про ШІ. В охороні здоров'я Концепція розвитку електронної охорони здоров'я передбачає системи підтримки клінічних рішень, персоналізовану медицину, великі дані та ШІ [214]. Проте загальне медичне законодавство не містить завершеного спеціального режиму сертифікації алгоритмічних клінічних рішень, розподілу відповідальності між розробником, закладом і лікарем, а також вимог до інформованої згоди щодо суттєвого використання ШІ. Ці питання доцільно розглядати в секторальному підрозділі, тоді як у межах 2.4 достатньо зафіксувати фрагментарність правової основи.

У правоохоронній сфері Комплексний стратегічний план реформування органів правопорядку на 2023-2027 роки передбачає використання ШІ, блокчейну, хмарних обчислень, біометричного зіставлення й аналітичних технологій [201]. Водночас загальне нормативне орієнтування на «широке використання» штучного інтелекту в діяльності органів правопорядку потребує конкретизації з огляду на різну правову природу відповідних технологічних застосувань. До основних напрямів фактичного та перспективного використання ШІ у сфері громадської безпеки належать автоматизована відеоаналітика в режимі реального часу, біометрична ідентифікація осіб, автоматизоване розпізнавання номерних знаків, аналіз аудіосигналів і виявлення пострілів, опрацювання відкритих джерел та соціальних мереж засобами OSINT і SOCMINT, класифікація й узагальнення текстової інформації, прогнозування криміногенних ризиків, визначення територій підвищеної небезпеки, оптимізація розподілу поліцейських ресурсів, моніторинг масових заходів і динаміки натовпу, а також інтеграція інформації з камер, датчиків, систем екстреного реагування та елементів інфраструктури «розумного міста».

Зазначені напрями істотно відрізняються за інтенсивністю втручання у права людини. Якщо автоматизація внутрішньої звітності або технічне сортування інформації переважно має допоміжний характер, то біометрична ідентифікація в публічному просторі, прогнозна поліцейська аналітика, алгоритмічне профілювання та постійний моніторинг переміщень осіб здатні безпосередньо впливати на право на приватність, свободу пересування, свободу мирних зібрань, принцип недискримінації та презумпцію невинуватості. Тому їх правове регулювання не може обмежуватися загальним дозволом на цифровізацію правоохоронної діяльності, а має залежати від мети, способу, масштабу, тривалості та правових наслідків застосування конкретної системи ШІ [221; 222].

В освіті та науці правові проблеми охоплюють захист персональних даних, прозорість автоматизованого оцінювання, недискримінаційний доступ,

академічну доброчесність і визначення допустимої ролі генеративних систем. Сучасні дослідження обґрунтовано вказують на потребу в алгоритмічному аудиті та незалежних інституційних гарантіях захисту прав учасників освітнього процесу [28]. Водночас такі пропозиції ще не утворюють єдиного нормативного режиму, а майбутні методичні рекомендації, передбачені Планом на 2025-2026 роки, не замінять законодавчих гарантій у разі прийняття рішень, що істотно впливають на право на освіту.

У медіа та інформаційному просторі головними проблемами є маркування синтетичного контенту, відповідальність за поширення недостовірної інформації, дотримання журналістських стандартів, авторських прав і прав аудиторії. Дослідники підкреслюють необхідність секторальних рекомендацій для відповідального використання генеративного ШІ [183]. Цей приклад демонструє загальну закономірність: рамковий закон має встановлювати спільні вимоги до прозорості, оцінки ризиків і відповідальності, тоді як конкретні стандарти повинні деталізуватися галузевим законодавством та професійними правилами.

В оборонній сфері використання ШІ для розвідки, логістики, планування й управління може підвищити оперативність, але також створює ризики надмірної автоматизації рішень, кіберуразливості та розмивання персональної відповідальності [260]. Національне регулювання має враховувати особливості режиму державної таємниці й воєнного стану, однак безпекові винятки не повинні перетворюватися на повне вилучення систем із правового контролю. Навіть у сфері національної безпеки необхідні внутрішні процедури тестування, журналювання, визначення командної відповідальності та змістовного людського контролю.

Таким чином, секторальні акти підтверджують фактичне поширення ШІ, але не замінюють рамкового регулювання. Їх спільною проблемою є те, що вони переважно визначають напрями впровадження, а не юридичні межі. Саме тому правова модель повинна поєднувати горизонтальні норми - поняття,

класифікацію ризиків, загальні обов'язки, нагляд і відповідальність - із вертикальними правилами для конкретних сфер.

Євроінтеграційний та міжнародно-правовий вимір. Євроінтеграційний курс України зумовлює необхідність наближення національного права до цифрового *acquis* ЄС. Як зазначає О. В. Костенко, Україна, перебуваючи на шляху євроінтеграції та післявоєнної відбудови, повинна активно впроваджувати цифрові технології як ключовий драйвер економічного зростання.

Відповідний напрям впливає з Угоди про асоціацію та участі України у програмі «Цифрова Європа» [254; 255]. Для українських постачальників AI Act має також практичне транскордонне значення, оскільки його правила можуть застосовуватися до систем і моделей, що вводяться в обіг у ЄС або результати яких використовуються на території Союзу [138]. Тому майбутнє українське регулювання має забезпечити не механічне копіювання термінів, а функціональну сумісність процедур оцінки відповідності, документації, нагляду та захисту прав.

Регламент (ЄС) 2024/1689 закріплює ризикоорієнтовану модель: заборонені практики, спеціальні вимоги до високоризикових систем, обов'язки прозорості для визначених застосувань і правила для моделей загального призначення [353]. Важливо уникати спрощення, ніби AI Act універсально забороняє будь-яке автоматизоване рішення. Його логіка полягає в диференціації вимог залежно від призначення, контексту й ризику та у забезпеченні ефективного людського нагляду за високоризиковими системами. Для України це означає необхідність точно визначити, де автоматизація є допустимою, де вона потребує посиленого контролю, а де практика має бути заборонена.

Порівняння визначень ШІ в українській Концепції та AI Act свідчить, що національна дефініція потребує оновлення з урахуванням здатності системи робити висновки й генерувати прогнози, рекомендації, контент або рішення, які впливають на фізичне чи віртуальне середовище. На цю проблему звертається

увага і в сучасній літературі, де підкреслюється, що базове визначення Концепції ускладнює гармонізацію з європейськими стандартами [227]. Однак надмірно широке визначення також є небезпечним: воно може поширити спеціальний режим на звичайне програмне забезпечення. Тому дефініція має бути технологічно нейтральною, але правочутливою.

Додатковим міжнародно-правовим орієнтиром є Рамкова конвенція Ради Європи про ШІ, права людини, демократію та верховенство права - перший юридично обов'язковий міжнародний договір у цій сфері [347]. Україна підписала її 15 травня 2025 року [350]. Конвенція вимагає дотримання людської гідності, автономії, рівності, приватності, прозорості, підзвітності та надійності, а також передбачає оцінювання ризиків і впливу, процедурні гарантії, можливість оскарження та запровадження заборон або мораторіїв щодо окремих практик. Для спеціальності 12.00.07 особливо важливо, що ці вимоги адресовані насамперед діяльності публічної влади та приватних суб'єктів, які діють від її імені.

Методичний матеріал, підготовлений у взаємодії Офісу Омбудсмана та Міністерства цифрової трансформації, також акцентує на попередніх консультаціях, тестуванні, системному моніторингу, якості даних, відповідальності, захисті персональних даних та оцінюванні ризиків [213]. Попри рекомендаційний характер, ці положення є важливими для формування національних адміністративних процедур, оскільки переводять абстрактні принципи прав людини у послідовність операцій, які мають виконувати розробник і орган-розгортувач до, під час і після використання системи.

Системні прогалини національного регулювання.

Проведений аналіз дає підстави виокремити взаємопов'язану систему прогалин. Першою є понятійна невизначеність. Офіційне визначення міститься у стратегічній Концепції, однак відсутнє в законі загальної дії. Це ускладнює встановлення адресатів майбутніх обов'язків, розмежування систем ШІ і традиційного програмного забезпечення та застосування єдиних критеріїв у різних галузях. Вітчизняні автори обґрунтовано вказують на потребу

комплексної законодавчої бази, що поєднуватиме відповідальність, прозорість, етичність і захист даних [228; 229].

Другою прогалиною є відсутність законодавчої класифікації ризиків. Наявні акти містять згадки про використання ІІІ у чутливих сферах, але не встановлюють юридичних наслідків віднесення системи до певної категорії. Через це однакові загальні правила формально можуть застосовуватися і до чат-бота довідкового характеру, і до системи біометричної ідентифікації чи оцінки ризику особи. Ризикоорієнтований підхід повинен пов'язувати рівень потенційної шкоди з інтенсивністю обов'язків і контролю.

Третьою є інституційна невизначеність. Мінцифри формує політику й координує стратегічні ініціативи, окремі органи відповідають за кібербезпеку, стандартизацію, захист персональних даних, конкуренцію, секторальний нагляд. Однак не визначено, який орган здійснюватиме ринковий та адміністративний нагляд за високоризиковими системами, координуватиме розслідування інцидентів, вести реєстр, застосовувати заходи реагування і взаємодіяти з європейськими інституціями. Майбутня модель може бути централізованою або мережевою, але розподіл компетенції повинен бути встановлений законом.

Четверта прогалина має процедурний характер. Українське право не встановлює єдиної обов'язкової процедури оцінювання впливу системи ІІІ на основоположні права до її використання органом публічної влади. Не врегульовані також мінімальний зміст технічної документації, вимоги до наборів даних, незалежний аудит, державна реєстрація визначених систем, постринковий моніторинг, повідомлення про серйозні інциденти та правила суттєвої модифікації. Унаслідок цього контроль часто можливий лише після настання шкоди, що суперечить превентивній логіці адміністративного права у високоризикових сферах.

П'ятою є недостатність індивідуальних гарантій. Особа повинна мати право знати про істотне використання ІІІ, отримати зрозумілу інформацію про роль системи, подати заперечення, вимагати перегляду компетентною людиною

та оскаржити як саме рішення, так і неправомірне застосування системи. Ці гарантії впливають із Конституції, адміністративної процедури та Рамкової конвенції, але потребують спеціальної законодавчої конкретизації. Комерційна таємниця не може повністю блокувати доступ суду чи наглядового органу до відомостей, необхідних для перевірки законності.

Шостою прогалиною є невизначеність відповідальності. Чинне цивільне, адміністративне, кримінальне та дисциплінарне законодавство може застосовуватися до окремих наслідків, однак не формує цілісного розподілу обов'язків між постачальником, імпортером, розгортувачем, оператором, органом влади та посадовою особою. Неприпустимим є перенесення відповідальності на саму систему ШІ. Відповідальними мають залишатися реальні фізичні та юридичні особи, які визначили призначення, ввели систему в експлуатацію, надали дані, контролювали її роботу або прийняли юридично значуще рішення.

Сьомою є відсутність спеціально врегульованого режиму використання ШІ під час воєнного стану. Безпекові потреби можуть обґрунтовувати обмеження відкритості, прискорені процедури або особливі правила закупівель, але не усувають принципів законності, необхідності й пропорційності. Для систем, що використовуються у правоохоронній, розвідувальній та оборонній діяльності, потрібні захищені форми незалежного контролю, внутрішній аудит, журналювання, тестування на помилки та чітке визначення людської відповідальності. Інакше виняток для безпеки створюватиме простір фактичної нерегульованості.

Виявлені прогалини дають підстави запропонувати трирівневу модель нормативного вдосконалення національного регулювання штучного інтелекту.

Перший рівень має становити рамковий Закон України «Про безпечне та відповідальне використання систем штучного інтелекту». Його призначення полягає у закріпленні уніфікованого понятійного апарату, класифікації систем штучного інтелекту за рівнем ризику, переліку заборонених практик, вимог до високоризикових систем, принципів прозорості, людського нагляду, оцінки

впливу на основоположні права, аудиту, логування, державного нагляду та юридичної відповідальності. Прийняття такого акта має забезпечити системну правову основу, якої наразі не створюють стратегічні та рекомендаційні документи.

Другий рівень передбачає внесення узгоджених змін до чинних законів України. Зокрема, законодавство про адміністративну процедуру доцільно доповнити гарантіями для випадків використання ШІ під час підготовки або прийняття адміністративних актів: обов'язком повідомляти особу про застосування алгоритмічної системи, забезпечувати змістовний людський контроль, мотивувати рішення та надавати можливість його перегляду уповноваженою посадовою особою. Законодавство про захист персональних даних має бути доповнене спеціальними вимогами щодо автоматизованої обробки, профілювання, біометричних даних, оцінки ризиків та забезпечення прав суб'єктів даних. У законах про доступ до публічної інформації, публічні електронні реєстри та публічні закупівлі доцільно закріпити вимоги до розкриття інформації про застосування систем ШІ, якості й походження даних, журналювання операцій, закупівлі та експлуатації високоризикових систем.

Третій рівень мають становити підзаконні нормативно-правові акти Кабінету Міністрів України, необхідні для процедурної реалізації рамкового закону. До них належать порядок проведення оцінки впливу високоризикових систем ШІ на основоположні права, порядок ведення державного реєстру відповідних систем і повідомлення про серйозні інциденти, а також порядок функціонування регуляторного експериментального середовища. Такі акти повинні визначати суб'єктів процедур, строки, критерії оцінювання, вимоги до документації, форми державного контролю та юридичні наслідки виявлення неприйняттого ризику.

Запропонована система не передбачає механічного копіювання положень AI Act. Її зміст має враховувати структуру українського адміністративного та інформаційного законодавства, правовий режим воєнного стану, стан публічних електронних реєстрів, рівень інституційної спроможності органів

влади та необхідність збереження умов для технологічних інновацій. Деталізоване обґрунтування зазначеної моделі доцільно викласти в розділі 4 дисертації, а розроблені автором тексти проєктів нормативно-правових актів - у відповідних додатках.

Формування спеціального регулювання не повинно перетворюватися на невинуватене блокування технологічного розвитку. М. В. Карчевський обґрунтовує «неможливість абсолютної заборони розробок систем ІІІ», зазначаючи, що правове регулювання відповідної сфери має бути спрямоване «на стимулювання соціально ефективного використання технологій ІІІ та мінімізацію ризиків зловживань її використання». Такий підхід відповідає принципу пропорційності: жорсткість нормативних вимог має залежати від рівня ризику, характеру впливу системи на права людини та сфери її застосування [123].

Отже, сучасний стан українського права доцільно характеризувати як перехід від фрагментарного стратегічного й секторального регулювання до майбутньої системи юридично обов'язкових ризикоорієнтованих норм. Національне правове поле вже містить конституційні, інформаційно-правові й адміністративно-процедурні засади, які дозволяють оцінювати законність використання ІІІ. Водночас ці засади не замінюють спеціального механізму, оскільки не визначають усіх елементів життєвого циклу системи, компетенції наглядових органів і спеціальних гарантій для осіб, на права яких впливають алгоритмічні рішення.

У межах подальшого формування правової політики необхідно розглядати адміністративно-правовий та інформаційно-правовий механізм обмеження ІІІ як єдність п'яти взаємопов'язаних елементів: нормативного, інституційного, процедурного, контрольно-наглядового та юрисдикційно-захисного. Нормативний елемент має охоплювати рамковий закон і секторальні акти; інституційний - визначення компетентного регулятора та координації; процедурний - класифікацію, оцінювання впливу, відповідність, реєстрацію, аудит і людський контроль; контрольно-наглядовий - моніторинг, перевірки та

реагування на інциденти; юрисдикційно-захисний - відповідальність, адміністративне й судове оскарження та відновлення порушених прав.

Важливим компонентом такого механізму має бути постійний правовий моніторинг використання алгоритмічних систем. Є. А. Тимошенко визначає правове забезпечення застосування ІІІ як систему трьох взаємопов'язаних напрямів: «1) комплексних науково-теоретичних розробок щодо технічної та правової природи ІІІ в контексті його ефективного та безпечного використання; 2) вдосконалення правового механізму, яким регулюється застосування ІІІ, відповідно до отриманих результатів використання; 3) правовий моніторинг стану застосування окремих систем ІІІ в різних галузях життя в Україні». Правовий моніторинг має охоплювати аналіз інцидентів, практики використання високоризикових систем, дискримінаційних наслідків, ефективності людського контролю та відповідності фактичного функціонування систем заявленій меті [193].

Отже, подальший розвиток правового регулювання штучного інтелекту в Україні має здійснюватися не шляхом накопичення розрізнених стратегічних і секторальних положень, а через формування узгодженого адміністративно-правового та інформаційно-правового механізму. Його законодавче ядро має становити рамковий акт про безпечне й відповідальне використання систем ІІІ, доповнений змінами до базового інформаційного та адміністративного законодавства і процедурними актами Кабінету Міністрів України. Запропонована конструкція є безпосередньою нормативною відповіддю на виявлені прогалини та становить основу для подальшого обґрунтування авторської моделі правової політики у наступних розділах дисертації.

Таким чином, Україна сформувала стратегічні й окремі нормативні передумови регулювання ІІІ, однак вони ще не утворюють цілісного механізму обмеження його використання. Подальша імплементація AI Act і Рамкової конвенції Ради Європи повинна відбуватися не шляхом формального копіювання, а через узгодження з Конституцією України, Законом «Про адміністративну процедуру», інформаційним законодавством та особливостями

національної системи публічного адміністрування. Саме така інтеграція дозволить одночасно забезпечити інноваційний розвиток, правову визначеність, ефективність державного управління та пріоритет прав людини.

Висновки до розділу 2

1. Доведено об'єктивну необхідність розширення класичної структури механізму правового регулювання в умовах експансії високоавтономних цифрових систем.

2. Обґрунтовано, що специфіка ШІ (недетермінованість, здатність до самонавчання та прийняття нелінійних рішень, що тягнуть юридично значущі наслідки) вимагає включення до МПР новітніх органічно-функціональних компонентів.

3. Доведено, що ефективність сучасного інформаційно-правового та адміністративно-правового впливу забезпечується не лише сукупністю імперативних приписів, а й інтеграцією у структуру механізму таких елементів, як: управління ризиками, оцінка відповідності (*conformity assessment*), алгоритмічна прозорість, незалежний техніко-юридичний аудит, сертифікація та превентивний державний нагляд.

4. Виявлено та типізовано концептуальний дуалізм розвитку глобальної інформаційно-правової політики у сфері ШІ. На універсальному рівні (акти ООН, Окінавська хартія, Женевська декларація) тривалий час домінував підхід, за якого штучний інтелект «розчинявся» в загальному секторі інформаційно-комунікаційних технологій (ІКТ), орієнтованому на подолання цифрової нерівності, без виокремлення ШІ як самостійного об'єкта безпекового регулювання. На європейському регіональному рівні (Рада Європи, ЄС) сформовано упереджувальну, ціннісно орієнтовану модель «керованої автономії» (від етичних настанов *Ethics Guidelines for Trustworthy AI* та Рекомендації CM/Rec(2020)1 до імперативних режимів «жорсткого права», кодифікованих в *EU AI Act* та Рамковій конвенції Ради Європи про ШІ) [347,

348, 353]. Ця модель трансформує техніко-етичні вимоги (людський контроль *human-in-the-loop*, прозорість, пояснюваність) у правові фільтри допуску технологій на ринок.

5. Здійснено критичний доктринальний аналіз правосуб'єктності у цифрову епоху та обґрунтовано правову неделіктоздатність штучного інтелекту. Спираючись на інтегративні властивості правосуб'єктності, доведено теоретичну неспроможність концепції «електронної особи» як самостійного суверенного суб'єкта права через повну відсутність у ШІ автономної правової волі, правосвідомості та психоемоційного компонента вини (інтелектуально-вольового критерію осудності).

6. Запропоновано авторське функціональне розмежування на: *неавтономний ШІ* (перебуває на стадії інституційного навчання під телеологічним контролем людини); *автономний ШІ* (здатний виконувати завдання під системним стратегічним наглядом людини, але без її покрокового керування).

7. Обґрунтовано підпорядкування штучного інтелекту правовому режиму джерела підвищеної небезпеки та «мислячої речі» (*res cogitans*), де загальний тягар ризиків та безвинна деліктна відповідальність покладаються виключно на людського суб'єкта (розробника або оператора/володільця), що унеможливорює використання ШІ як інструмента розмивання юридичної відповідальності.

8. Систематизовано та диференційовано за п'ятьма групами суб'єктний склад правовідносин у сфері використання ШІ на основі їхнього функціонального призначення в національному МПР (на відміну від ринкової класифікації *EU AI Act*).

9. Виявлено комплекс системних прогалин чинного адміністративно-правового та інформаційно-правового регулювання використання ШІ в Україні. Встановлено, що наявне нормативне середовище є фрагментарним: стратегічні документи (Концепція 2020 р., Дорожня карта, Біла книга Мінцифри) та експериментальні інструменти (*AI Sandbox 2025 р.*) мають програмно-

декларативний характер і не здатні встановити загальнообов'язкових заборон, санкцій чи інституційної моделі нагляду. Секторальне законодавство (в охороні здоров'я, правоохоронній сфері, освіті) фіксує технологічне впровадження ІІІ, але не визначає юридичних меж його застосування. Констатовано відсутність законодавчого визначення ІІІ, ризик-орієнтованої класифікації систем, превентивних процедур оцінки впливу на фундаментальні права (*FRIA/HRIA*) до впровадження систем органами влади, а також спеціального режиму використання ІІІ в умовах воєнного стану.

10. Розроблено та обґрунтовано цілісну трирівневу модель нормативного вдосконалення національного законодавства, яка забезпечує створення ефективного та адаптивного механізму *AI governance* в Україні без механічного копіювання іноземних норм: перший рівень (законодавче ядро): ухвалення рамкового Закону України «Про безпечне та відповідальне використання систем штучного інтелекту», що закріплює понятійний апарат, ризик-орієнтований підхід, заборонені практики та компетенцію наглядового органу; другий рівень (взаємоузгоджені зміни до базових законів): доповнення Закону України «Про адміністративну процедуру» положеннями про обов'язок фіксації «алгоритмічного сліду» посадовою особою та право особи на змістовне пояснення і перегляд автоматизованого рішення людиною; модернізація законів про захист персональних даних (регулювання профілювання), про доступ до публічної інформації, публічні реєстри та публічні закупівлі; третій рівень (процедурний): постанови Кабінету Міністрів України, що регламентують порядок проведення оцінки впливу високоризикових систем на основоположні права, ведення Державного реєстру таких систем, фіксацію інцидентів та функціонування регуляторних «пісочниць». Сформована модель виступає теоретичним підґрунтям для розробки конкретних правових інструментів у наступних розділах дисертаційного дослідження.

РОЗДІЛ 3. ОБМЕЖЕННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОКРЕМИХ СФЕРАХ ПРАВОВІДНОСИН

3.1. Соціальні передумови обмеження використання штучного інтелекту в окремих сферах життєдіяльності людини

Збалансоване та таргетоване нормативне обмеження використання штучного інтелекту в окремих сферах суспільних відносин виступає більш ефективною моделлю забезпечення безпечного розвитку технологій, ніж надмірна превентивна зарегульованість, здатна стримувати технологічний прогрес ще до повноцінної інтеграції відповідних систем у суспільні процеси.

Така позиція детермінована виявленою у Розділі 1 закономірністю, відповідно до якої соціальні побоювання та позитивні очікування щодо використання штучного інтелекту перебувають у тісному взаємозв'язку. Суспільство остерігається саме тих властивостей систем ШІ, які водночас забезпечують їхні очевидні переваги порівняно з людськими можливостями. Результати опитування серед представників ІТ-сфери свідчать про значне зближення позицій фахової спільноти та нефахової аудиторії. Обидві групи респондентів загалом однаково визначають як сфери підвищеного ризику застосування ШІ, так і напрями, у яких його використання сприймається як суспільно корисне та бажане. Водночас існує низка сфер, у яких інтеграція штучного інтелекту є об'єктивно необхідною, проте потребує обов'язкового людського контролю та присутності оператора у процесі прийняття рішень. Такий підхід безпосередньо впливає на формування доктрини правосуб'єктності ШІ, моделі цивільно-правової відповідальності, а також особливості страхування технологічних ризиків у разі заподіяння шкоди. У цьому контексті для розуміння меж допустимої алгоритмізації суспільних процесів важливе значення має класична критика штучного інтелекту, сформульована Х'юбертом Дрейфусом крізь призму чотирьох фундаментальних припущень [1]:

- *біологічного*, згідно з яким процеси обробки інформації людиною мають дискретний характер і здійснюються на основі певного біологічного еквівалента перемикальних систем;
- *психологічного*, відповідно до якого мислення розглядається як обробка формалізованої інформації у бінарному (двоїчному) коді за визначеними алгоритмічними правилами;
- *епістемологічного*, яке виходить із того, що будь-яке знання може бути формалізоване та виражене через систему логічних відношень і булевих функцій;
- *онтологічного*, за яким навколишній світ може бути представлений як сукупність автономних фактів, кожен із яких логічно не залежить від інших [351].

Зазначені концептуальні положення Х. Дрейфуса тривалий час слугували теоретичним підґрунтям для критичного осмислення меж формально-алгоритмічного підходу до штучного інтелекту. Водночас сучасний етап розвитку генеративних моделей ШІ та нейромережевих архітектур засвідчує необхідність переоцінки окремих із цих положень з урахуванням нелінійного характеру машинного навчання, ефекту «чорної скриньки» та розвитку технологій віртуальної і доповненої реальності. У цьому контексті біологічне припущення Х. Дрейфуса щодо неможливості відтворення специфіки людського сприйняття поза межами людської біологічної природи частково втрачає категоричність.

Практика інтеграції людини у цифрові середовища демонструє здатність свідомості адаптуватися до штучно змодельованих сенсорних і поведінкових контекстів. У зв'язку з цим окремі механізми обробки інформації та моделювання поведінкових реакцій можуть бути відтворені за допомогою складних алгоритмічних систем, що ставить під сумнів абсолютність окремих психологічних та біологічних обмежень, сформульованих у межах ранньої критики штучного інтелекту.

Перші два припущення Х. Дрейфуса, які виходили з необхідності

наявності у машини фізичного втілення, подібного до людського, та специфічної соціальної адаптації для досягнення людиноподібного інтелекту [350], значною мірою нівелюються в умовах розвитку сучасних цифрових технологій та віртуальних середовищ. Для систем ШІ наявність матеріальної оболонки не є визначальною умовою функціонування, оскільки ключового значення набуває здатність алгоритму сприймати, обробляти, аналізувати інформацію та автономно ухвалювати рішення у межах заданої архітектури [229, с. 9].

Складні нейромережеві системи та генеративні моделі ШІ вже сьогодні здатні демонструвати поведінкові патерни, що імітують окремі когнітивні та комунікативні реакції людини. У зв'язку з цим психологічне припущення Х. Дрейфуса щодо принципової неможливості алгоритмізації мислення поза жорсткими бінарними моделями в сучасних умовах дедалі більше трансформується у проблему обчислювальної складності, архітектурного дизайну та меж машинного навчання.

Водночас слушною залишається позиція Х. Дрейфуса щодо неможливості повного заміщення людського досвіду, контекстуального розуміння та морального судження алгоритмічними системами. Особливої актуальності це набуває у сферах охорони здоров'я, правосуддя та публічного управління, де автономне використання ШІ без належного людського контролю здатне спричиняти істотні помилки та етичні ризики [351, с. 308-320].

Особливого значення для сучасної правової доктрини набуває виокремлена Х. Дрейфусом проблема підриву унікального людського досвіду та суб'єктивного судження, що зумовлено відсутністю у систем ШІ ситуативного й контекстуального розуміння, притаманного людині. Унаслідок цього алгоритмічні системи не здатні повною мірою інтерпретувати складні соціальні взаємозв'язки чи вирішувати морально-етичні дилеми, які потребують людського досвіду, емпатії та відповідальності. Відтак делегування ШІ функцій ухвалення критично важливих рішень, зокрема у сфері охорони здоров'я, правосуддя чи публічного управління, здатне породжувати істотні

правові та етичні ризики.

Окрему увагу Х. Дрейфус приділяв проблемі людської автентичності. Аналізуючи здатність алгоритмів імітувати емоційні реакції та поведінкові моделі, він попереджав про небезпеку антропоморфізації цифрових систем і поступового розмивання меж між людською та машинною взаємодією. Це, своєю чергою, може призводити до втрати глибини міжособистісних зв'язків та заміщення справжньої комунікації її алгоритмічною імітацією.

Серед ризиків для особистої автономії та приватності, на думку вченого, особливу небезпеку становлять системи ШІ, що функціонують на основі масштабних масивів персональних даних. Вони створюють потенційні можливості для маніпулювання поведінкою, уподобаннями та вибором людини. Накопичення й аналіз значних обсягів інформації дозволяють формувати високоточні механізми впливу на суспільну свідомість та поведінкові моделі.

Концептуальні застереження Х. Дрейфуса щодо розвитку штучного інтелекту набувають безпосереднього значення для сучасної правової доктрини, оскільки виокремлений ним комплекс ризиків пов'язаний із підривом людського досвіду та автономного судження, розмиванням автентичності міжособистісної взаємодії, втручанням у приватність, можливістю маніпулювання людською поведінкою, а також поглибленням соціально-економічної нерівності. Це зумовлює необхідність правового обмеження використання ШІ у сферах підвищеного ризику та збереження пріоритетної ролі людини у процесі прийняття суспільно значущих рішень.

У сучасному науковому дискурсі зазначені побоювання трансформувалися у концептуальні застереження представників трансгуманістичного напрямку та експертів у сфері високих технологій, серед яких особливе місце посідають праці Ніка Бострома, Ілона Маска, Стюарта Рассела, Макса Тегмарка та Рея Курцвейла.

Аналізуючи потенційні екзистенційні ризики розвитку штучного інтелекту, Н. Бостром виокремлює три ключові проблеми: проблему контролю [308, с. 116-130], проблему узгодження цінностей (value alignment) [308, с. 227-

230] та конкурентні перегони у сфері розробки ШІ, які можуть призводити до зниження рівня безпеки відповідних технологій [308, с. 254-267].

Сутність «проблеми контролю» полягає у забезпеченні того, щоб системи штучного інтелекту діяли відповідно до людських цінностей, цілей та встановлених обмежень [308, с. 112-115]. У міру розвитку й ускладнення систем ШІ вони можуть набувати дедалі більшої автономності, виходячи з-під безпосереднього людського контролю. Це підвищує ризик того, що такі системи діятимуть всупереч інтересам людства – або внаслідок помилкової інтерпретації поставлених завдань, або через невідповідність алгоритмічних рішень базовим суспільним цінностям.

Обґрунтовуючи необхідність випереджальних досліджень у сфері безпеки ШІ та створення ефективних технічних і правових запобіжників, Н. Бостром наголошує: «Терміновість розробки надійних можливостей для контролю суперінтелекту неможливо переоцінити. < ... > Міжнародна співпраця у дослідженнях безпеки є життєво необхідною до того, як конкурентні динаміки зроблять це неможливим» [308, с. 112-113].

Ключовою проблемою, на якій ґрунтуються міркування Н. Бострома, є проблема узгодження цінностей (value alignment). В ідеалі системи штучного інтелекту мають бути спроектовані таким чином, щоб їхнє функціонування відповідало людським етичним орієнтирам та суспільним пріоритетам. Проте практична реалізація такого підходу є надзвичайно складною, оскільки некоректна формалізація аксіологічних засад людської поведінки може призвести до помилкової інтерпретації алгоритмами поставлених цілей і, як наслідок, – до непрогнозованих наслідків взаємодії ШІ як з людиною, так і з іншими об'єктами. Саме тому Н. Бостром наголошує на необхідності системних досліджень і досягнення міжнародного консенсусу щодо принципів етичного та безпечного програмування систем штучного інтелекту.

Не менш важливим є застереження Н. Бострома щодо ризиків конкурентних перегонів у сфері розробки штучного інтелекту. На його думку, отримання окремою організацією, корпорацією чи державою вирішальної

технологічної переваги у сфері ШІ може призвести до небезпечного дисбалансу сил та створити передумови для неконтрольованого або зловмисного використання відповідних технологій. Саме тому дослідник наголошує на необхідності міжнародного співробітництва, відповідального розвитку систем штучного інтелекту та формування ефективних механізмів глобального контролю у сфері високих технологій.

Резюмуючи підходи Н. Бострома, слід зазначити, що виокремлені ним проблеми контролю, узгодження цінностей та конкурентних перегонів у сфері ШІ мають розглядатися не лише як потенційні технологічні загрози, а і як концептуальні орієнтири для формування превентивної моделі правового регулювання штучного інтелекту. У цьому аспекті його застереження виконують важливу методологічну функцію для розробки сучасних правових механізмів безпечного використання ШІ.

Важливе місце у сучасному дискурсі щодо ризиків штучного інтелекту посідають публічні заяви Ілона Маска. У своїх виступах та інтерв'ю він неодноразово висловлював занепокоєння не стільки щодо самого факту розвитку ШІ, скільки щодо ризиків, пов'язаних із безконтрольним розробленням та впровадженням високорозвинених автономних систем. Подібні застереження І. Маск послідовно висловлював під час Саміту з безпеки штучного інтелекту 2023 року (MIT AeroAstro Centennial Symposium, AI Safety Summit 2023) [451], а також у низці публічних інтерв'ю 2023 р., акцентуючи увагу на ризиках втрати контролю над передовими системами штучного інтелекту [449].

Його застереження щодо розвитку штучного інтелекту ґрунтуються на припущенні про потенційну здатність автономних систем перевищити окремі когнітивні можливості людини. У такому випадку відсутність ефективних механізмів контролю та належного правового регулювання може призвести до функціонування ШІ поза межами реального людського нагляду, що створює ризики виникнення непередбачуваних наслідків для суспільства та безпеки людства. У своїх виступах 2023 р. І. Маск прямо пов'язував розвиток

надпотужного ШІ з потенційними цивілізаційними ризиками та необхідністю випереджального регулювання відповідних технологій [503; 450].

Однією з ключових загроз І. Маск вважає можливість використання штучного інтелекту у протиправних та кримінальних цілях. На його думку, за відсутності належних етичних стандартів, механізмів контролю та правових обмежень системи ШІ можуть використовуватися для заподіяння шкоди людині, маніпулювання інформацією або експлуатації вразливостей цифрових систем. Крім того, І. Маск висловлює занепокоєння щодо впливу штучного інтелекту на ринок праці. У міру розвитку технологій ШІ зростає ризик масштабної автоматизації, що може призвести до структурного безробіття та поглиблення соціально-економічної нерівності.

Характерно, що І. Маск є одним із небагатьох представників сучасного технологічного дискурсу, хто послідовно наголошує на необхідності належного державного та міжнародного регулювання процесів розробки і використання систем штучного інтелекту. Він підкреслює важливість формування єдиних стандартів і принципів, спрямованих на забезпечення безпечного та етичного використання ШІ. На його переконання, уряди держав та експертне середовище мають консолідувати зусилля для створення ефективної нормативної бази, у межах якої пріоритетними залишатимуться безпека та благополуччя людини. Вказані підходи І. Маск послідовно відстоює необхідність випереджального міжнародного регулювання розвитку штучного інтелекту [451; 503].

Резюмуючи основні позиції І. Маска щодо розвитку штучного інтелекту, слід зазначити, що він не є противником ідеї співіснування людини та ШІ. Навпаки, будучи одним із провідних інвесторів і розробників у сфері високих технологій, І. Маск є послідовним прихильником керованого, безпечного та контрольованого розвитку систем штучного інтелекту.

Сутність його застережень полягає не у запереченні перспектив розвитку ШІ, а у необхідності формування ефективних правових, етичних і технічних механізмів контролю за процесами створення та впровадження автономних систем. На його переконання, лише за умови належного регулювання та

відповідального використання штучний інтелект може стати інструментом суспільного прогресу, а не джерелом деструктивних ризиків для людства.

Вагоме значення для сучасного дискурсу щодо безпечного розвитку штучного інтелекту мають праці відомого фахівця у сфері комп'ютерних наук Стюарта Рассела. Дослідник наголошує, що створення систем ШІ без урахування людських цінностей та цілей здатне спричинити непередбачувані наслідки, небезпечні для людини та суспільства. У зв'язку з цим С. Рассел акцентує увагу на необхідності узгодження функціонування систем штучного інтелекту з людськими цінностями, а також на важливості постійного людського контролю за автономними системами. Особливе занепокоєння вченого викликає можливість того, що високорозвинені системи ШІ можуть переслідувати власні цілі без належного врахування безпеки та добробуту людини. Саме тому С. Рассел застерігає від створення повністю автономних систем, які не здатні належним чином інтерпретувати гуманістичні цінності та суспільні інтереси, оскільки це може призвести до ухвалення рішень, що суперечать фундаментальним інтересам людства

Отже, одним із ключових викликів у сфері розвитку штучного інтелекту С. Рассел визначає проблему узгодження цінностей (value alignment problem). Розкриваючи її сутність, дослідник зазначає: «Системам штучного інтелекту важливо розуміти та дотримуватися людських цінностей, оскільки ці цінності визначають наше прийняття рішень та моральні міркування. Без належного узгодження цінностей AI системи можуть інтерпретувати інструкції буквально, що призводить до потенційно катастрофічних результатів» [479, с. 146]. У зв'язку з цим С. Рассел наголошує на необхідності міжнародної наукової співпраці та формування ефективних правових і технічних механізмів, спрямованих на забезпечення відповідності систем ШІ людським цінностям та інтересам. На його думку, лише за таких умов штучний інтелект може функціонувати як надійний і безпечний інструмент розвитку суспільства, а не як джерело потенційних загроз.

Поділяючи занепокоєння інших дослідників щодо соціальних наслідків

розвитку ШІ, С. Рассел також звертає увагу на ризик посилення соціальної нерівності та алгоритмічної дискримінації. Він наголошує, що створення систем штучного інтелекту без належного врахування їхнього впливу на різні соціальні групи, а також без залучення таких груп до процесу розробки технологій, може призвести до формування дискримінаційних алгоритмів. За відсутності цілеспрямованих правових та етичних механізмів протидії алгоритмічній упередженості (algorithmic bias) ШІ здатний поглиблювати соціально-економічну нерівність та посилювати існуючі суспільні диспропорції.

З метою мінімізації зазначених ризиків С. Рассел наголошує на необхідності постійного людського нагляду та контролю за функціонуванням систем штучного інтелекту. Розвиваючи концепцію «ШІ як хорошого партнера», він виходить із моделі взаємодії, за якої штучний інтелект має не заміщувати людину, а допомагати їй та розширювати її можливості. У зв'язку з цим дослідник виступає за обов'язкову інтеграцію людських цінностей, суджень та контролю у процеси ухвалення рішень системами ШІ, наголошуючи, що остаточне рішення у критично важливих питаннях повинно залишатися за людиною-оператором.

Узагальнюючи аналітичні застереження С. Рассела, слід зазначити, що весь спектр виокремлених ним загроз корелює з фундаментальною правовою дилемою: ризиком створення та функціонування автономних систем штучного інтелекту, не узгоджених із людськими цінностями, безпекою та суспільними інтересами.

Важливе місце у сучасному дискурсі щодо безпечного розвитку штучного інтелекту посідають праці Макса Тегмарка – відомого фізика та дослідника проблематики ШІ. Однією з ключових проблем, на яких акцентує увагу М. Тегмарк, є проблема контролю за розвитком високорозвинених інтелектуальних систем. На його думку, у міру зростання когнітивних можливостей штучного інтелекту існує ризик досягнення системами ШІ рівня надінтелекту (Artificial Superintelligence), здатного перевищити окремі

інтелектуальні можливості людини. У разі втрати ефективного людського контролю або функціонування таких систем у супереч інтересам людства наслідки можуть мати глобальний і потенційно деструктивний характер.

У зв'язку з цим М. Тегмарк наголошує на необхідності узгодження цілей та функціонування систем ШІ з людськими цінностями й етичними принципами, що має забезпечити безпечний і контрольований розвиток відповідних технологій.

Поряд із проблемою контролю М. Тегмарк висвітлює іншу екзистенційну загрозу – здатність штучного інтелекту виступати каталізатором соціально-економічної поляризації суспільства. Обґрунтовуючи цей виклик, він зазначає: «Якщо системи штучного інтелекту розробляються і впроваджуються не з урахуванням принципу справедливості, вони можуть посилити упередженість та дискримінацію у суспільстві. Це може призвести до подальшої поляризації та маргіналізації певних груп» [489, с. 182-183]. У зв'язку з цим дослідник наголошує на необхідності нормативного закріплення принципів справедливості, інклюзивності та алгоритмічної прозорості (explainable AI / XAI), покликаних мінімізувати ризики цифрової дискримінації ще на етапі розробки інтелектуальних систем.

Актуалізуючи ризики мілітаризації штучного інтелекту, М. Тегмарк висловлює категоричне застереження щодо перспектив використання повністю автономних систем озброєння (lethal autonomous weapons systems – LAWS). На його переконання, в умовах сучасних збройних конфліктів усунення людини з процесу ухвалення рішень щодо ураження цілей здатне призвести до катастрофічних наслідків, включаючи неконтрольовану ескалацію конфліктів та порушення норм міжнародного гуманітарного права.

З метою мінімізації таких ризиків М. Тегмарк виступає прихильником міжнародної наукової співпраці та демократичних механізмів регулювання розвитку штучного інтелекту. Він наголошує на важливості міждисциплінарної взаємодії за участю фахівців у сфері комп'ютерних наук, права, філософії та етики. На його думку, саме відкритий експертний діалог і міжнародна

координація здатні забезпечити формування ефективних правових і технічних механізмів захисту людства від неконтрольованого розвитку автономних систем.

Узагальнюючи підходи М. Тегмарка, слід зазначити, що основним джерелом потенційних загроз він вважає безвідповідальне ставлення до розробки та впровадження систем штучного інтелекту, орієнтоване виключно на технологічну, комерційну або геополітичну перевагу. У зв'язку з цим учений наголошує на необхідності формування стійких механізмів правового та технічного контролю, спрямованих на недопущення як поглиблення цифрової дискримінації, так і небезпечного використання автономного ШІ у військовій сфері.

Особливе місце у сучасному дискурсі щодо майбутнього штучного інтелекту посідають концептуальні розробки Р. Курцвейла – відомого футуролога та винахідника. Визнаючи значний потенціал розвитку ШІ, дослідник водночас застерігає щодо ризиків його неконтрольованої еволюції для людської цивілізації. Акцентуючи увагу на необхідності випереджального правового та технічного контролю, Р. Курцвейл наголошує: «якщо ми не зможемо правильно керувати вибухом інтелекту, результатом може стати катастрофа для людства» [428, с. 263].

Однією з ключових ідей Р. Курцвейла є прогноз щодо можливого досягнення системами штучного інтелекту рівня, за якого їхні когнітивні можливості перевищуватимуть людські. Хоча подібний технологічний прорив може створити безпрецедентні можливості для розвитку цивілізації, дослідник водночас застерігає, що він здатний спричинити втрату ефективного людського контролю над автономними системами. Екстраполюючи темпи технологічного розвитку, Р. Курцвейл припускає, що у часовому проміжку між 2029 та 2045 роками може настати етап Технологічної Сингулярності, коли штучний інтелект перевищить людські когнітивні можливості. За відсутності належного узгодження функціонування ШІ з людськими цінностями та інтересами це створює ризик ухвалення автономними системами рішень, які людина не зможе

повною мірою зрозуміти, передбачити або контролювати [428, с. 405-410].

Р. Курцвейл також звертає увагу на проблему алгоритмічної непрозорості високорозвинених систем ШІ. У разі стрімкого ускладнення інтелектуальних моделей автономні системи можуть ухвалювати рішення, які людина не зможе повною мірою зрозуміти або передбачити. У правовому аспекті це створює ризик неспроможності суспільства своєчасно прогнозувати та ефективно реагувати на потенційно небезпечні наслідки автономних дій штучного інтелекту.

Ще одним важливим викликом, на який звертає увагу Р. Курцвейл, є ризик неправомірного або зловмисного використання технологій штучного інтелекту. У міру розвитку високорозвинених систем ШІ особливого значення набуває необхідність формування чітких етичних і правових принципів їхнього використання. На думку дослідника, недостатня врегульованість процесів розробки та використання ШІ створює ризик його застосування у деструктивних цілях, зокрема для ведення кібервійн, масового цифрового спостереження або порушення фундаментальних прав людини [428, с. 405-410]. У зв'язку з цим Р. Курцвейл наголошує на необхідності забезпечення такого розвитку й застосування ШІ, який відповідатиме етичним принципам та інтересам безпеки людства [428, с. 412-416].

Окрему увагу дослідник приділяє впливу штучного інтелекту на сферу зайнятості. Ускладнення та розширення функціональних можливостей автономних систем створює ризик масштабного витіснення людської праці з окремих професійних сфер [428, с. 174-175]. Хоча розвиток нових технологій здатний формувати нові напрями зайнятості, перехідний період може супроводжуватися економічною нестабільністю, зростанням безробіття та поглибленням соціально-економічної нерівності [428, с. 197]. Саме тому Р. Курцвейл наголошує на необхідності завчасної адаптації державних і соціальних інститутів до умов технологічної трансформації суспільства [428, с. 209-215].

Побоювання Р. Курцвейла щодо розвитку штучного інтелекту пов'язані

насамперед із ризиком втрати ефективного людського контролю над високорозвиненими автономними системами, можливістю їхнього неправомірного використання, а також масштабним впливом технологічної автоматизації на сферу зайнятості. Дослідник наголошує, що подальший розвиток ШІ потребує врахування не лише технологічних переваг, а й соціальних, економічних та етичних наслідків, зокрема ризиків дестабілізації ринку праці та поглиблення демографічних криз. У зв'язку з цим він обґрунтовує необхідність відповідального та превентивного підходу до розробки і впровадження систем штучного інтелекту.

Отже, ключовою ідеєю праць Р. Курцвейла є необхідність формування превентивної моделі взаємодії людини та штучного інтелекту. Визнаючи значний потенціал розвитку ШІ, дослідник водночас наголошує, що без дотримання етичних принципів, узгодження функціонування ШІ з людськими цінностями та належного соціального й правового планування розвиток таких технологій може призвести до втрати контролю, зловживання автономними системами та масштабної соціально-економічної дестабілізації.

Компаративний аналіз підходів представників трансгуманістичного та футурологічного дискурсу дозволяє констатувати їхню загальну солідарність щодо визначення втрати людського контролю над штучним інтелектом як однієї з ключових екзистенційних загроз. Некерований розвиток автономних систем розглядається дослідниками як ризик втрати людиною можливості ефективно впливати на процеси ухвалення рішень та забезпечувати безпечне функціонування ШІ.

У контексті захисту людської гідності особливе значення надається проблемі невідповідності функціонування ШІ людським цінностям та моральним орієнтирам (Н. Бостром, С. Рассел). Буквальна інтерпретація алгоритмами людських команд без урахування морального контексту, соціального досвіду та етичних нюансів розглядається як чинник, здатний підривати людську автономію та справжність соціальної взаємодії. І. Маск та Р. Курцвейл додатково акцентують увагу на маніпулятивному потенціалі

штучного інтелекту, пов'язаному з використанням великих масивів даних, що в нових реаліях є доволі актуальною проблемою [518] та створює підвищені ризики неправомірного впливу на свідомість людини, порушення приватності та свободи волевиявлення. Водночас М. Тегмарк звертає увагу на небезпеку делегування автономним системам права ухвалення рішень у військовій сфері, що може призвести до деградації гуманістичних засад права та втрати людиною контролю над застосуванням сили.

Отже, у межах трансгуманістичного дискурсу захист людської гідності та безпеки пов'язується насамперед із необхідністю забезпечення людського нагляду, етичного програмування та збереження людини як центрального суб'єкта ухвалення суспільно значущих рішень

Не менш важливим викликом у контексті розвитку штучного інтелекту є проблема нерівномірного розподілу технологічних благ, що пов'язана з ризиками економічної нерівності та структурного безробіття. Н. Бостром звертає увагу на небезпеку дисбалансу сил унаслідок конкурентних перегонів у сфері ШІ, тоді як І. Маск, С. Рассел та Р. Курцвейл прогнозують масштабну автоматизацію праці, здатну суттєво посилити соціально-економічний розрив між різними групами населення. Своєю чергою, М. Тегмарк акцентує увагу на проблемі алгоритмічної упередженості (*algorithmic bias*), яка може поглиблювати дискримінацію та суспільну поляризацію. На думку дослідників, мінімізація таких ризиків потребує впровадження принципів справедливості та інклюзивності у процеси розробки систем штучного інтелекту, обов'язкового оцінювання алгоритмів на предмет дискримінаційного впливу (*fairness assessment*), а також належного соціального й правового планування технологічної трансформації суспільства.

Додатковий спектр застережень представників трансгуманістичного дискурсу охоплює ризики неправомірного використання високих технологій (І. Маск, Р. Курцвейл), а також загрозу витіснення людської праці та конкуренції між автономними системами й людиною (Н. Бостром). У зв'язку з цим дослідники наголошують на необхідності превентивного регулювання,

міждисциплінарної співпраці, формування етичних стандартів і розвитку міжнародної координації у сфері ШІ. Водночас штучний інтелект розглядається ними не як ворожа людині сила, а як інструмент і партнер, розвиток якого має здійснюватися під постійним людським контролем та відповідно до гуманістичних цінностей

Системний аналіз концептуальних підходів представників трансгуманістичного дискурсу дозволяє виокремити ключові етико-правові перестороги, які мають виступати критеріями нормативного обмеження та регулювання систем штучного інтелекту:

1) *приватність та захист персональних даних* – необхідність мінімізації ризиків маніпулювання поведінкою людини, порушення приватності та несанкціонованого цифрового контролю, що виникають унаслідок накопичення й обробки системами ШІ значних масивів даних;

2) *неупередженість та справедливість* – запобігання алгоритмічній упередженості (algorithmic bias), за якої системи ШІ, треновані на упереджених даних, здатні посилювати дискримінацію та соціальну нерівність; при цьому критерії оцінювання справедливості алгоритмів (fairness assessment) мають виконувати функцію механізму захисту вразливих соціальних груп;

3) *підзвітність та алгоритмічна прозорість* – забезпечення зрозумілості та інтерпретованості механізмів ухвалення рішень системами ШІ, оскільки ефект «чорної скриньки» (black box) унеможливорює ефективний контроль та підриває суспільну довіру;

4) *автономія людини та людський контроль* – недопущення ситуацій, за яких автономні системи штучного інтелекту функціонуватимуть усупереч людським інтересам, ігноруючи цінності, безпеку та принципи юридичної відповідальності;

5) *безпека та надійність систем ШІ* – формування механізмів мінімізації системних помилок, зловживань та технічних інцидентів, у тому числі шляхом запровадження засобів аварійного блокування та зупинки автономних систем (emergency stop);

б) *соціально-економічна безпека та адаптація суспільства до автоматизації* – необхідність створення державних і соціальних механізмів підтримки в умовах трансформації ринку праці, пов'язаної з автоматизацією, скороченням робочих місць та ризиками посилення соціальної поляризації.

Отже, сучасний науковий та правотворчий дискурс щодо безпечного розвитку штучного інтелекту фактично підтверджує актуальність застережень, свого часу сформульованих Х. Дрейфусом, водночас пропонуючи принципово інший підхід до регуляторного реагування. Йдеться не про загальне стримування технологічного прогресу, а про таргетоване обмеження використання ШІ у сферах, де ризики для прав людини, демократичних інститутів та соціальної справедливості є найбільш критичними.

Саме такий методологічно врівноважений підхід відображений у сучасних міжнародно-правових актах, зокрема у Законі Європейського Союзу про штучний інтелект (AI Act), концепція якого ґрунтується на поєднанні підтримки інноваційного розвитку з установленням чітких заборон і спеціальних превентивних режимів для високоризикових систем штучного інтелекту.

Таким чином, соціальні та догматичні передумови нормативного обмеження використання штучного інтелекту зводяться до кількох ключових тез.

По-перше, різні сфери застосування ШІ характеризуються неоднаковим рівнем ризику. Поряд із галузями, де потенційні переваги використання штучного інтелекту суттєво переважають можливі загрози навіть за умов мінімального регуляторного втручання, існують сфери, у яких будь-яка помилка, технічний збій або зловживання можуть спричинити незворотні наслідки для людини, суспільства чи держави.

По-друге, сама структура сучасного правопорядку вже містить нормативні орієнтири, які вказують на необхідність особливого правового режиму для рішень та технологій, що безпосередньо зачіпають життя, здоров'я, свободу, приватність, людську гідність і доступ до базових соціальних благ.

По-третє, зазначені правові орієнтири значною мірою збігаються з інтуїтивними та емпірично підтвердженими суспільними пересторогами щодо використання штучного інтелекту.

Такий підхід дозволяє перейти від загальнотеоретичних узагальнень до предметно-орієнтованого аналізу конкретних сфер сучасного й перспективного використання ІІІ – автономних систем озброєння, охорони здоров'я, правоохоронної діяльності та діяльності спеціальних служб, судочинства, освіти і науки. У межах кожної із зазначених сфер буде послідовно досліджено специфіку суспільних очікувань і побоювань, проаналізовано чинні правові режими, визначено характер трансформації ризиків під впливом ІІІ, а також обґрунтовано обмежувальні механізми, необхідні для забезпечення безпеки та захисту прав людини.

3.2. Правове регулювання використання штучного інтелекту в автономній зброї

Концептуальні підходи до обмеження використання ІІІ значною мірою кореспондують раннім етичним моделям контролю автономних систем, найбільш відомими з яких стали принципи роботехніки Айзека Азімова [294; 296]. Попри їх художнє походження, саме у них вперше було системно сформульовано ідею пріоритету безпеки людини над автономністю машини.

Перший закон робототехніки передбачав, що робот не може завдати шкоди людині або своєю бездіяльністю допустити заподіяння їй шкоди.

Другий закон визначав, що робот має виконувати накази людини, якщо вони не суперечать першому закону.

Третій закон встановлював обов'язок робота дбати про власну безпеку тією мірою, якою це не суперечить першому та другому законам.

У 1986 р. Айзек Азімов додав ще так званий «нульовий закон робототехніки» [295], відповідно до якого робот не може завдати шкоди людству або своєю бездіяльністю допустити заподіяння такої шкоди.

Зазначені підходи, але у сучасному баченні набули нових інтерпретацій у контексті етичних і правових пересторог щодо застосування ІІІ, насамперед у високоризикових сферах. Зокрема, у доповіді «Етика та управління штучним інтелектом у сфері охорони здоров'я» («Ethics and governance of artificial intelligence for health») Всесвітньої організації охорони здоров'я (ВООЗ) сформульовано базові етичні принципи та рамки управління ІІІ у медичній сфері, які передбачають:

- захист автономії людини;
- сприяння добробуту та безпеці людей і суспільним інтересам;
- забезпечення прозорості та зрозумілості функціонування систем ІІІ;
- підвищення відповідальності та підзвітності;
- забезпечення інклюзивності та справедливості;
- просування гнучкого та сталого штучного інтелекту [530].

Важливим аспектом оцінки потенціалу та ризиків використання ІІІ є розуміння його принципової відмінності від інших технічних систем, відомих раніше. *Ключовою ознакою ІІІ є машинне навчання. Саме машинне навчання формує принципово інший підхід до створення програмного забезпечення, оскільки ІІІ навчається на прикладах [310], а не функціонує виключно на основі наперед запрограмованого результату.*

Саме завдяки переходу від жорстко запрограмованих інструкцій до навчання на даних системи ІІІ здатні не лише відтворювати наперед задані алгоритми, а й виявляти приховані закономірності у великих масивах інформації, узагальнювати попередній досвід та адаптувати свою поведінку до нових ситуацій. Це, з одного боку, відкриває значні можливості для автоматизації складних аналітичних завдань, а з іншого – робить результати роботи таких систем чутливими до якості, репрезентативності та неупередженості тих даних, на яких вони «вчаться». У зв'язку з цим оцінка ризиків використання ІІІ має враховувати не лише технічні характеристики моделі, а й джерела, структуру та історичну зумовленість навчальних наборів даних.

Окреслюючи специфіку цього процесу, дослідники зазначають, що «машинне навчання є практичним застосуванням ІІІ, яке імітує зазначену здатність і дозволяє комп'ютерним програмам переймати досвід» [474]. Разом з тим особливого значення для сфери кримінального правосуддя набувають технології ідентифікації образів, оскільки «людина здатна ефективно виявляти системні зв'язки і на основі досвіду вчитися диференціювати предмети, осіб, складні емоційні стани, інформацію та щоденні умови, тоді як ІІІ спроможний відтворити цю людську властивість за допомогою алгоритмів та апаратного забезпечення» [474].

Вказані функціональні властивості машинного навчання пояснюють, чому ІІІ поступово проникає в найбільш чутливі сфери, де ставкою є не лише економічна ефективність, а й життя, безпека, честь, гідність та фундаментальні права людини. У військовій сфері цей вплив виявляється у створенні автономних систем, здатних самостійно ідентифікувати цілі та приймати рішення про застосування сили; у правоохоронній діяльності – у впровадженні предиктивної аналітики, розпізнавання облич і профілювання ризиків. Паралельно з цим у правосудді застосовуються інструменти аналізу доказів та оцінки ймовірності рецидивів, у медицині – діагностичні системи підтримки прийняття клінічних рішень (CDSS), а в освіті – технології адаптивного навчання, автоматизованого оцінювання та аналізу навчальної поведінки здобувачів.

У всіх наведених випадках традиційні людські когнітивні механізми доповнюються або частково замінюються алгоритмічними моделями, що якісно змінює характер супутніх ризиків та актуалізує вимоги до правового контролю.

Водночас у кожній із зазначених сфер конфігурація суспільно небезпечних наслідків є специфічною. Зокрема, для автономної зброї ключовим постає питання допустимості делегування машині рішень про позбавлення життя, дотримання норм міжнародного гуманітарного права та встановлення контролю за розробкою і розповсюдженням військових систем ІІІ.

У діяльності поліції та спецслужб у центрі уваги перебувають ризики масового спостереження, довільного втручання в приватне життя, селективного переслідування та зловживання спеціальними повноваженнями під прикриттям «об'єктивних» алгоритмів. Для системи правосуддя вагому небезпеку становлять загрози підміни судового розсуду непрозорими моделями, посилення структурної дискримінації та підлив гарантій справедливого суду. У медичній галузі критичними є помилкові клінічні рішення, нерівний доступ до лікування та дискримінація вразливих груп, а в освітньому просторі – академічна недоброчесність, алгоритмічно упереджене оцінювання, надмірний нагляд за здобувачами та ерозія ролі педагога.

З огляду на таку різноманітність ризиків подальший аналіз буде структуровано за п'ятьма блоками (підрозділами 3.2.1-3.2.5), що відповідають ключовим секторам застосування ШІ з підвищеним ризиком для прав людини та безпеки: автономні системи озброєння, правоохоронна діяльність і робота спецслужб, правосуддя, медична сфера та освіта. У кожному з підрозділів буде проаналізовано чинні та проєктні міжнародні й європейські стандарти, включно з підходом Регламенту про штучний інтелект (AI Act) до класифікації відповідних систем як високоризикових. На основі цього окреслено межі допустимого використання ШІ, визначено необхідні обмеження, а також запропоновано концептуальні орієнтири для адаптації цих підходів у правовому полі України з урахуванням її безпекового контексту, освітньої політики та євроінтеграційних зобов'язань.

Обрані для подальшого аналізу сфери – автономні системи озброєння, медицина, правоохоронна діяльність та діяльність спецслужб, правосуддя, а також освіта і наука – не вичерпують усіх можливих галузей застосування штучного інтелекту. Проте вони становлять ядро тих сфер, де поєднуються три ключові критерії підвищеного ризику.

1. Безпосередній деструктивний вплив на життя, здоров'я, тілесну недоторканність і фізичну безпеку індивіда (воєнна сфера, охорона здоров'я, правопорядок).

2. Вирішальне значення для забезпечення та реалізації права на справедливий суд і процесуальні гарантії (правоохоронна діяльність, судочинство).

3. Тривалий, кумулятивний вплив на формування людського капіталу, ціннісних орієнтирів і здатності до автономного мислення (освіта і наука).

Зазначена селекція повною мірою кореспондує регуляторному підходу Регламенту про штучний інтелект (AI Act), де вказані галузі переважно віднесені до категорії високоризикових або чутливих. Своєю чергою, сучасний український контекст, обтяжений чинниками повномасштабної війни, інтенсивних інформаційно-психологічних операцій і радикальної цифровізації публічних послуг, робить дослідження цих секторів найбільш репрезентативним.

Для забезпечення методологічної єдності у кожному з наступних підрозділів дотримано уніфіковану структуру викладу, що передбачає: окреслення фактичних та прогнозованих технологічних сценаріїв застосування ШІ у відповідній сфері; виокремлення ключових застережень й ризиків з урахуванням міжнародного дискурсу та вітчизняного досвіду; критичний аналіз наявних правових режимів на міжнародному, європейському та національному рівнях з метою виявлення правових прогалин; формулювання пропозицій щодо імплементації обмежувальних і запобіжних механізмів обмежувальних і запобіжних механізмів.

Такий предметно орієнтований підхід дозволить не лише конкретизувати загальні теоретичні та догматичні засади обмеження використання штучного інтелекту, а й довести, що потреба у спеціальних обмежувальних механізмах щодо технологій ШІ має прагматичний галузевий характер і повинна знаходити своє відображення у стратегічних політичних рішеннях, спеціальному законодавстві та підзаконних нормативно-правових актах.

З огляду на застереження провідних експертів у галузі високих технологій (зокрема оцінки Б. Гейтса щодо пріоритетного розвитку воєнних технологій [325]), а також ризики непрогнозованої поведінки автономних

систем, стає очевидним, що людство наблизилося до межі, коли нормативно-правове обмеження використання ІІІ є не менш важливим, ніж його технологічне проектування. Оскільки повна відмова від автоматизації вже фактично неможлива, саме воєнний сектор виступає первинним випробуванням здатності міжнародного права контролювати цифрові загрози. У зв'язку з цим особливої актуальності набуває питання правової природи та меж допустимості функціонування систем, здатних діяти без безпосередньої участі людини.

Правове регулювання використання штучного інтелекту в автономних системах озброєння (Autonomous Weapon Systems; далі – АСО) та летальних автономних системах озброєння (Lethal Autonomous Weapons Systems; далі – ЛАСО) формується в специфічному нормативному полі, яке істотно відрізняється від загальної ринково орієнтованої моделі регулювання ІІІ у цивільних сферах. На відміну від механізмів управління ризиками, характерних для загального законодавства у сфері цифрових технологій, відповідний нормативний підхід ґрунтується насамперед на положеннях міжнародного гуманітарного права, спеціальних міжнародних конвенціях щодо окремих видів звичайної зброї, офіційних позиціях Міжнародного Комітету Червоного Хреста (International Committee of the Red Cross; далі – МКЧХ) та Організації Об'єднаних Націй (United Nations; далі – ООН), а також на експертних підходах до етики застосування летальної сили.

Функціональне призначення АСО та ЛАСО орієнтоване на безпосередню участь у збройних конфліктах, забезпечення тактичної автономії, контроль над інформаційним простором поля бою, а також на підтримку військовослужбовців і систем командування та управління (C2) [409]. З огляду на оборонну специфіку таких завдань, Регламент про ІІІ (AI Act) встановлює для них імперативне виключення. Зокрема, у частині 3 статті 2 документа визначено, що він «не застосовується до систем ІІІ, якщо і остільки вони виводяться на ринок, вводяться в експлуатацію або використовуються з модифікацією чи без виключно для військових, оборонних або цілей

національної безпеки, незалежно від типу суб'єкта, який здійснює таку діяльність».

Відповідно, нормативно-правові обмеження застосування ІІІ в межах АСО та ЛАСО на сучасному етапі зафіксовані у комплексі джерел, а не в єдиній спеціалізованій конвенції. До зазначеного масиву належать такі групи документів:

1. **Міжнародне гуманітарне право (МГП).** Базові імперативи містяться у Женевських конвенціях про захист жертв війни, Додаткових протоколах до них [77], а також у Конвенції про заборону або обмеження застосування конкретних видів звичайної зброї, які можуть вважатися такими, що завдають надмірних ушкоджень або мають невибірккову дію 1980 року (КЗЗ) та протоколах до неї [111]. Ці акти встановлюють універсальні заборони на використання невибіркових, надмірно жорстоких чи неконтрольованих засобів ведення війни, що поширюються на будь-які перспективні види озброєнь, включно із системами на основі ІІІ;

2. **Позиційні документи МКЧХ.** Офіційні роз'яснення Комітету [410] орієнтують держави на імплементацію нових юридично обов'язкових норм, спрямованих на повну заборону окремих категорій АСО та жорстке обмеження систем із високим рівнем автономії критичних функцій.

3. **Матеріали Групи урядових експертів ООН.** Мандати й звіти Групи урядових експертів з ЛАСО (GGE on LAWS), зокрема схвалені 11 Керівних принципів (Guiding Principles) щодо АСО та ЛАСО [392], безпосередньо регламентують автономні операційні функції (ідентифікацію та ураження цілей), підтверджують обов'язковість дотримання МГП і констатують необхідність збереження ефективного людського контролю (*meaningful human control*) над оборонними системами.

4. **Резолюції та доповіді інституцій ООН.** Ключове значення мають Резолюції Генеральної Асамблеї ООН № 78/241 «Летальні автономні системи озброєння» (2023 р.) [507] та № 79/77 «Летальні автономні системи озброєння» (2024 р.) [509], а також відповідні доповіді Генерального секретаря ООН. Ці

документи формують глобальну політико-правову рамку, закликають до кодифікації нових норм і підкреслюють, що інтеграція технологій ІІІ у мілітарну сферу має здійснюватися виключно з дотриманням принципів міжнародного права та захисту прав людини.

Аналізуючи динаміку правової дискусії щодо мілітарних технологій, Р. Г. Меликов слушно зауважує, що хоча обговорення автономних систем озброєння у площині міжнародного гуманітарного права триває вже тривалий час, саме повномасштабне російське вторгнення в Україну у 2022 році актуалізувало це питання з гостротою, до якої доктрина міжнародного права виявилася теоретично неготовою. Дослідник наголошує, що першочерговим викликом залишається забезпечення дотримання базових принципів міжнародного гуманітарного права – розрізнення та пропорційності. Стрімка еволюція автономних систем озброєння формує комплекс взаємопов'язаних правових, політичних і морально-етичних проблем, за яких нормативні підходи, розроблені щодо одного типу технологій, швидко втрачають ефективність стосовно інших. Це, своєю чергою, зумовлює нагальну потребу у формуванні цілісної системи нормативного регулювання використання АСО в умовах збройних конфліктів [149].

Науковці визначають категорії ризиків, пов'язаних з розробкою, використанням та експортом автономних систем озброєння (АСО).

По-перше, ризик порушення норм міжнародного гуманітарного права, зокрема принципів розрізнення, пропорційності та вжиття запобіжних заходів, закріплених у Додатковому протоколі І до Женевських конвенцій 1949 року. Недостатня здатність автономних систем розмежовувати комбатантів і цивільних осіб або оцінювати співвідношення між військовою перевагою та можливими втратами серед цивільного населення може спричинити порушення міжнародного гуманітарного права, що, залежно від обставин, тягне міжнародно-правову відповідальність держави або індивідуальну кримінальну відповідальність за воєнні злочини [148, с. 317].

По-друге, ризик атрибуції відповідальності, який полягає у складності встановлення юридичного зв'язку між автономними діями системи, державою чи конкретною особою. Високий рівень автономності АСО ускладнює визначення суб'єкта відповідальності, створюючи так званий «вакуум відповідальності», оскільки сама система штучного інтелекту не є суб'єктом права [84, с. 401].

По-третє, ризик порушення міжнародного права щодо застосування сили. Автономне функціонування таких систем може призвести до неконтрольованої ескалації збройного конфлікту, порушення заборони застосування сили, закріпленої у статті 2 Статуту ООН, а також принципів необхідності та пропорційності під час реалізації права держави на самооборону відповідно до статті 51 Статуту ООН [84, с. 401].

По-четверте, ризик недостатності міжнародно-правового регулювання, який обумовлений відсутністю універсального міжнародного договору, що комплексно визначав би правові засади розробки, використання та контролю автономних систем озброєння і військового штучного інтелекту [80, с. 92].

Варто вказати, що підґрунтя для дефініювання цих систем було закладене Міжнародним Комітетом Червоного Хреста ще у 2014 році в експертному звіті «Технічні, військові, правові та гуманітарні аспекти автономних систем озброєння»². У цьому документі АСО визначалися як перспективний ресурс для держав у контексті подальшого вивчення супутніх технічних, правових та етичних викликів [409]. Незважаючи на відсутність єдиного універсального визначення, у тезаурусі звіту МКЧХ було запропоновано розглядати АСО як зброю, здатну самостійно вибирати та атакувати цілі, тобто таку, що володіє автономією у «критичних функціях» [409] захоплення, відстеження, селекції та безпосереднього вогневого ураження. Отже, МКЧХ ще на початкових етапах дискусії прогнозував появу систем, запрограмованих на автономне прийняття

² Autonomous weapon systems technical, military, legal and humanitarian aspects. Expert meeting report. International Committee of the Red Cross. 01/11/ 2014. URL: <https://www.icrc.org/en/document/report-icrc-meeting-autonomous-weapon-systems-26-28-march-2014>

рішень та здійснення деструктивного впливу без прямої участі людського оператора.

Разом з тим станом на сьогодні міжнародно-правовий статус АСО залишається нормативно некодифікованим. Такий правовий вакуум частково зумовлений тим, що реальне функціонування таких комплексів пов'язане не стільки з окремими моделями штучного інтелекту, скільки з інтегрованими цифровими екосистемами, побудованими на концепції Інтернету речей (Internet of Things – IoT). У мілітарній сфері ця технологічна парадигма трансформувалася у концепції Інтернету військових речей [313] (далі – ІВР; англ. Internet of Military Things – IoMT) та Інтернету речей поля бою [490] (далі – ІБР; англ. Internet of Battlefield Things – IoBT).

Організація Північноатлантичного договору (НАТО) [457; 456], окремі її держави-члени [515; 345; 400], а також інші країни світу активно здійснюють розробку АСО на базі технологій Інтернету речей та штучного інтелекту, включно з ЛАСО, які забезпечують суттєву асиметричну перевагу в сучасних збройних конфліктах. З огляду на це прогнозується, що у перспективі ведення військових операцій значною мірою залежатиме не від живої сили, а від взаємопов'язаних технологічних комплексів. Це передбачає інтеграцію потенціалу безпілотних систем і машинного навчання для досягнення принципово нового рівня оборонних спроможностей. Інтеграція АСО з архітектурою ІВР та ІБР дозволяє об'єднати військовослужбовців із когнітивними технологіями, інтегрованими у засоби індивідуального захисту, зв'язку та озброєння. Подібна конвергенція розширює сенсорне сприйняття особового складу, оптимізує ситуаційну обізнаність, забезпечує предиктивну аналітику, підвищує якість оцінки операційних ризиків та формує єдиний інформаційно-координаційний простір [501].

У подальшому допустимо очікувати поглиблення синергії цих систем із ШІ, що дозволить не лише агрегувати та транслювати тактичні дані, а й делегувати алгоритмам функцію прийняття рішень у визначених сферах застосування. Незважаючи на те, що сучасні проєкти АСО переважно

базуються на мережевих інфраструктурах Інтернету речей, етичні застереження та правові рамки, які формуються під час їхнього розгортання, згодом екстраполюватимуться на процеси нормативного регулювання АСО, що функціонують на основі штучного інтелекту.

Доцільно детальніше проаналізувати потенційні спроможності та класифікацію АСО, що функціонують у контурі ІВР та ІБР, а також наявні концепції етичних обмежень їх застосування з урахуванням подальшої екстраполяції цих підходів на мілітарні системи нового покоління.

Вагомим напрямом розвитку ІБР виступає організація тактичної взаємодії між автономними цифровими агентами та військовослужбовцями. Автономні агенти характеризуються високою швидкістю аналітичних операцій і реакцій, що забезпечує оперативне реагування на динамічну зміну бойових обставин без зниження загальної ефективності місії. Зокрема, такі спроможності критично важливі під час ведення бойових дій у складних міських умовах [430].

Водночас проєктування АСО на базі технологій Інтернету речей виступає суперечливим технологічним чинником, оскільки, крім оптимізації точності та оперативності вогневого ураження, воно створює суттєві загрози для архітектури глобальної безпеки. Імовірність технічних збоїв в алгоритмах автономної зброї або її несанкціонованого захоплення деструктивними суб'єктами становить критичний ризик для життя населення та стратегічної стабільності.

На відміну від конвенційних засобів ураження, АСО спроможні функціонувати в автономному режимі. Подібний ступінь самостійності обумовлює підвищений рівень операційної небезпеки, оскільки після активації комплексу пряме дистанційне керування ним може бути ускладнене або неможливе. У зв'язку з цим виникає реальний ризик системних помилок моделі, що здатні призвести до ненавмисного завдання шкоди цивільним об'єктам або ураження власних військ («дружнього вогню»). Крім того, потрапляння АСО до суверенно неконтрольованих воєнізованих формувань чи терористичних угруповань створює передумови для актів агресії та масових руйнувань.

Окреслюючи перспективи впровадження III та Інтернету речей у мілітарну сферу, Ілон Маск зазначає, що штучний інтелект здатний забезпечити наявність більш досконалої зброї на полі бою, яка реагує швидше за будь-яку людину. За його оцінками, будь-які майбутні війни між технологічно розвиненими державами або країнами, які володіють безпілотними технологіями, трансформуються переважно у протистояння дронів [452]. Наведений приклад використання безпілотних літальних апаратів ілюструє концепцію ІБР, яку дослідники та практики все частіше розглядають у контексті розвитку III [418].

Подібні підходи поділяють й інші фахівці. Зокрема, Олександр Котт, аналізуючи характеристики інтелектуальної автономії в межах архітектури ІБР, фактично ототожнює її з функціоналом III, вказуючи, що численні мережеві об'єкти зі штучним інтелектом заповнять поле бою майбутнього, діятимуть у тісній співпраці з військовослужбовцями та вестимуть бойові дії у складі команд у надзвичайно ворожому середовищі [423].

Екзистенційний характер цих загроз став підставою для широкого міжнародного заклику. Так, у 2017 році до Організації Об'єднаних Націй було спрямовано відкритий лист за підписом понад 100 засновників провідних світових компаній у сфері III та робототехніки. У цьому документі автори наголосили, що летальна автономна зброя загрожує стати третьою революцією у військовій справі. Після розгортання таких систем вони дозволять вести збройні конфлікти у значно більших масштабах, ніж будь-коли, і в часових вимірах, які людина не здатна досягнути. Дослідники застерегли, що ЛАСО може перетворитися на зброю терору, яку деспоти та радикальні угруповання застосовуватимуть проти мирного населення, або ж на системи, піддані кібератакам із метою зміни їхньої цільової поведінки. Наголошуючи на обмеженості часу для прийняття рішень, автори листа резюмували: «Коли цю скриньку Пандори відкриють, її буде вкрай важко закрити» [385].

О. В. Кутовий та С.К. Бурма справедливо підкреслюють: «У цьому контексті особливої уваги заслуговує практика Європейського суду з прав

людини (далі – ЄСПЛ), який уже неодноразово розглядав справи, пов'язані з надмірним застосуванням сили, обмеженням приватності в умовах технологічного нагляду, неналежним розслідуванням смерті або тілесних ушкоджень. Зобов'язання держав у сфері захисту права на життя, заборони катувань, рабства та дотримання принципу *nulla poena sine lege* мають характер *erga omnes* і залишаються чинними за будь-яких обставин» [141].

Зокрема, доцільно звернути увагу, що Практика Європейського суду з прав людини послідовно виходить із того, що право на життя, гарантоване статтею 2 Конвенції про захист прав людини і основоположних свобод, покладає на державу не лише негативний обов'язок утримуватися від свавільного позбавлення життя, а й позитивний обов'язок створити належну систему правового регулювання та контролю за діяльністю, яка потенційно становить загрозу життю людини.

Так, у справі *McCann and Others v. the United Kingdom* (№ 18984/91, рішення від 27 вересня 1995 року) ЄСПЛ наголосив, що навіть за умов боротьби з тероризмом застосування сили повинно відповідати критерію «абсолютної необхідності» (*absolute necessity*), а державні органи зобов'язані належним чином планувати та контролювати свої операції з метою мінімізації ризику для життя людини [437].

Аналогічний підхід відображено у справі *Güleç v. Turkey* (№ 21593/93, рішення від 27 липня 1998 року), де ЄСПЛ зазначив, що позитивні зобов'язання держави за статтею 2 Конвенції охоплюють не лише заборону свавільного позбавлення життя, а й обов'язок забезпечити належне планування, організацію та контроль діяльності державних органів, якщо така діяльність пов'язана з потенційною небезпекою для життя людини [394].

У справі *Ergi v. Turkey* (№ 23818/94, рішення від 28 липня 1998 року) ЄСПЛ підкреслив, що навіть під час проведення операцій у зоні збройного конфлікту держава повинна вживати всіх можливих заходів для мінімізації ризику для цивільного населення, дотримуючись принципів обережності та пропорційності при застосуванні сили [357].

Наведена практика свідчить, що у випадках, коли діяльність або технології створюють потенційну загрозу життю людини, держава зобов'язана забезпечити превентивне правове регулювання, ефективний контроль та належні механізми управління ризиками. Саме цей підхід, сформований у практиці ЄСПЛ, може бути покладений в основу ризик-орієнтованих тестів правової оцінки використання систем III [141, с. 190].

У 2017 році Уряд США виділив 25 мільйонів доларів США на перші п'ять років десятирічної програми досліджень у межах наукового об'єднання (*Alliance*), створеного на базі Дослідницької лабораторії Сухопутних військ Командування розвитку бойових спроможностей армії США (англ. *U.S. Army Combat Capabilities Development Command Army Research Laboratory*, далі – DEVCOM ARL) [487]. Метою цього об'єднання визначено вивчення потенціалу ІБР та розробку інтелектуальних цільових технологій. До складу зазначеного консорціуму, окрім фахівців DEVCOM ARL, увійшли представники Університету Карнегі-Меллона, Університету Каліфорнії в Берклі, Університету Каліфорнії в Лос-Анджелесі, Університету Массачусетсу, Університету Південної Каліфорнії, Джорджтаунського університету та Університету Іллінойсу [513].

Фундаментальне завдання проєкту полягає у «розвитку базової науки про всеосяжне, розподілене, гетерогенне зондування та обчислення у великомасштабних мережах для покращення контролю над інформаційним бойовим простором і тактичною автономією». Очікується, що це забезпечить мініатюризацію засобів, інформаційну підтримку військовослужбовців та систем командування й управління (C2), а також підвищить аналітичні спроможності протидії супротивнику, гарантуючи «інтелектуальну, гнучку та стійку перевагу у швидкості прийняття рішень в умовах значної протидії та за оптимального темпу» [513]. Прикметно, що в офіційних стратегічних цілях проєкту відсутні прямі посилання на розробку класичного штучного інтелекту, а акцент зміщено на інфраструктуру ІБР та ІБР. Натомість аналіз визначеної мети чітко засвідчує людиноцентрований характер ініціативи, спрямований на

«покращення контролю» та інформаційне забезпечення особового складу й систем командування і управління. Оприлюднені дані відображають лише відкриту частину мілітарних досліджень, тоді як значний масив технологічних розробок здійснюється в умовах суворой конфіденційності.

Умови, зумовлені повномасштабною збройною агресією РФ проти України з 2022 року, суттєво актуалізували застереження щодо застосування АСО. Вони підсилили розуміння як критичних загроз таких технологій, так і невідворотності їхнього подальшого розвитку. Попри дискусії про потенційні ризики мілітаризації ШІ, жодна держава світу не здатна в односторонньому порядку припинити проектування подібних систем, як не зупиняються сьогодні процеси впровадження інфраструктур ІВР та ІБР, зважаючи на їхні виняткові асиметричні переваги над людським ресурсом у сучасних воєнних конфліктах.

Як і базовий Інтернет речей, системи ІВР та ІБР не володіють суб'єктністю у прийнятті рішень: їхній функціонал обмежений збором, аналітичною обробкою та трансляванням інформації, тоді як остаточний вибір (зокрема щодо застосування засобів ураження) залишається за людиною-оператором. Натомість системи на основі ШІ спроможні генерувати автономні рішення за визначенням, що відображає саму сутність АСО нового покоління. Характеризуючи цю загрозу, Ілон Маск у контексті інтеграції ШІ метафорично зазначив, що наявність технологічного «джина», здатного виконати будь-яке завдання, формує фундаментальну небезпеку [452].

Своєю чергою, у Звіті наради експертів Міжнародного Комітету Червоного Хреста «Автономні системи зброї: технічні, військові, правові та гуманітарні аспекти» [409] зафіксовано консолідовану позицію фахівців, які пропонують розглядати автономну зброю як програмно-апаратні комплекси на базі ШІ, що запрограмовані на самостійне визначення власних дій, прийняття складних рішень та адаптацію до умов операційного середовища. Попри розбіжності у поглядах експертів щодо часових рамок появи повнофункціональних систем такого типу [409], домінує консенсус стосовно нагальної потреби зосередження уваги на регулюванні взаємодії між людиною

та машиною. Це є ключовою умовою для гарантування збереження ефективного людського контролю над функціонуванням зазначених систем.

Попри відсутність офіційного декларування АСО на базі повнофункціонального штучного інтелекту, у межах концепцій ІВР та ІБР на сучасному етапі виокремлюють три базові моделі інтеграції людського оператора в контур управління системами. Залежно від ступеня залученості людини, ці моделі класифікуються у такий спосіб:

людина «в контурі управління» («human-in-the-loop») – архітектура, за якої система виконує тактичні завдання, обрані оператором, проте допускає поточне коригування параметрів місії та вимагає обов'язкової санкції людини для здійснення вогневого ураження [454];

людина «над контуром управління» («human-on-the-loop») – модель, у межах якої комплекс після активації діє автономно, але надає оператору можливість здійснювати моніторинг операційного процесу та оперативно втручатися в алгоритм дій у разі виявлення аномалій або виникнення критичних ситуацій;

людина «поза контуром управління» («human-out-of-the-loop») – автономна система, яка після первинного запуску спроможна самостійно здійснювати селекцію та ураження цілей без будь-якого подальшого залучення чи контролю з боку людини [321].

Реалізація схеми людина «поза контуром управління» пов'язана з найвищими юридичними та безпековими ризиками, оскільки після активації комплексу оператор повністю втрачає можливість впливати на вибір об'єктів атаки. В умовах динамічної зміни обстановки на полі бою (наприклад, під час розгортання роїв безпілотних апаратів) технічні обмеження сенсорів або похибки алгоритмів ШІ можуть призвести до помилкової ідентифікації цивільних об'єктів. Це прямо порушує фундаментальний принцип розрізнення МГП та створює загрозу неконтрольованої ескалації бойових дій, де зброя фактично трансформується у самостійного суб'єкта (*актора*).

Крім того, застосування таких систем суттєво ускладнює встановлення юридичної відповідальності за порушення законів та звичаїв війни. Оскільки оператор лише здійснює первинний запуск, а деструктивні рішення приймає програмний алгоритм, виникає феномен «прогалини у відповідальності» (*accountability gap*), що суперечить чинним імперативам міжнародного права. Додатковим деструктивним чинником виступає вразливість перед зовнішнім кібервтручанням: хакерські атаки здатні перехопити управління АСО, змінити польотні завдання чи цільові орієнтири, перетворюючи оборонні комплекси на інструмент терору, протидіяти якому за відсутності механізмів віддаленого відключення буде неможливо.

Важливим застереженням на цьому етапі дослідження є необхідність акцентування уваги на феномені «упередження автоматизації» (*automation bias*), виявленому під час бойового застосування АСО. Зазначене явище становить один із ключових психологічних ризиків у процесі взаємодії оператора з АСО в контурі ІБР та ІШ. Його сутність полягає в надмірній довірі людини до рекомендацій або рішень, згенерованих автоматизованою системою, що призводить до ігнорування суперечливих даних чи операційних аномалій. Це зумовлює критичні помилки, виконання хибних команд або пропуск реальних загроз. Вказаний ефект був емпірично зафіксований під час досліджень процесів управління роями безпілотних літальних апаратів (зокрема, американських мікро-БПЛА *Perdix* [345]) та аналізу функціонування тактичних комплексів (таких як ізраїльська система *Iron Dome* [417]). Розкриваючи зміст *automation bias*, дослідники визначають його як схильність індивіда беззастережно покладатися на інформацію, надану машиною, та надмірно довіряти їй навіть тоді, коли суперечливі або альтернативні дані з інших джерел є доступними або можуть бути отримані за умови належного моніторингу [326].

Етичний вакуум, характерний для моделі «людина поза контуром управління» (*human-out-of-the-loop*), загрожує деструкцією системи стримувань і противаг у військах, оскільки особовий склад психологічно звикає до

делегування летальних рішень алгоритмам ШІ під постійним впливом «упередження автоматизації». У довгостроковій перспективі це здатне призвести до накопичення системних помилок, які нівелюватимуться під приводом «технологічного вдосконалення». Подібна динаміка створює передумови для розгортання неконтрольованої гонки озброєнь із повною автономією мілітарних систем, що повністю ігноруватиме сучасні заклики ООН та МКЧХ щодо імперативної заборони таких моделей.

У межах моделі «людини над контуром управління» (*human-on-the-loop*) оператор здійснює моніторинг автономних операцій, за якого безпосереднє втручання алгоритмічно передбачене виключно у разі виявлення аномалій. Подібна архітектура певною мірою створює ілюзію контролю, проте практичні чинники, такі як затримка передачі даних унаслідок застосування засобів радіоелектронної боротьби, пригнічення сигналу, кібератак чи критичного перевантаження мережі, нівелюють ефективність моніторингу. Наведені деструктивні фактори стають особливо критичними під час координації дій роїв безпілотних апаратів.

Крім того, автономний комплекс спроможний здійснити вогневе ураження цілі (зокрема помилкове) до моменту фізичної реакції оператора, оскільки людина об'єктивно не здатна оперативно опрацювати надмірний масив вхідних сигналів. Ця проблема загострюється під час ведення бойових дій у щільній міській забудові за наявності множинних цілей та під впливом ефекту упередження автоматизації (*automation bias*). З огляду на це виникає комплекс невирішених проблем у площині гуманізму, дотримання імперативів МГП та встановлення міжнародно-правової відповідальності.

Своєю чергою, модель «людини у контурі управління» (*human-in-the-loop*) передбачає безперервне коригування параметрів місії оператором. Проте в умовах функціонування ІБР такий підхід істотно обмежує швидкість реакції всієї системи порівняно з повністю автономними комплексами. Досліджуючи психофізіологічні аспекти цієї взаємодії, Дж. Морроу звертає увагу на фактор ментальної втоми оператора під час управління роєм дронів, зазначаючи, що

людина перетворюється на обмежувальний чинник системи [448]. Суб'єктивні фактори (стрес, виснаження) неминуче призводять до помилок у процесі селекції цілей, особливо за високої щільності об'єктів у зоні бойових дій.

Етичні дилеми «моделі людини у контурі управління» *human-in-the-loop* зосереджені навколо колосального психоемоційного навантаження на людину, яка безпосередньо санкціонує завдання летальних ударів. Відтак у цій системі морально-психологічний стан, витривалість та емоційна стабільність військовослужбовця виступають визначальними критеріями, які, проте, піддаються природним людським обмеженням.

Отже, інтеграція технологій Інтернету речей у процесі проєктування АСО пов'язана з комплексом істотних ризиків, серед яких ключовими є непередбачуваність операційної поведінки, помилки під час ідентифікації цілей, а також ускладненість або неможливість екстреного дистанційного вимкнення комплексів у процесі виконання місії [492]. Ефективним інструментом мінімізації зазначених загроз [453] здатна стати імплементація уніфікованих етичних настанов щодо розробки та застосування таких видів озброєнь [360]. Водночас потенційні виклики зростатимуть за експонентою у разі переходу до АСО на базі повнофункціонального ШІ, оскільки спектр їхнього алгоритмічного впливу розшириться з координаційно-виконавчої площини на сферу автономного прийняття рішень та управління. З огляду на це, попри те, що використання ШІ як самостійного суб'єкта мілітарних відносин перебуває на стадії розробки, питання проактивного правового регулювання етичних меж його застосування є нагальним уже сьогодні. Саме такий превентивний підхід дозволить обмежити неконтрольовані технологічні небезпеки.

Відповідно, поточні спроби нормативного закріплення етичних засад функціонування АСО в межах концепцій ІВР та ІБР мають стати концептуальним фундаментом для майбутньої регламентації мілітарних систем на основі ШІ. Головним орієнтиром у цьому процесі мають виступати єдині, консолідовані та стратегічні принципи воєнної етики. Наголошуючи на

пріоритетності випереджального оцінювання загроз, Поль Шарре зазначає: «Поки військові думають про те, як інтегрувати автономію в перспективну зброю, ми маємо забезпечити належну оцінку ризиків, пов'язаних із її функціонуванням. Збої в роботі автономної зброї здатні призвести до жертв серед цивільного населення, мілітарного братовбивства або ненавмисної ескалації кризових ситуацій. Розуміння цих ризиків є критично важливим як для політичних діячів і фахівців, відповідальних за закупівлю та розробку автономного озброєння, так і для військових командирів, які безпосередньо використовують його в бойових умовах» [360, с. 7].

У сучасному науковому дискурсі підходи до етичних обмежень застосування автономної зброї не є однорідними. Спектр експертних думок коливається від вимог щодо повної та імперативної заборони розробки АСО з посиланням на засадничі принципи міжнародного гуманітарного права (зокрема, у працях А. Герценцвайга [393]) до концепцій нормативно-етичної регламентації, які визнають прерогативу створення та розгортання систем, контрольованих людиною на всіх етапах операційного циклу. Прикладом другого підходу виступає позиція П. Шарре, який у монографії «Автономна зброя та операційний ризик» наполягає на необхідності надання пріоритету моделі синергетичної взаємодії людини та машини («людина у контурі управління» – *human-in-the-loop*) [360]. Разом з тим дослідник допускає використання інших модифікацій АСО у випадках, коли безперервне людське керування є технічно неможливим або небезпечним для оператора, «наприклад, під водою, а також під час безпосереднього спрямування зброї на військові транспортні засоби та автономні системи озброєння» [360, с. 5].

Вказана теза знаходить своє нормативне відображення на сторінках Міжнародного журналу Червоного Хреста (№ 913), де обґрунтовується концепція диференційованого або контекстного людського контролю. Доктрина МКЧХ виходить з того, що єдиного універсального стандарту залученості оператора не існує: рівень допустимої автоматизації може бути вищим у відносно ізольованих середовищах (підводний або космічний простір),

проте в умовах високої щільності цивільного населення та під час ведення бойових дій у щільній міській забудові контроль людини над критичними функціями вибору та ураження цілей має залишатися абсолютним [МКЧХ-913/1]» [408].

У Спільному заклику Генерального секретаря ООН Антоніу Гутерріша та Президентки МКЧХ Мір'яни Споляріч Еггер наголошується на пріоритетності гуманітарного вектора у сучасних безпекових реаліях. Очільники міжнародних інституцій закликають світових лідерів невідкладно розпочати предметні переговори щодо створення нового, юридично обов'язкового міжнародно-правового інструменту для встановлення чітких заборон та обмежень стосовно автономних систем зброї, визначивши кінцевим терміном завершення цього процесу 2026 рік [511].

Очевидно, що проектування АСО на основі ІІІ здатне забезпечити суттєві технологічні переваги в умовах збройного протистояння та дозволяє мінімізувати втрати особового складу, що є ключовим пріоритетом військового командування. Проте неконтрольована розробка та розгортання таких комплексів загрожують катастрофічними наслідками у разі виникнення системних операційних збоїв чи алгоритмічних помилок.

Зважаючи на це, міжнародна спільнота має консолідувати зусилля задля приведення процесів розробки та контролю за функціонуванням АСО у сувору відповідність до засадничих імперативів гуманітарного права. Обґрунтовуючи цю позицію, керівники ООН та МКЧХ у зверненні 2023 року зауважують: «Необхідні нові міжнародні правила щодо автономної зброї, які б дозволили уточнити та посилити чинне законодавство. Вони мають виступити як превентивний захід, що забезпечить захист осіб, котрі можуть постраждати від застосування такої зброї, та дозволить уникнути критичних загроз для людства» [511]. Як на базовий координаційний майданчик для розробки нормативно-етичних обмежень АСО, автори заклику посиляються на Конвенцію про заборону або обмеження застосування конкретних видів звичайної зброї, які можуть вважатися такими, що завдають надмірних ушкоджень або мають

невибірково дію 1980 року [111].

Інтеграція штучного інтелекту в архітектуру АСО, особливо в контурі ІБР, суттєво мультиплікує операційні ризики внаслідок непередбачуваності алгоритмічних моделей під час селекції цілей та прийняття тактичних рішень. У межах моделі «людини поза контуром управління» (*human-out-of-the-loop*) відсутність стійкого зв'язку з оператором після первинної активації комплексу робить систему критично вразливою до помилок розрізнення. Подібний деструктивний ефект є найбільш імовірним під час розгортання роїв безпілотних апаратів, де ШІ нездатний чітко диференціювати цивільне населення та комбатантів [393, с. 58], що прямо порушує імперативні принципи МГП [141, с. 191-193].

Для моделі «людини над контуром управління» (*human-on-the-loop*) критичні загрози зумовлені потенційними затримками або розривами каналів зв'язку. У ситуаціях, коли оператор здійснює моніторинг операцій, але зовнішні радіоелектронні перешкоди або кібератаки блокують можливість дистанційного втручання, алгоритм ШІ продовжує функціонувати в автономному режимі. Аналіз експлуатації комплексів (зокрема, мікро-БПЛА *Perdix* [345] чи тактичних систем *Iron Dome* [417]) засвідчує, що це призводить до виникнення ефекту упередження автоматизації (*automation bias*). У таких умовах оператор психологічно схильний беззастережно довіряти системним даним, ігноруючи операційні аномалії [327], що створює пряму загрозу для мирного населення та може спричинити масові жертви під час ведення бойових дій у щільній міській забудові.

У разі реалізації схеми «людини у контурі управління» (*human-in-the-loop*) безперервна взаємодія з оператором суттєво обмежує масштабованість воєнного застосування комплексів. Надмірний потік даних в інфраструктурі ІБР перевантажує когнітивні спроможності людини, зумовлюючи помилки у процесі ухвалення рішень. Своєю чергою, вимушений розрив каналу зв'язку з оператором (що є спільним уразливим чинником і для моделі *human-on-the-loop*) призводить до повної втрати боєздатності системи, перетворюючи АСО

на статичну та вразливу мішень [141, с. 187] для засобів ураження противника.

Ураховуючи зазначені чинники, навіть без відносної інтеграції ШІ в архітектуру мілітарних систем, вітчизняні дослідники, які аналізують практику застосування АСО в умовах сучасної війни в Україні, наголошують, що «розвиток і застосування АСО вимагає не лише технічного регулювання, а й перегляду юридичних категорій, уточнення меж відповідальності, адаптації судової практики до нових реалій, а також посилення ролі міжнародних судових і квазісудових інституцій у збереженні людського контролю як основи законності у сфері застосування сили». З огляду на це, особливу увагу «слід приділити формулюванню чіткої української позиції щодо меж допустимої автономії бойових систем, яка поєднувала б безпекові інтереси з міжнародно-правовими зобов'язаннями». Україна як держава, що перебуває в епіцентрі масштабного збройного конфлікту та активно впроваджує інноваційні цифрові рішення в оборонній сфері, володіє унікальним потенціалом для напрацювання практичних стандартів правомірного використання автономних засобів ведення війни [141, с. 193].

Нормативно-правове регулювання функціонування АСО з елементами Інтернету речей та штучного інтелекту потребує розробки системи імперативних обмежень та заборон. Оскільки Регламент про ШІ (*AI Act*) містить пряме виключення щодо воєнного сектору, базовим регуляторним інструментом залишаються норми МГП, які встановлюють обов'язкові рамки крізь призму принципів розрізнення, пропорційності та недопущення заподіяння надмірних страждань.

Підсумовуючи, слід зазначити, що під час формування безпекових обмежень для АСО нового покоління визначальним критерієм оцінки операційних ризиків має виступати комплексний облік як суто технічних уразливостей (кібератаки, розриви каналів зв'язку), так і раніше дослідженого психофізіологічного фактора упередження автоматизації (*automation bias*). Системна протидія цим загрозам є обов'язковою умовою для збереження правового контуру управління мілітарними технологіями та недопущення

деструктивних наслідків для цивільного населення.

Таким чином, узагальнення операційно-правових та етичних викликів дозволяє диференціювати ключові загрози застосування АСО залежно від обраної архітектури людського контролю.

У моделях «людина поза контуром управління» (*human-out-of-the-loop*) деструктивний потенціал штучного інтелекту є максимальним. Повне вилучення оператора з циклу прийняття тактичних рішень унеможливорює дотримання імперативних принципів розрізнення та пропорційності МГП, формуючи критичну «прогалину у відповідальності» (*accountability gap*). Такі системи мають високий потенціал етичних порушень через непередбачуваність ІІІ.

У схемах «людина над контуром управління» (*human-on-the-loop*) ключові ризики лежать у площині психологічної взаємодії. Ефект упередження автоматизації (*automation bias*) зумовлює пасивність оператора та його небажання втручатися в дії алгоритму. Подібна розмитість ролі людини нівелює ефективність моніторингу в динамічних бойових умовах і ускладнює юридичну фіксацію провини за помилки системи.

У концепціях «людина у контурі управління» (*human-in-the-loop*) головним джерелом уразливості стає безпосередньо людський фактор. Спроба зберегти тотальний контроль в умовах високоінтенсивного обміну даними у мережах ІБР призводить до психофізіологічного перевантаження, ментальної втоми та зниження когнітивної ефективності військовослужбовця, що неминуче провокує помилки під час селекції цілей або створює передумови для операційного саботажу.

Зважаючи на викладене, жодна з існуючих моделей не забезпечує абсолютного балансу між технологічною ефективністю та правовою безпекою, що підтверджує нагальну потребу імперативного міжнародно-правового обмеження автономізації летальної сили.

Неконтрольовані перегони озброєнь у сфері автономних систем створюють критичні ризики ескалації збройних протистоянь,

несанкціонованого поширення технологій та глобальної дестабілізації. У зв'язку з цим актуалізується потреба в імперативному вдосконаленні правових обмежень щодо АСО на базі ІІІ, які функціонують у моделі «людина поза контуром управління» (*human-out-of-the-loop*), а також у запровадженні жорстких регуляторних рамок для розробки та впровадження систем із контурами «людина над контуром управління» (*human-on-the-loop*) та «людина у контурі управління» (*human-in-the-loop*) на рівні МГП.

З огляду на зазначене, у документах ООН, Ради Європи та в межах численних експертних ініціатив послідовно висувається вимога щодо забезпечення ефективного (змістовного) людського контролю (*meaningful human control*) над ЛАСО [3.2]. У цьому контексті йдеться не про формальну присутність оператора на етапі запуску комплексу, а про реальну здатність людини розуміти принципи функціонування системи, адекватно оцінювати контекст її застосування, приймати усвідомлені рішення щодо використання вогневого ураження та нести персональну правову відповідальність. У випадках, коли такий контроль є об'єктивно неможливим унаслідок високої швидкості операційних процесів, непрозорості алгоритмів («ефекту чорної скриньки») або дефіциту тактичної інформації, постає питання про повну недопустимість експлуатації відповідного комплексу з погляду міжнародного права.

Прикметно, що проблематика автономізації не обмежується виключно кінетичними воєнними системами. Інтеграція ІІІ у сферу здійснення кібероперацій, проведення інформаційно-психологічних заходів, управління безпілотними платформами різного базування, а також у функціонування систем тотального спостереження й таргетингу формує додатковий вимір безпекових ризиків. Алгоритми здатні масштабувати й автоматизувати дії, які раніше вимагали залучення значних людських та часових ресурсів, що суттєво знижує рівень контролю над ними. У таких сценаріях автономія виявляється не лише у виборі фізичного об'єкта для знищення, а й у спроможності ІІІ самостійно виявляти системні вразливості інфраструктури, моделювати

варіанти атак та генерувати адаптивні дезінформаційні кампанії. Для сучасної юриспруденції це означає необхідність розширення зони дії обмежувальних правових режимів щодо застосування ІІІ в оборонній сфері далеко за межі класичного розуміння конвенційної зброї.

У цьому контексті визначального значення набуває офіційно зафіксований у матеріалах МКЧХ «людиноцентрований підхід» (*human-centred approach*) до мілітаризації технологій ІІІ та машинного навчання. Міжнародно-правова позиція Комітету чітко констатує, що штучний інтелект за жодних умов не може володіти суб'єктністю в межах МГП. Відтак, будь-які алгоритмічні рішення воєнного характеру мають оцінюватися виключно крізь призму спроможності людини-командира залишатися свідомим суб'єктом морально-етичного та правового вибору, що виключає можливість делегування машинам права на позбавлення життя [МКЧХ-913/2].

Сучасний український контекст надає зазначеній проблематиці особливої гостроти. Повномасштабна війна супроводжується інтенсивним застосуванням безпілотних комплексів, високоточного озброєння, засобів розвідки та цілевказання, у тому числі з інтегрованими елементами ІІІ. За таких умов держава об'єктивно зацікавлена в прискореному розвитку технологічних спроможностей, але водночас має забезпечувати збереження контролю над застосуванням сили, недопущення розмивання відповідальності та суворе дотримання міжнародних гуманітарних стандартів. Це означає, що під час планування, розробки та закупівлі оборонних систем із використанням ІІІ необхідно імперативно закладати вимоги щодо збереження ефективного людського контролю, прозорості алгоритмів (у межах, що не порушують режим військової таємниці), обов'язкового проходження процедури оцінки відповідності нормам МГП, а також запобігання впровадженню комплексів, здатних приймати повністю автономні рішення про застосування летальної сили.

З огляду на це, стратегічна правова політика України у сфері координації ІІІ та оборонного сектору має базуватися на таких засадничих положеннях:

1. Недопустимість проектування та експлуатації мілітарних систем, які повністю позбавляють людського оператора можливості реального контролю над ухваленням рішення про застосування летальної сили.
2. Обов'язковість комплексної юридичної оцінки відповідності будь-яких нових зразків озброєнь із елементами III нормам міжнародного гуманітарного права ще на етапах їхнього конструювання, моделювання та полігонних випробувань.
3. Чітка делімітація та розподіл юридичної відповідальності між профільними державними органами, підприємствами-виробниками оборонної продукції та безпосередніми операторами таких систем.
4. Послідовна та прозора позиція України у межах міжнародних переговорних процесів щодо заборони або обмеження ЛАСО, що покликано продемонструвати не лише технологічну, а й нормативно-етичну зрілість держави на світовій арені.

3.3. Правове регулювання обмеження використання штучного інтелекту в медицині

Всесвітня організація охорони здоров'я у 2021 році запропонувала перший цілісний етичний каркас для використання штучного інтелекту в галузі охорони здоров'я [530] (далі – Звіт ВООЗ 2021). У цьому документі зафіксовано, що ШІ володіє значним потенціалом для покращення якості життя мільйонів людей, проте водночас здатний завдати суттєвої шкоди у разі зловживання технологіями чи неналежного нормативного регулювання (абз. 1). Відтак, на рівні ВООЗ вихідною точкою концептуалізації виступає не технічний оптимізм, а ризик-орієнтований баланс між суспільною користю та потенційною шкодою. На сучасному етапі зазначений підхід трансформувався у юридично обов'язкові вимоги Регламенту (ЄС) 2017/745 про медичні вироби (англ. *Medical Devices Regulation* – MDR) [468], Регламенту про ШІ (AI Act) [472], стандартів Управління з продовольства і медикаментів США щодо

програмного забезпечення як медичного виробу (англ. *Software as a Medical Device*, далі – FDA-підходи до SaMD [514]), а також настанов Міжнародної ради з гармонізації технічних вимог до фармацевтичних продуктів (далі – керівництво *ICH E6(R3)*) [411].

У Звіті ВООЗ 2021 року сформульовано шість фундаментальних принципів безпечного впровадження цифрових технологій. Вони задають нормативно-етичні межі застосування медичного ШІ, орієнтовані на пріоритет автономії пацієнта, прозорість, підзвітність, інклюзивність та сталість національних систем охорони здоров'я.

Зокрема, принцип «захисту автономії людини» визначено як імператив збереження контролю з боку людського експерта над функціонуванням системи охорони здоров'я та ухваленням клінічних рішень, а також як гарантію недоторканності приватного життя. Акцент на автономії деталізується через механізми мінімізації ризиків неправомірного збирання й аналізу чутливих даних, загрози несанкціонованого доступу, кібератак, моніторингу стану здоров'я без усвідомленої згоди особи та маніпуляції психічними станами пацієнтів.

Фактично, зазначений принцип окреслює зміст сучасних юридичних вимог до інформованої згоди, конфіденційності та суворо цільового використання медичної інформації. Ці елементи знайшли відображення в положеннях Регламенту про ШІ (*AI Act*) [472] у частині управління даними та забезпечення їхньої якості для високоризикових мікросистем ШІ (ст. 6, 9–10), а також у нормах керівництва *ICH E6(R3)* [411] щодо безумовного пріоритету прав (пп. 1.1 п. 1), інформованої згоди (пп. 2.3 п. 2), безпеки та благополуччя учасників клінічних досліджень над інтересами науки чи суспільства [468].

Принцип «сприяння добробуту й безпеці людей, а також суспільним інтересам» покладає на розробників обов'язок гарантувати безпеку, точність та доведену ефективність цифрових технологій. У звіті ВООЗ наголошується на відносному та багатоаспектному характері зазначених категорій. Обґрунтовано, що суто технічна точність роботи алгоритму не є тотожною його етичності,

фізична безпека пацієнта автоматично не охоплює інформаційну безпеку (конфіденційність даних), а операційна ефективність за певних умов може бути спрямована як на лікування, так і на заподіяння шкоди індивіду чи суспільству.

З огляду на це, європейське медичне право трансформує вказану нормативно-етичну вимогу у конкретні юридичні обов'язки суб'єктів ринку. Зокрема, норми MDR передбачають проведення обов'язкової клінічної оцінки, впровадження постмаркетингового нагляду та безперервне управління ризиками протягом усього життєвого циклу медичного виробу, включно із програмним забезпеченням на основі ШІ (ст. 10, ст. 61, ст. 83–86, Правило 11 Додатка VIII MDR) [468].

Своєю чергою, принцип «забезпечення прозорості та зрозумілості» вимагає від суб'єктів проєктування оприлюднення достатнього обсягу інформації для проведення громадських консультацій та фахових експертиз. Це є передумовою для адекватної оцінки суспільством допустимості й доцільності впровадження конкретних медичних систем ШІ. Така прозорість виступає ключовим інструментом реалізації об'єктивного соціального контролю над технологіями та прогнозування наслідків їхньої експлуатації, що становить основу етичної та відповідальної взаємодії між державою, розробником і пацієнтом.

На європейському нормативному рівні зазначена етична вимога трансформувалася в імперативні обов'язки забезпечення прозорості та відстежуваності високоризикових систем ШІ. Згідно з Регламентом про ШІ (*AI Act*) [472], це передбачає обов'язкове ведення системних логів (автоматизоване логування), підготовку детальної технічної документації та забезпечення інтерпретованості й пояснюваності алгоритмічних рішень (ст. 11–13). Своєю чергою, у сфері обігу лікарських засобів та проведення клінічних випробувань цей підхід відображений у стандартах керівництва *ICH E6(R3)* [411] щодо повноти та деталізації документування протоколів, методології та верифікації результатів досліджень (Розділ II, п. 2.10–2.13; Додаток 1, розд. 2.6, 2.8, 2.10).

Принцип «підвищення відповідальності та підзвітності» декларує

необхідність чіткого визначення юридичної відповідальності всіх зацікавлених суб'єктів за неналежне або неправомірне використання технологій ШІ. У джерелах ВООЗ це положення позиціонується як засадничий орієнтир для делімітації меж, де закінчується юридична відповідальність розробника програмного забезпечення й починається деліктна або кримінальна відповідальність медичного закладу та безпосередньо лікаря-оператора. Сучасні регуляторні інструменти – MDR, Регламент про ШІ та стандарти FDA щодо програмного забезпечення як медичного виробу (SaMD) на базі штучного інтелекту й машинного навчання – вирішують цю дилему через розгортання багаторівневого ланцюга підзвітності. Цей контур охоплює виробників, постачальників, імпортерів, дистриб'юторів та кінцевих користувачів (заклади охорони здоров'я), закріплюючи як персональний (людський), так і корпоративний виміри відповідальності. Зокрема, архітектура такої підзвітності структурована в такий спосіб:

у межах MDR – через ст. 10 (регламентація обов'язків виробників щодо розгортання систем управління якістю, мінімізації ризиків, проведення клінічної оцінки та постмаркетингового нагляду), ст. 13–14 (закріплення зобов'язань уповноважених представників та імпортерів), ст. 15 (інститут відповідальної особи виробника), а також ст. 93–100 (визначення наглядових повноважень компетентних органів, алгоритмів коригувальних дій, обмеження чи повної заборони введення виробів в обіг) [468];

у межах Регламенту про ШІ (AI Act) – через ст. 16–29 (диференціація обов'язків постачальників, імпортерів, дистриб'юторів та користувачів високоризикових систем ШІ, включно з медичними комплексами), ст. 62–68 (процедури координації та завдання наглядових органів на рівні ЄС), а також ст. 71–74 (уніфікована система жорстких санкцій та адміністративних штрафів за порушення вимог безпеки) [472];

у межах FDA-підходів до технологій AI/ML-SaMD – через План дій щодо програмного забезпечення як медичного виробу на базі ШІ та машинного навчання (*AI/ML-Based Software as a Medical Device Action Plan* [511]), який

фіксує відповідальність розробника за валідацію системи управління якістю, прозорість алгоритмічних модифікацій та постринковий моніторинг реальної ефективності у розділах: «Доринковий огляд» (*Premarket review*), «Належна практика машинного навчання» (*Good Machine Learning Practice*) та «Постринкова ефективність у реальних умовах» (*Postmarket Real-World Performance*). Крім того, загальні рамки підзвітності конкретизовані у галузевих керівництвах FDA: «Політика щодо функцій програмного забезпечення пристроїв та мобільних медичних додатків» (*Policy for Device Software Functions and Mobile Medical Applications*) та вимогах до обов'язкового виконання «Попередньо узгоджених планів контролю змін» (*Predetermined Change Control Plans*), оскільки здатність ШІ до динамічної саомодифікації алгоритмів є одним із його ключових операційних критеріїв.

Принцип «забезпечення інклюзивності та справедливості» декларує імператив рівноправного доступу до медичних технологій ШІ незалежно від соціальної, расової, гендерної чи економічної приналежності пацієнтів. Фактично, зазначене положення адаптує до медичної сфери загальновизнані вимоги Загальної декларації прав людини (ст. 1, 2, 25) [81], Декларації про право на розвиток (ст. 1, ч. 1 ст. 8) [340], Декларації тисячоліття ООН (п. 6–7) [510] та Окінавської хартії глобального інформаційного суспільства (преамбула, п. 3–5) [458] в частині забезпечення універсального доступу до благ наукового прогресу. На сучасному етапі цей етичний орієнтир інтегрований у структуру глобального права на розвиток та охорону здоров'я.

У площині технічних стандартів і профільної регуляторики вказаний принцип конкретизується через жорсткі вимоги щодо недискримінаційності архітектури даних, обов'язкової оцінки впливу алгоритмів на фундаментальні права людини та захисту інтересів вразливих груп пацієнтів під час моделювання й клінічного тестування цифрових систем. Відповідні імперативи нормативно кодифіковані у положеннях Регламенту про ШІ (*AI Act*) [472], стандартів MDR [468] та керівництва *ICH E6(R3)* [411].

Зокрема, Регламент про ШІ визначає, що високоризикові системи,

включно з медичними цифровими комплексами, мають проєктуватися та навчатися виключно на основі релевантних, репрезентативних і максимально вільних від системних помилок наборів даних (*datasets*). При цьому розробник зобов'язаний враховувати специфіку груп осіб, щодо яких планується застосування системи (ч. 2–3 ст. 10). Крім того, документ покладає на суб'єктів ринку обов'язок здійснювати превентивну оцінку та мінімізацію ризиків для основоположних прав (ст. 9), а також дотримуватися спеціальних вимог щодо прозорості й інформування кінцевих користувачів (ст. 13) [472].

Своєю чергою, тексти MDR через механізми обов'язкової клінічної оцінки, збалансування співвідношення ризиків і користі та безперервний постмаркетинговий нагляд (ст. 10, 61, 83–86) [468], а також через правила класифікації програмного забезпечення як медичного виробу (Правило 11 Додатка VIII) імперативно вимагають підтвердження безпеки та ефективності цифрових продуктів для різних категорій пацієнтів, що дозволяє запобігти заподіянню системної шкоди окремим групам населення.

Цю нормативну архітектуру доповнюють стандарти *ICH E6(R3)* [411]. Вони закріплюють на рівні базових принципів безумовний пріоритет прав, безпеки та благополуччя учасників клінічних досліджень над інтересами науки чи суспільства (розд. II, п. 1–1.1). Також регламентуються обов'язки щодо належного інформування й додаткового захисту вразливих груп пацієнтів (Додаток 1, розд. 2.8) та вимоги до детального документування протоколів, методології та результатів випробувань (розд. II, пп. 2.10–2.13; Додаток 1, розд. 2.6, 2.10). Це створює надійні процесуальні гарантії справедливого ставлення до всіх суб'єктів клінічного процесу.

Фінальний принцип ВООЗ – «просування гнучкого та сталого штучного інтелекту» – апелює до необхідності безперервної та прозорої оцінки цифрових технологій безпосередньо під час їхньої експлуатації з метою перевірки відповідності жорстким стандартам медичної сфери. Зазначений принцип, який на перший погляд має декларативний характер, доцільно розглядати як концептуальну основу для регламентації рутинного використання та

проектування майбутніх генерацій медичного ШІ. На сучасному етапі на цій логіці ґрунтуються настанови FDA щодо циклічного оновлення програмного забезпечення як медичного виробу (*AI/ML-SaMD*) [514], закріплені у розділах «Належна практика машинного навчання для медичних виробів на базі ШІ» (*Good Machine Learning Practice for AI/ML-Based Medical Devices*), «Доринковий огляд медичного софту на базі ШІ» (*Premarket Review of AI/ML-Based SaMD*) та «Постринкова ефективність у реальних умовах» (*Postmarket Real-World Performance*). Аналогічний підхід відображений у вимогах *ICH E6(R3)* [411] у частині управління операційними ризиками, моніторингу безпеки пацієнтів та впровадження адаптивного дизайну клінічних досліджень (розд. II, п. 2–2.3; Додаток 1, розд. 3.3–3.5, 3.13).

Проведений аналіз засвідчує, що шість фундаментальних принципів поведінки з ШІ в медицині, задекларованих у Звіті ВООЗ 2021 року, формують нормативно-етичну архітектуру взаємодії людини з цифровими технологіями. Цей базис, орієнтований на прозорість, підзвітність, інклюзивність та автономію, протягом наступних років поступово інтегрувався у жорсткі регуляторні контури MDR, Регламенту про ШІ (*AI Act*), стандартів FDA та керівництва *ICH E6(R3)*. Відтак, зазначені принципи доцільно розглядати як вихідну точку для конструювання правових режимів допустимого та високоризикового застосування ШІ в охороні здоров'я.

Важливе значення для формування сучасної концепції адміністративно-правового регулювання використання штучного інтелекту має доповідь Ради Європи «The Impact of Artificial Intelligence on the Doctor-Patient Relationship» (2022) [442]. Автори наголошують, що використання систем штучного інтелекту не змінює природи правовідносин, однак істотно трансформує механізм прийняття рішень, структуру взаємодії між суб'єктами та розподіл відповідальності.

Особливу увагу приділено ризикам використання ШІ, серед яких виокремлено алгоритмічну упередженість, недостатню прозорість, порушення приватності, послаблення ролі людини у прийнятті рішень, невизначеність

відповідальності та нерівність доступу. При цьому підкреслюється, що зазначені ризики зумовлені не лише технічними характеристиками алгоритмів, а й зміною механізму прийняття рішень та характеру правовідносин.

Доповідь обґрунтовує, що зі зростанням автономності систем штучного інтелекту повинні посилюватися вимоги до *meaningful human oversight*, алгоритмічної прозорості та пояснюваності рішень. Водночас прозорість розглядається не лише як технічна характеристика, а як юридична вимога, що охоплює відомості про джерела даних, порядок розроблення, тестування та можливість перевірки функціонування системи.

Окремо автори звертають увагу на явища алгоритмічної дискримінації та *automation bias*, що можуть призводити до безкритичного сприйняття алгоритмічних рішень і поступового зниження ролі людини у процесі їх прийняття. У зв'язку з цим обґрунтовується необхідність запровадження комплексного алгоритмічного аудиту та чіткого розподілу відповідальності між усіма суб'єктами життєвого циклу системи штучного інтелекту.

Таким чином, доповідь Ради Європи формує універсальну правозахисну модель використання штучного інтелекту, відповідно до якої об'єктом правового регулювання повинні бути не лише технічні характеристики систем, а й їх вплив на права людини, механізми прийняття рішень, людський контроль і систему юридичної відповідальності [442].

Сучасні базові моделі взаємодії людини з автономними системами – «людина в контурі управління» (*human-in-the-loop*), «людина над контуром управління» (*human-on-the-loop*) та «людина поза контуром управління» (*human-out-of-the-loop*) – історично сформувалися у мілітарній сфері як відповідь на операційні ризики зброї з автономними компонентами. Проте вказані режими мають не менше значення для теоретико-правового аналізу медичного ШІ. У медичній галузі ці моделі перестають бути суто технічними режимами керування. Трансформуючись у юридичні критерії допустимості або небезпечності використання ШІ, вони визначають архітектуру взаємин у тріаді «розробник – лікар – пацієнт» – від повної автономії програмного алгоритму до

безперервної присутності лікаря в контурі прийняття клінічних рішень. На цих засадах сьогодні ґрунтуються ключові нормативні вимоги, визначені на рівні MDR [468], Регламенту про ШІ (*AI Act*) [472], керівництва *ICH E6(R3)* [411] та національних стандартів (зокрема, FDA-підходів до *AI/ML-SaMD* [514]) для високоризикових медичних систем штучного інтелекту.

У межах моделі «людини поза контуром управління» (*human-out-of-the-loop*) система після первинної активації самостійно обирає та реалізує операційні дії без будь-якого подальшого втручання оператора. Якщо в мілітарній площині це означає автономне визначення об'єктів ураження, то в медицині зазначена логіка передбачає повністю автоматизовану діагностику або хірургічне втручання без реального контролю з боку лікаря. Відповідно, такий сценарій є найбільш критичним і ризикованим із погляду принципів автономії пацієнта, безпеки та підзвітності. Правове регулювання цієї моделі має акцентуватися на безумовній передбачуваності алгоритмів, покладанні повної деліктної відповідальності на людину-оператора за параметри запуску системи, а також на відповідальності розробника за прозорість архітектури рішень. Вказані імперативи нормативно регламентуються такими механізмами:

настановами MDR у частині безперервного управління ризиками та забезпечення безпеки пацієнтів з урахуванням сучасного рівня розвитку техніки (зокрема, ст. 10 щодо впровадження систем управління якістю та ризиками, ст. 61 про обов'язковість клінічної оцінки, а також ст. 83–86, які регулюють процеси постмаркетингового нагляду та післяринкової клінічної оцінки) [468];

положеннями Регламенту про ШІ (*AI Act*) щодо архітектури систем управління ризиками (ст. 9), суворих вимог до управління даними (*data governance*) (ст. 10), ведення детальної технічної документації (ст. 11), автоматизованого логування (ст. 12), а також забезпечення прозорості й інформування кінцевих користувачів високоризикових систем штучного інтелекту (ст. 13) [472];

стандартами FDA США щодо технологій *AI/ML-SaMD*, які закріплюють обов'язок виробника впроваджувати концепцію повного

життєвого циклу продукту, здійснювати безперервний постмаркетинговий моніторинг реальної ефективності та превентивно фіксувати межі застосування софту, сценарії його оновлень і механізми контролю модифікацій через «Попередньо визначені плани контролю змін» (*Predetermined Change Control Plans*). Даний підхід деталізовано у керівництвах: «Належна практика машинного навчання для медичних виробів на базі ШІ» (*Good Machine Learning Practice for AI/ML-Based Medical Devices*), «Доринковий огляд медичного софту на базі ШІ» (*Premarket Review of AI/ML-Based SaMD*) та «Постринкова ефективність у реальних умовах» (*Postmarket Real-World Performance*).

Модель людини над контуром управління (*human-on-the-loop*) описує режим безперервного спостереження, координації та надання оператору можливості своєчасного зупинення чи скасування дій системи ШІ. За такої архітектури суб'єкт не просто задає первинні параметри місії, а здійснює постійний моніторинг та інтервенцію в алгоритм, що повністю відповідає міжнародно-правовій концепції «змістовного людського нагляду» (*meaningful human oversight*).

Зазначений підхід нормативно кодифікований у положеннях Регламенту про ШІ (*AI Act*) [472], зокрема у статті 14, яка безпосередньо регламентує параметри людського нагляду за високоризиковими системами штучного інтелекту у поєднанні із загальними вимогами до архітектури управління ризиками та забезпечення якості даних (ст. 9–10). На аналогічних засадах ґрунтуються імперативи керівництва *ICH E6(R3)* [411] (розд. II, п. 1–1.1; Додаток 1, розділи «Медична допомога учасникам випробувань» (*Medical Care of Trial Participants*) та «Оцінка та звітність щодо безпеки» (*Safety Assessment and Reporting*)), які фіксують обов'язок безперервного моніторингу безпеки пацієнтів та право невідкладного коригування або повного припинення клінічного дослідження у разі виявлення критичних ризиків.

У межах цього правового режиму регуляторні механізми мають деталізувати не лише технічні вимоги до програмних алгоритмів, а й процедурний порядок організації безпосереднього людського нагляду. Зокрема,

нормативному визначенню підлягає коло суб'єктів, які здійснюють моніторинг, регламент та періодичність контрольних операцій, обсяг імперативних повноважень оператора для екстреної зупинки цифрової системи, а також юридичні наслідки й міра деліктної відповідальності у разі неналежного виконання вказаних обов'язків

Найбільш відповідною етичним орієнтирам ВООЗ та класичній доктрині медичного права є модель «людини у контурі управління» (*human-in-the-loop*). У межах цієї архітектури людина незмінно перебуває в центрі ухвалення рішень, тоді як система ШІ виконує виключно допоміжну функцію, акумулюючи дані, генеруючи прогнози чи пропонуючи рекомендаційні сценарії дій, проте в жодному разі не замінюючи індивідуальний клінічний розсуд фахівця. Зазначений режим виступає базовим для процесів сучасної діагностики й терапії, коли лікар використовує результати комп'ютерного аналізу медичних зображень, обробки великих масивів даних (*Big Data*) або прогностичного моделювання, однак остаточний діагноз і стратегію лікування затверджує самостійно, враховуючи персональні особливості конкретного пацієнта.

У нормативно-правовому аспекті цей підхід повністю узгоджується з вимогами MDR та Регламенту про ШІ (*AI Act*) щодо високоризикових медичних систем. Вказані акти імперативно регламентують необхідність постійного людського нагляду, обов'язкове забезпечення можливості верифікації та перегляду людиною результатів роботи алгоритму, а також обов'язок гарантувати інтерпретованість, пояснюваність та автоматизоване логування рішень цифрової системи. Аналогічно, ця модель кореспондує фундаментальним принципам керівництва *ICH E6(R3)* [411] щодо безумовного пріоритету прав і благополуччя пацієнта над будь-якими інтересами наукового прогресу, навіть якщо математичний алгоритм прогнозує вищу потенційну ефективність експериментального методу.

Проте інші моделі залученості людини також знаходять своє обмежене застосування в охороні здоров'я. Зокрема, у діагностичній практиці значна

частина асистуючих функцій (первинний скринінг зображень, опитувальники чат-ботів, агрегація лабораторних показників) може функціонувати у режимі «людини поза контуром управління» (*human-out-of-the-loop*), за умови, що фінальний клінічний висновок залишається виключною прерогативою лікаря. За такого підходу цифрова екосистема регулюється як високоризиковий інструмент із обов'язковим людським контролем підсумкового результату, а не як автономний суб'єкт діагностичного процесу.

Водночас розробка та коригування персоналізованих планів лікування, де критично важливо враховувати непередбачуваність перебігу патологій, коморбідні стани пацієнта та динамічну зміну клінічної картини в реальному часі, вимагає беззастережної реалізації моделі «людини у контурі управління» (*human-in-the-loop*). Норми MDR, Регламенту про ШІ та стандартів ICH E6(R3) солідарно не допускають у цій площині ухвалення повністю автономних рішень з боку ШІ, оскільки такий алгоритмічний автоматизм становить пряму загрозу для життя людини та означає суттєве неправомірне втручання у фундаментальні права пацієнта.

У сфері розробки лікарських засобів та проведення клінічних випробувань штучний інтелект спроможний виконувати широкий спектр аналітичних функцій: від дослідження великих масивів даних (*Big Data*) медичних карт, стратифікації пацієнтів і пошуку перспективних біомаркерів до перепрофілювання існуючих препаратів та прогнозування потенційних побічних ефектів. Для суто дослідницьких (доклінічних) завдань допустимим є ширше застосування моделі «людини поза контуром управління» (*human-out-of-the-loop*) за умови суворого нагляду компетентних органів за якістю вхідних даних та валідацією методів. Натомість будь-яке безпосереднє втручання у процес лікування реальних пацієнтів, моніторинг стану здоров'я експериментальних груп, а також ухвалення рішень про продовження або припинення терапії вимагають обов'язкової реалізації режимів «людини у контурі управління» (*human-in-the-loop*) або принаймні «людини над контуром управління» (*human-on-the-loop*). Зазначені імперативи чітко закріплені у

стандартах належної клінічної практики (розд. II, п. 1–1.1; Додаток 1, розд. 2.7.1, 3.13 *ICH E6(R3)*) [411], а також у вимогах Регламенту про ШІ (*AI Act*) [472] щодо обов'язкової оцінки впливу алгоритмів на фундаментальні права людини та забезпечення належного людського нагляду за високоризиковими цифровими системами.

Таким чином, моделі *human-in-the-loop*, *human-on-the-loop* та *human-out-of-the-loop* трансформуються зі зручної наукової типології на ефективний правовий механізм для адаптації загальних етичних принципів БООЗ у площину конкретних юридичних обов'язків, зафіксованих у нормах MDR, стандартах FDA, керівництвах *ICH E6(R3)*, Регламенті про ШІ та національних законодавствах у сфері охорони здоров'я. Вони дозволяють констатувати, що ключова проблема правового регулювання медичного ШІ полягає не у факті використання математичних алгоритмів як таких, а в тому, наскільки глибоко вони інтегруються у контур прийняття клінічних рішень і чи зберігається за людиною (лікарем) статус остаточного та беззастережного суб'єкта юридичної відповідальності.

У зв'язку з цим доцільно поетапно проаналізувати межі допустимості застосування зазначених моделей у процесах діагностики, терапії, а також у фармакології та клінічних дослідженнях.

Діагностика пацієнта за своєю правовою суттю є «розпізнаванням захворювання, встановленням діагнозу, що є медичним висновком про певну хворобу (травму) або причину смерті та про епідеміологічні ситуації» [70]. У своїх працях М. Мірбабаї, С. Стегліц та Н. Р. Дж. Фрік розгортають цей процес як контур послідовних етапів: від виникнення проблеми зі здоров'ям і звернення до системи охорони здоров'я, збору інформації (анамнез, інтерв'ю, об'єктивний огляд, лабораторні та інструментальні тести, консультації) до інтеграції й інтерпретації даних, формулювання робочого діагнозу, планування терапевтичних заходів та ретроспективного аналізу клінічних помилок з метою оптимізації подальших рішень [441]. За такого комплексного підходу діагностика постає не одноразовим актом, а безперервним циклічним процесом,

де кожна ітерація вимагає верифікації та потенційної корекції попередніх висновків. З огляду на це інтеграція технологій ІІІ не просто доповнює наявну медичну практику, а докорінно змінює її структуру, перерозподіляючи між лікарем та програмним алгоритмом функції збору, обробки й аналітики чутливої інформації.

Впровадження технологій штучного інтелекту в діагностичний процес здатне істотно оптимізувати діяльність медичного персоналу в багатофункціональному та динамічному клінічному середовищі. Інтеграція ІІІ забезпечує ефективну інформаційну підтримку молодих спеціалістів, оперативне відстеження стрімкої зміни соматичних показників пацієнта та акумуляцію даних про нетипові варіанти патогенезу. Технологічні рішення на основі ІІІ спроможні забезпечити високошвидкісну обробку великих масивів інформації (*Big Data*), включаючи автоматизований аналіз медичної документації, скринінг радіологічних зображень, а також первинну обробку діагностичних опитувальників цифрових чат-ботів.

У межах моделі «людини поза контуром управління» (*human-out-of-the-loop*) програмні модулі ІІІ можуть автономно аналізувати результати променевої діагностики (комп'ютерної та магнітно-резонансної томографії, рентгенографії), лабораторні показники та записи в електронних медичних картах, здійснюючи попередній тріаж (розподіл) пацієнтів за ступенем невідкладності стану. Натомість ключові етапи діагностичного процесу – встановлення остаточного клінічного діагнозу, ухвалення рішень у нестандартних ситуаціях та деонтологічна комунікація з пацієнтом – за своєю правовою та етичною природою вимагають реалізації схеми «людини у контурі управління» (*human-in-the-loop*). За такої архітектури індивідуальний розсуд лікаря не замінюється математичним алгоритмом, а верифікується та підкріплюється ним.

На подібній делімітації функцій між людиною та технологіями наполягають сучасні міжнародні регуляторні механізми. Зокрема, норми MDR кваліфікують значну частину діагностичного програмного забезпечення як

самостійні медичні вироби, зобов'язуючи постачальників гарантувати проведення клінічної оцінки, безперервне управління ризиками протягом усього життєвого циклу продукту, а також належний післяринковий нагляд (ст. 10, 61, 83–86). Своєю чергою, у Плані дій FDA щодо програмного забезпечення як медичного виробу на базі штучного інтелекту та машинного навчання (*AI/ML-Based SaMD Action Plan*) [514] закріплено концепцію повного життєвого циклу діагностичних систем. Цей підхід передбачає постійне циклічне оновлення алгоритмів на основі принципів належної практики машинного навчання (*Good Machine Learning Practice*), обов'язкове впровадження «Попередньо визначених планів контролю змін» (*Predetermined Change Control Plans*), надання доказів клінічної користі, а також збереження центральної ролі лікаря-клініциста, який має чітко усвідомлювати верифікаційні межі застосування прогностичних моделей у реальних умовах.

Регламент про ШІ (*AI Act*) трансформує зазначений підхід у чітку нормативну рамку, класифікуючи більшість медичних цифрових систем як високоризикові. Це автоматично зумовлює імперативні вимоги щодо якості й репрезентативності даних, ведення технічної документації, автоматизованого логування, забезпечення прозорості та реалізації «значущого людського нагляду» (*meaningful human oversight*) [3.2]. Відповідно, навіть якщо конкретний програмний модуль функціонує в режимі «людини поза контуром управління» (*human-out-of-the-loop*) (наприклад, під час автоматичного розпізнавання клінічних образів), архітектура ШІ має бути спроектована так, щоб лікар міг чітко усвідомлювати межі компетентності алгоритму, оцінювати достовірність згенерованих рекомендацій, верифікувати первинні дані та за потреби відхилити підсумковий висновок системи.

Таким чином, автономна робота окремого модуля ШІ в режимі «людини поза контуром управління» (*human-out-of-the-loop*) не суперечить загальному правилу застосування моделі «людини у контурі управління» (*human-in-the-loop*) щодо взаємодії з цифровою системою в цілому. Подібна синергія має виступати базовим стандартом для ухвалення клінічних рішень під час

діагностики, що повністю відповідає концептуальному змісту європейського законодавства.

Свою чергою, стандарти належної клінічної практики *ICH E6(R3)* доповнюють цей методологічний підхід ще одним суттєвим виміром – безумовним пріоритетом прав, безпеки та благополуччя пацієнтів над інтересами технологічного прогресу чи суспільства, навіть якщо математичні моделі прогнозують підвищення операційної ефективності (п. 1.1). Для діагностичних систем на основі ШІ це означає, що: їх експлуатація має спиратися на належну превентивну валідацію та верифіковані клінічні докази; пацієнти мають бути належним чином поінформовані про залучення інтелектуальних систем у процесі їхнього обстеження; результати, згенеровані алгоритмом, за жодних умов не можуть розглядатися як абсолютна істина, якщо вони суперечать об'єктивній клінічній картині чи життєвим інтересам людини.

Під час діагностичного процесу вагоме значення має також збір соціологічної інформації, зокрема проведення популяційних опитувань та епідеміологічного моніторингу. Ці процедури можуть здійснюватися за допомогою інтелектуальних чат-ботів та аналізу великих масивів даних (*Big Data*). У таких умовах системи ШІ спроможні функціонувати майже повністю в режимі «людини поза контуром управління» (*human-out-of-the-loop*), оскільки процеси агрегації даних, виявлення груп ризику, фіксації нетипової симптоматики та сигналізування про загрози епідемії можуть реалізовуватися автономно, без прямої участі людського оператора. Проте і за цього сценарію правове регулювання залишається імперативним. Регуляторні вимоги щодо захисту персональних даних (відповідно до стандартів *GDPR*), забезпечення інформованої згоди пацієнтів та недопущення алгоритмічної дискримінації діють у медичній сфері незалежно від того, чи застосовується ШІ для індивідуального клінічного аналізу чи для загального популяційного моніторингу.

Нормативно-етичні принципи, зафіксовані у Звіті BOOЗ [530] (автономія,

прозорість, інклюзивність, сталий III), та загальна регуляторна рамка Регламенту про III (*AI Act*) комплексно взаємодіють із секторальним медичним правом, створюючи цілісну систему стримувань і противаг. Ця архітектура дозволяє поєднувати застосування моделей «людини поза контуром управління» (*human-out-of-the-loop*) для автоматизованого аналізу даних, скринінгу зображень та тріажу (ранжування) пацієнтів із обов'язковим збереженням моделі «людини у контурі управління» (*human-in-the-loop*) на етапі встановлення остаточного діагнозу. Зазначена синергетична позиція повністю узгоджується з вимогами MDR, стандартами FDA, керівництвом *ICH E6(R3)* і Регламентом про III (*AI Act*), а відтак може слугувати концептуальною основою для розробки національної стратегії регулювання медичного III в Україні.

Окремим перспективним напрямом є делегування системам III функцій з моделювання складних, комплексних персоналізованих планів терапії. На основі фундаментальних галузевих знань, ретроспективного аналізу медичних кейсів, обробки інформації *Big Data*, результатів актуальних клінічних досліджень та затверджених протоколів лікування III здатний формувати багатоваріантні рекомендації, корелюючи їх із поточними результатами діагностики та предиктивними прогнозами перебігу захворювання.

Технологічні рішення на основі III виступають ефективними інструментами для виявлення індивідуальних соматичних особливостей пацієнта, пропонуючи оптимальні схеми терапевтичного впливу, а також забезпечуючи безперервний моніторинг і прогнозування результатів лікування, процесів відновлення та реабілітації [416]. Саме в клінічній практиці найвиразніше виявляється потенціал штучного інтелекту щодо ідентифікації прихованих системних закономірностей та аномалій, які можуть бути пропущені людиною [399]. Водночас у цій площині виникає найбільше застережень стосовно допустимого рівня автономії програмного алгоритму.

Процес планування та моделювання схем лікування не може бути зведений до механічної алгоритмізації. Під час розробки терапевтичної

стратегії обов'язково мають враховуватися непередбачуваність перебігу патології, поточний статус пацієнта та динамічній зміні клінічної картини в реальному часі. Зазначені фактори є спонтанними та не можуть бути повною мірою спрогнозовані й закладені в математичну модель ШІ на етапах її проектування чи машинного навчання. З огляду на це, делегування системі, що функціонує в режимі «людини поза контуром управління» (*human-out-of-the-loop*), повного циклу призначення лікування означало б фактично передати алгоритму право на істотне втручання у фундаментальні права пацієнта без надання процесуальних гарантій оперативного людського коригування.

Відтак, застосування ШІ під час стратегічного планування лікування є допустимим виключно в межах моделі «людини у контурі управління» (*human-in-the-loop*). За такої архітектури цифрова система акумулює й аналізує масиви даних, моделює варіанти розвитку подій та пропонує клінічні опції, проте остаточне рішення ухвалює виключно лікар. Саме людський експерт спроможний комплексно оцінити пропозиції алгоритму з урахуванням індивідуального деонтологічного та соматичного контексту пацієнта, беручи на себе персональну правову відповідальність за подальшу тактику лікування.

Європейське та міжнародне правове регулювання застосування штучного інтелекту в медицині повністю підтверджує зазначену концептуальну тезу. Зокрема, архітектура діючих регуляторних механізмів структурована таким чином:

у межах регламентних норм MDR визначається, що програмне забезпечення, яке використовується для ухвалення чи підтримки клінічних рішень щодо лікування, має проходити обов'язкову клінічну оцінку, а його безпека та ефективність – підтверджуватися верифікованими доказами. При цьому виробник не має права позиціонувати цифровий продукт як заміну індивідуального клінічного розсуду лікаря, а зобов'язаний чітко зафіксувати його операційні обмеження та специфічні умови експлуатації (ст. 2, 5, 10, пп. 17.1, 23.1, 23.4 Додатка I) [468];

у межах положень Регламенту про ШІ (AI Act) системи підтримки

прийняття клінічних рішень (СППКР) класифікуються як високоризикові. Це покладає на суб'єктів ринку додаткові зобов'язання щодо забезпечення якості даних, прозорості, інтерпретованості алгоритмів, автоматизованого протоколювання та наявності «значущого людського нагляду» (*meaningful human oversight*). Технологія ІІІ може пропонувати варіанти терапевтичного впливу, проте вона має бути інтегрована в клінічний процес виключно так, щоб фахівець міг повноцінно досягнути, етично оцінити та за потреби відхилити будь-яку рекомендацію системи (ст. 6, 9–15) [472];

у межах стандартів належної клінічної практики *ICH E6(R3)* закріплено вимогу, згідно з якою права, безпека та благополуччя пацієнтів мають безумовний пріоритет над інтересами технологічного прогресу, науки чи суспільства. Цей імператив залишається непорушним навіть у випадках, коли алгоритмічний інструмент демонструє статистично вищу ефективність порівняно з конвенційними методами (Принцип 1.1) [411].

У контексті моделювання персоналізованої терапії вказані нормативні вимоги означають, що:

- програмний алгоритм не спроможний автоматично змінювати схему лікування без верифікації та затвердження з боку лікаря;
- будь-які прогностичні моделі мають впроваджуватися виключно як допоміжні, а не директивні інструменти клінічного процесу;
- пацієнт повинен бути належним чином поінформований про залучення технологій ІІІ до планування терапії, а його інформована згода має бути адаптована до умов цифрової трансформації медицини.

Таким чином, логіка міжнародних нормативних документів підтверджує, що застосування штучного інтелекту під час планування лікування є допустимим виключно в межах моделі «людини у контурі управління» (*human-in-the-loop*) [40, с. 28-29]. За такої архітектури обов'язковим є чітке юридичне закріплення деліктної відповідальності лікаря та розробника за наслідки практичної реалізації алгоритмічних рекомендацій. Відтак, персоналізоване лікування за участю ІІІ не означає делегування медичних функцій машині;

воно виступає інструментальним розширенням можливостей лікаря за повного збереження його статусу як головного носія професійних знань, а також суб'єкта правової та етичної відповідальності.

Своєю чергою, розробка лікарських засобів (фармакологія) є однією з тих сфер, де технології ШІ здатні суттєво оптимізувати темпи та структуру наукового прогресу. ШІ спроможний значно прискорити відкриття нових молекул та сполук шляхом аналізу великих масивів даних (*Big Data*) медичних кейсів, електронних амбулаторних карт пацієнтів та інформації про особливості перебігу захворювань під впливом різних фармакологічних агентів. Це дозволяє оперативно виявляти як найбільш ефективні комбінації, так і речовини, що викликають неприпустимі побічні реакції. Крім того, ШІ може координувати роботу інтелектуальних чат-ботів, орієнтованих на цільові групи пацієнтів, що полегшує формування репрезентативних фокус-груп, спрощує збір інформації про дефіцит конкретних медикаментів та фіксує реальні довгострокові ефекти терапії. Подібна аналітична діяльність може здійснюватися переважно в режимі «людини поза контуром управління» (*human-out-of-the-loop*), оскільки вона формує валідний науковий фундамент для синтезу нових та випереджального перепрофілювання вже відомих лікарських препаратів.

Крім того, технології ШІ можуть залучатися до процесів супроводження пацієнтів, які беруть участь у клінічних випробуваннях, а також до статистичного аналізу результатів досліджень. Інтелектуальні системи спроможні здійснювати безперервний моніторинг життєвих показників, оперативно фіксувати побічні ефекти, виявляти кореляції та ідентичні соматичні реакції на фармакологічний вплив, а також забезпечувати точну стратифікацію пацієнтів [520]. За такого підходу ШІ виступає високоефективним інструментом, що дозволяє не лише оптимізувати архітектуру клінічних випробувань шляхом автоматизації рутинних операційних процесів і мінімізації витрат, а й відкривати нові терапевтичні можливості через глибинний аналіз даних.

Проте на межі між теоретичною аналітикою та безпосереднім втручанням

у процес лікування людини неминує постає застереження щодо допустимого рівня автономії ІІІ. Правове регулювання фармакологічного застосування інтелектуальних систем має базуватися на принципі диференціації, передбачаючи гнучке розгортання моделей «людини поза контуром управління» (*human-out-of-the-loop*), «людини у контурі управління» (*human-in-the-loop*) або «людини над контуром управління» (*human-on-the-loop*) залежно від характеру завдань:

- модель «людини поза контуром управління» (*human-out-of-the-loop*) є допустимою для систем, які виконують виключно функції наукової розвідки та доклінічного моделювання (скринінг великих масивів даних (*Big Data*), математичний обрахунок терапевтичної ефективності сполук, перепрофілювання відомих препаратів, узагальнення результатів популяційних опитувань). Експлуатація ІІІ в такому автономному режимі можлива за умови суворого регуляторного контролю за методологією розробки та якістю вхідних даних;

- моделі «людини у контурі управління» або «людини над контуром управління» (*human-in-the-loop* або *human-on-the-loop*) є безальтернативними на етапах безпосереднього дослідження, динамічного спостереження та інтерактивного опитування експериментальних груп пацієнтів. Оскільки цей контур безпосередньо пов'язаний із факторами підвищеного ризику та непередбачуваності для здоров'я людини, ухвалення будь-яких рішень щодо коригування дозування, фіксації ускладнень чи припинення тестування має залишатися під безперервним та дієвим людським контролем.

Стандарти *ICH E6(R3)* [411] прямо визначають, що права, безпека й благополуччя учасників клінічних досліджень мають безумовний пріоритет над інтересами науки та суспільства; усі процедури мають базуватися на надійних наукових доказах, операційні ризики повинні бути мінімізовані, а прогнозована користь – обґрунтованою (Принцип 1.1, Принцип 2, пп. 2.1–2.3). Це означає, що алгоритми, які впливають на стратифікацію пацієнтів, призначення схем терапії або ухвалення рішень про продовження чи припинення випробувань, не можуть

функціонувати без людського нагляду. Будь-які припущення цифрової системи мають бути валідовані людиною на рівні загальних принципів та вимог щодо належного управління ризиками й забезпечення надійності результатів, а застосування ШІ має бути прозоро описане у протоколах досліджень і доведене до відома учасників (Розділ 2).

Своєю чергою, Регламент про ШІ (*AI Act*) класифікує системи штучного інтелекту, що застосовуються в управлінні клінічними процесами та підтримці життєво важливих рішень у сфері охорони здоров'я, як високоризикові (ст. 6, Додаток III). До таких комплексів застосовуються суворі вимоги щодо якості даних, ведення технічної документації, автоматизованого протоколювання, превентивної оцінки впливу на фундаментальні права людини та забезпечення «значущого людського нагляду» (ст. 9–15, 27) [472].

Отже, у міжнародно-правовому просторі закріплена диференційована модель взаємодії з ШІ у сфері фармакології та клінічних випробувань. За такої моделі рутинна прагматична розвідка та збір даних можуть бути доручені «моделі людини поза контуром управління» (*human-out-of-the-loop*), проте всі клінічні рішення щодо аналізу результатів такої розвідки та безпосереднє ухвалення стратегічних рішень мають здійснюватися виключно в межах режимів «людини у контурі управління» (*human-in-the-loop*) або «людини над контуром управління» (*human-on-the-loop*).

Таким чином, комплексний аналіз нормативно-правового регулювання у сферах діагностики, терапії та фармакології дозволяє констатувати формування консолідованої міжнародної моделі застосування ШІ в медицині. Відповідно до вимог Регламенту про ШІ (*AI Act*), стандартів MDR та настанов належної клінічної практики *ICH E6(R3)*, межі допустимості технологій чітко диференціюються залежно від операційного контексту: якщо процеси збору первинних даних, популяційного моніторингу та доклінічної наукової розвідки можуть делегуватися автоматизованим модулям у режимі «людини поза контуром управління» (*human-out-of-the-loop*), то будь-яке безпосереднє ухвалення клінічних рішень та верифікація результатів досліджень мають

здійснюватися виключно в межах режимів «людини у контурі управління» (*human-in-the-loop*) або «людини над контуром управління» (*human-on-the-loop*). Подібний підхід забезпечує непорушність засадничого принципу медичного права щодо безумовного пріоритету безпеки й благополуччя пацієнта та зберігає за лікарем статус остаточного суб'єкта правової та етичної відповідальності.

Самостійного аналітичного вивчення потребує площина точної (персоналізованої) медицини, де визначального значення набуває здатність ШІ досліджувати генетичні й молекулярні масиви даних, фіксувати конкретні молекулярні мішені для патологій та ідентифікувати релевантні групи пацієнтів, які отримають максимальний терапевтичний ефект від специфічних методів лікування. У зазначеному сегменті алгоритми спроможні функціонувати як у режимі «людини поза контуром управління» (*human-out-of-the-loop*) на етапах фундаментальної аналітики, пошуку таргетів і моделювання патогенетичних механізмів, так і в режимі «людини у контурі управління» (*human-in-the-loop*), коли детерміновані результати інтегруються у безпосередні клінічні рішення щодо конкретного пацієнта.

Проте норми керівництва *ICH E6(R3)* та Регламенту про ШІ (*AI Act*) імперативно вимагають, щоб будь-яка екстраполяція результатів алгоритмічного аналізу з рівня теоретичної гіпотези на рівень практичної клінічної дії супроводжувалася комплексною оцінкою операційних ризиків, прозорістю впровадженої методології та збереженням остаточного консолідованого рішення за лікарем-дослідником (Принципи 1.1, 2, 7, Додаток 1 *ICH E6(R3)* [411]; ст. 9, 13, 14 *AI Act* [472]). Відтак, міжнародно-правові стандарти допускають високий рівень автономії ШІ на етапі виявлення та систематизації наукових знань, проте повністю виключають його суб'єктність під час ухвалення рішень, які безпосередньо зачіпають життя, соматичне благополуччя та фундаментальні права людини. У цьому полягає ключовий критерій диференціації меж допустимості ШІ у сфері розробки лікарських засобів та проведення клінічних випробувань.

Важливим етико-правовим аспектом впровадження штучного інтелекту в охорону здоров'я виступає інститут інформованої згоди пацієнта на отримання медичної допомоги із залученням інтелектуальних систем. Зазначена правова категорія є критично чутливою зоною, оскільки від її належної нормативної регламентації безпосередньо залежить рівень суспільної довіри до інтеграції ІІІ в клінічну практику та загальна соціальна рецепція феномену цифровізації медицини.

У розвинених юрисдикціях спеціалізованого законодавства щодо регулювання згоди на застосування ІІІ на сучасному етапі не існує, проте активно формується інститут розширеної інформованої згоди, у межах якого роль інтелектуальних систем підлягає обов'язковому окремому розкриттю [497; 422]. Формування механізму інформованої згоди на застосування ІІІ у сучасних правових системах, на нашу думку, ґрунтується на трьох основних вимірах: прозорому та інтерпретованому поясненні ролі ІІІ у клінічному процесі; акцентуванні уваги на експериментальному чи інноваційному характері впроваджених технологій; детальному інформуванні пацієнта про специфічні операційні ризики та наявні альтернативи [424; 517].

Здійснений аналіз нормативної бази показує, що у сфері діагностики та терапії в країнах ЄС та США нормативно закріплюється обов'язок повідомляти пацієнта про те, що його клінічний діагноз або терапевтичні рекомендації формуються за участю алгоритмічних систем ІІІ. Одночасно обов'язковому розкриттю підлягає статус таких систем: чи є вони складовою усталеного стандарту медичної допомоги, чи перебувають на стадії клінічних випробувань або експериментальної апробації [352; 422].

Практика етико-правового дискурсу в Німеччині, Великій Британії та США засвідчує, що під час використання лікарем інноваційних технологій (роботизованої хірургії, експериментальних методик чи медичного ІІІ) інформована згода має містити окреме застереження щодо технологічних невизначеностей, латентних ризиків, притаманних конкретному алгоритму

[517], а також інформацію про наявні традиційні (неалгоритмічні) методи лікування [424].

Відтак, інформована згода в контексті медичного ШІ трансформується з формально-бюрократичної процедури на один із центральних правових інструментів легітимації алгоритмічних рішень у сфері охорони здоров'я. Вона покликана забезпечити транспарентність функціонування систем ШІ, зафіксувати ступінь експериментальності відповідної технології та співвіднести потенційні ризики з наявними альтернативними сценаріями терапії. У такий спосіб розширена інформована згода виступає ключовим правовим механізмом збереження автономії пацієнта та підтримання рівня суспільної довіри до системи охорони здоров'я, тоді як інтелектуальні системи розглядаються виключно як допоміжні інструменти, що не підмінюють індивідуальний клінічний розсуд лікаря.

Проведене дослідження теоретико-правових засад регулювання та меж допустимості застосування штучного інтелекту в медицині дозволяє сформулювати такі узагальнені висновки.

Еволюція регулювання медичного ШІ демонструє поступовий перехід від етичних принципів до комплексних юридичних рамок, у межах яких автономія пацієнта, безпека, прозорість і підзвітність уже не лише декларуються, а набувають форми конкретних обов'язків для розробників, постачальників і користувачів систем ШІ. Етичні настанови ВООЗ щодо шести принципів використання ШІ у сфері охорони здоров'я фактично формують ціннісну основу для подальшого посилення відповідних вимог у медичному праві, стандартах належної клінічної практики застосування ШІ та ризик-орієнтованому підході до високоризикових систем [40, с. 30-31].

Запозичені з військової сфери моделі «людина поза контуром управління» (*human-out-of-the-loop*), «людина над контуром управління» (*human-on-the-loop*) та «людина в контурі прийняття рішення» (*human-in-the-loop*) у медичній сфері набувають ознак окремих режимів застосування ШІ, безпосередньо пов'язаних із вимогами міжнародних правових актів щодо

регулювання високоризикових систем. Вони вже не є виключно технічними моделями взаємодії людини з алгоритмом, а поступово перетворюються на інструменти юридичної диференціації режимів використання ШІ у чутливих сферах, насамперед у медицині.

Така градація дозволяє чітко розмежувати сфери, у яких може допускатися широка автономія систем ШІ, і сфери, де остаточне рішення безумовно має залишатися за людиною. У цьому контексті медичний ШІ стає своєрідним індикатором загальної дискусії щодо меж допустимої автономії алгоритмічних систем у сферах, чутливих до прав і свобод людини.

З точки зору перспектив національного регулювання медична сфера демонструє одну з найбільш послідовних моделей поєднання етичних принципів, технічних стандартів і загального законодавства у сфері ШІ. Вона засвідчує, що імплементація європейських підходів до регулювання ШІ неминуче потребуватиме одночасного врахування кількох нормативних рівнів: етичних принципів, загального акта про ШІ, секторальних медичних регламентів і міжнародних стандартів належної клінічної практики. У результаті саме медична сфера може стати галуззю, у межах якої в Україні будуть апробовані практичні моделі керованої автономії ШІ зі збереженням центральної ролі лікаря та пацієнта як основних носіїв прав і відповідальності.

Водночас слід зазначити, що українське законодавство, включаючи Концепцію розвитку штучного інтелекту в Україні 2020 р. та Закон України «Основи законодавства України про охорону здоров'я», наразі лише фрагментарно регулює питання цифровізації медичної сфери, електронної системи охорони здоров'я та обігу медичних даних, не містячи спеціальних положень щодо високоризикових систем ШІ.

Так, Закон України «Основи законодавства України про охорону здоров'я» [169] не містить спеціальних норм щодо залучення систем ШІ до процесу надання медичної допомоги. У зв'язку з цим інформована згода пацієнта на використання ШІ, у разі його застосування, має конструюватися як розширена форма інформованої добровільної згоди на медичне втручання,

передбаченої ст. 39, 43 та 43 [169] Основ законодавства України про охорону здоров'я, а також відповідними підзаконними нормативно-правовими актами у цій сфері.

Впровадження ШІ трансформує зміст інформованої згоди пацієнта. Класична доктрина виходить із того, що пацієнт має отримати зрозумілу інформацію про характер медичного втручання, можливі ризики та альтернативні варіанти лікування, після чого добровільно погоджується або відмовляється від нього. Однак у випадках, коли ключові клінічні рішення ґрунтуються на рекомендаціях або висновках алгоритмічних систем, постає питання про межі належного інформування пацієнта не лише щодо самої процедури, а й щодо ролі ШІ у її плануванні та здійсненні.

Для забезпечення поваги до автономії та гідності особи принципове значення має те, щоб пацієнт був поінформований: про факт використання системи ШІ у конкретному випадку; про функції, які така система виконує (діагностична підтримка, прогнозування, підбір терапії тощо); про обмеження та ризики, пов'язані з її застосуванням, зокрема можливість помилки або залежність результатів від якості вихідних даних.

Другою ключовою проблемою є визначення стандарту медичної допомоги в умовах використання ШІ.

З одного боку, ігнорування доступних алгоритмічних інструментів, здатних істотно підвищити точність діагностики або безпеку лікування, може розглядатися як недотримання сучасного професійного стандарту. З іншого боку, безкритичне покладання на рекомендації системи, яка має власні обмеження та потенційні похибки, створює ризик розмивання особистої професійної відповідальності лікаря.

Право має забезпечити баланс між цими крайнощами, виходячи з того, що ШІ у медичній сфері повинен виступати інструментом підтримки, а не заміни професійного клінічного судження. Остаточне рішення щодо встановлення діагнозу та вибору лікування має залишатися за лікарем, який зобов'язаний оцінювати як рекомендації алгоритмічної системи, так і

конкретний клінічний контекст.

У цьому контексті особливого значення набуває проблема розподілу відповідальності. Якщо шкода спричинена помилковим алгоритмічним рішенням або технічним збоєм системи ІІІ, пацієнт не повинен опинятися в ситуації, за якої жоден із суб'єктів не визнає обов'язку щодо відшкодування завданих збитків. Міжнародні та європейські підходи дедалі більше орієнтуються на модель розподіленої відповідальності, у межах якої вона покладається на всіх учасників відповідного технологічного ланцюга – від розробника та постачальника до закладу охорони здоров'я і лікаря – залежно від обсягу їх компетенції та характеру допущених порушень.

Важливого значення набуває також захист медичної таємниці та персональних даних, оскільки алгоритмічні системи потребують значних масивів інформації для навчання й подальшого функціонування, тоді як медичні дані належать до найбільш чутливих категорій персональної інформації. У цій сфері Україні необхідно не лише формально імплементувати європейські стандарти захисту даних, а й розробити спеціальні правові режими використання медичних даних у системах ІІІ з акцентом на деідентифікацію, мінімізацію даних, контроль доступу та забезпечення прозорості алгоритмічних процесів.

Важливим елементом цифрової трансформації медичної сфери є електронна система охорони здоров'я (eHealth) – державна інформаційно-комунікаційна система, що забезпечує автоматизацію обліку медичних послуг, обробку медичної інформації та інформаційну взаємодію між суб'єктами системи охорони здоров'я [75]. Використання такої системи створює передумови для інтеграції технологій штучного інтелекту, зокрема при автоматизованій обробці медичних даних, підтримці прийняття клінічних рішень та управлінні інформаційними процесами.

Порушення вимог щодо конфіденційності медичної інформації, зокрема незаконне розголошення лікарської таємниці або відомостей про стан здоров'я пацієнта, тягне цивільно-правову, дисциплінарну, а в окремих випадках й інші

види юридичної відповідальності. Це свідчить про те, що чинне законодавство вже сформувало базові правові механізми захисту прав пацієнтів у процесі використання цифрових медичних систем, які мають поширюватися й на застосування технологій штучного інтелекту.

Водночас важливим напрямом удосконалення правового регулювання є гармонізація національного законодавства з європейськими стандартами захисту персональних даних. З цією метою був розроблений проєкт Закону України № 8153 «Про захист персональних даних» [198], який передбачає деталізацію принципів обробки персональних даних, посилення вимог до отримання згоди суб'єкта даних, визначення правового статусу контролерів і операторів персональних даних, а також запровадження ефективних механізмів адміністративної та фінансової відповідальності за порушення законодавства у цій сфері [198]. Реалізація зазначених положень має важливе значення для забезпечення правомірного використання систем штучного інтелекту, діяльність яких значною мірою ґрунтується на обробці великих масивів персональних даних [51].

Нарешті, в умовах війни та післявоєнної відбудови особливого значення набуває використання ШІ у сфері медичної реабілітації, телемедицини та підтримки психічного здоров'я. Хоча таке впровадження відкриває значні можливості для підвищення доступності та якості медичної допомоги, особливо в умовах кадрового дефіциту, воно одночасно потребує посилення гарантій проти надмірної алгоритмізації рішень щодо найбільш уразливих категорій пацієнтів. У таких випадках обмеження використання ШІ мають бути спрямовані, насамперед, на забезпечення пріоритету людської гідності, індивідуального підходу та професійної відповідальності медичних працівників.

У сукупності наведені міркування дозволяють сформулювати для української правової політики кілька базових орієнтирів:

- закріплення вимоги обов'язкової інформованої згоди пацієнта з розкриттям ролі ШІ у процесах діагностики та лікування;

- визначення стандарту людиноцентричної медичної допомоги, у межах якого ІІІ виступає засобом підтримки, а не заміни професійного клінічного рішення лікаря;
- створення спеціальних правил розподілу відповідальності за шкоду, завдану внаслідок використання медичних систем ІІІ;
- запровадження особливого правового режиму захисту медичних даних, що використовуються для навчання та функціонування таких систем;
- встановлення додаткових обмежень щодо застосування ІІІ стосовно вразливих категорій пацієнтів.

Таким чином, правове регулювання медичного ІІІ має формуватися на засадах керованої автономії, за якої технологічний потенціал поєднується із пріоритетом людської гідності, професійної відповідальності та захисту прав пацієнта.

3.4. Правове регулювання обмеження використання штучного інтелекту в правоохоронній діяльності та діяльності спецслужб

Правоохоронна діяльність та діяльність спецслужб належать до найбільш чутливих сфер використання штучного інтелекту, оскільки безпосередньо пов'язані із реалізацією владних повноважень, застосуванням державного примусу, втручанням у приватне життя та обмеженням фундаментальних прав людини. У таких умовах інтеграція алгоритмічних систем у процеси оперативно-службової та розшуково-слідчої діяльності виходить за межі суто технологічної модернізації та набуває значення самостійної правової проблеми. У зв'язку з цим, на думку професора М. В. Карчевського, є актуальним «аналіз соціалізації технологій штучного інтелекту та дослідження тенденцій правового регулювання використання відповідних систем правоохоронними органами» [96].

Така актуалізація правового дискурсу зумовлена стрімкою цифровізацією безпекового сектору та зростанням ролі інформаційно-аналітичних технологій

у діяльності органів правопорядку. Прагнення держави підвищити ефективність управлінських процесів, оперативність реагування та результативність протидії правопорушенням стимулює активне впровадження інструментів штучного інтелекту у правоохоронну практику. Унаслідок цього системи ІІІ істотно розширили можливості органів правопорядку щодо аналізу великих масивів даних (Big Data), біометричної ідентифікації, прогнозування криміногенних ризиків, автоматизованого виявлення підозрілих зв'язків та аналітичної підтримки правоохоронної діяльності.

Разом з тим делегування окремих елементів правоохоронної діяльності алгоритмічним системам супроводжується виникненням складних етичних і правових проблем, пов'язаних із непрозорістю алгоритмічного оцінювання, ризиками дискримінації, масового цифрового спостереження, надмірного втручання у приватність та поступовим зменшенням реального людського контролю за застосуванням владних повноважень.

Проте реалізація зазначених концептуальних засад в Україні стикається не лише з правовими лакунами, а й із системними інституційними проблемами інфраструктурного характеру. Упровадження інтелектуальних аналітичних систем здійснюється на базі вже існуючих відомчих інформаційних ресурсів, значна частина яких формувалася без урахування сучасних вимог до цифрової інтеграції, обробки великих масивів даних та алгоритмічного аналізу інформації.

Оцінюючи цей стан, Т. І. Демчук справедливо зазначає, що «попри постійний розвиток інформаційних технологій та реформування правоохоронної системи України, ефективність застосування інформаційно-аналітичних та організаційних методів у практичній діяльності залишається обмеженою. Існує низка проблем, які знижують результативність роботи органів правопорядку та ускладнюють виконання завдань із забезпечення безпеки громадян» [66, с. 145].

Головним технологічним бар'єром для повноцінного впровадження моделей аналізу великих даних залишається відсутність єдиного інтегрованого

цифрового простору у сфері правоохоронної діяльності. Як зазначає вчений, «серед ключових проблем можна виокремити фрагментарність та недостатню інтеграцію відомчих інформаційних ресурсів, що призводить до дублювання інформації, втрати її актуальності та затримок у передачі даних між підрозділами» [66, с. 145].

На відсутність системності та комплексності щодо інформаційного забезпечення правоохоронних органів звертає увагу також І. П. Катеринчук, який розглядає принципи використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів як систему керівних ідей, що визначають зміст, спрямованість та межі правового регулювання процесів упровадження, застосування і контролю цифрових технологій [101, с. 22]. Такий підхід є особливо актуальним у контексті використання систем штучного інтелекту, функціонування яких потребує не лише технічного, а й постійного правового контролю, зокрема з боку правоохоронних органів [102, с. 29].

У контексті зазначених інституційних та технологічних проблем передчасне делегування окремих елементів правозастосовчої діяльності алгоритмічним системам може не лише відтворювати наявні інформаційні помилки, а й посилювати ризики порушення фундаментальних прав людини.

Водночас наявність таких інфраструктурних проблем не заперечує перспективності модернізації безпекового сектору, а навпаки, свідчить про необхідність формування цілісної системи цифрової інтеграції, стандартизації даних та належного правового й технічного забезпечення функціонування інтелектуальних аналітичних систем.

У сучасній правовій доктрині одним із напрямів подолання фрагментарності інформаційних ресурсів вважається перехід від накопичення даних до формування інтегрованих аналітичних систем на засадах Data Science. Досліджуючи цей вектор розвитку, М. В. Карчевський констатує, що «використання систем штучного інтелекту правоохоронними та судовими органами здатне забезпечити якісне оновлення їх діяльності» [100, с. 21], а впровадження інструментів машинного навчання та інтелектуального аналізу

даних є важливим напрямом розвитку сучасної системи превенції та розслідування правопорушень.

Проте автоматизація аналітичної функції поступово трансформує не лише технічні механізми обробки інформації, а й саму природу правозастосування. Якщо раніше алгоритми виконували переважно допоміжну роль, то сьогодні вони дедалі частіше впливають на формування підстав для юридично значущих рішень. За таких умов трансформації потребує і сама парадигма правового регулювання штучного інтелекту. Такої ж думки дотримуються В. М. Василенко [49], М. В. Корнієнко [124], О. С. Костенко [130], С. С. Кудінов [137], В. М. Підгородинський [178].

Ураховуючи вищевикладене вважаємо, що у сфері оперативно-службової та розшуково-слідчої діяльності концепція «юстиції штучного інтелекту» має полягати не у делегуванні владних повноважень алгоритмам, а у створенні системи правового контролю за їх функціонуванням. *За такої моделі використання інтелектуальних систем повинно бути чітко обмежене законом, а остаточне право перевірки, оцінювання та ухвалення юридично значущих рішень має незмінно залишатися за людиною.*

Проблемність використання ІІІ у правоохоронній діяльності полягає в тому, що алгоритмічні системи дедалі частіше не лише обробляють інформацію, а фактично формують підстави для вибору тактики правоохоронної діяльності, пріоритизації ресурсів, визначення зон підвищеної уваги, а в окремих випадках – впливають на оцінку особи та її процесуальний статус. За відсутності належних запобіжників це породжує ризики алгоритмічної упередженості, непрямой дискримінації, масового нагляду, порушення принципів законності, необхідності та пропорційності, а також поступового перетворення людини до пасивного виконавця алгоритмічних висновків, що несумісно з логікою правопорядку, заснованого на верховенстві права [35, с. 246].

Особливо гостро ці загрози проявляються у процесі використання біометричних технологій, зокрема розпізнавання облич у публічному просторі

та під час побудови прогнозних моделей злочинності, де статистичні закономірності можуть трансформуватися у механізми стигматизації окремих соціальних груп.

Розслідування злочинів традиційно ґрунтувалося на професійному досвіді, аналітичній роботі та оцінюванні доказів уповноваженими особами. Проте з упровадженням ІІІ у процеси виявлення та розслідування правопорушень істотно розширилися можливості інформаційно-аналітичного інструментарію правоохоронних органів та діяльності спецслужб. Такі системи здатні здійснювати складні зіставлення різномірної інформації, виявляти приховані взаємозв'язки між окремими подіями, моделювати поведінкові патерни, підтримувати оцінювання криміногенних ризиків та оптимізувати окремі процесуальні й аналітичні процедури.

Однією із ключових переваг застосування ІІІ у процесі досудового розслідування є здатність інтелектуальних систем оперативно та точно опрацьовувати значні обсяги відомостей, у тому числі звіти про злочини, записи камер спостереження та фінансові дані, щоб виявити закономірності та зв'язки, які можуть залишитися поза межами традиційного аналізу. Такі можливості суттєво підсилюють спроможність слідчих (детективів) до розкриття складних правопорушень, ідентифікації ключових підозрюваних та встановлення прихованих взаємозв'язків між, на перший погляд, непов'язаними між собою інцидентами.

ІІІ може використовуватися для прогнозування ризиків правопорушень шляхом опрацьовування масивів даних та виявлення закономірностей, що нерідко передують вчиненню вчиненню протиправних дій. Ураховуючи такі фактори, як час, місце та соціально-демографічні характеристики (за умови законності та обґрунтованості їх використання), алгоритми ІІІ можуть формувати прогнозні оцінки щодо потенційних зон підвищеного ризику та оптимізувати розподіл ресурсів правоохоронних органів. Такий превентивний підхід потенційно може сприяти зниженню рівня злочинності та підвищенню суспільної безпеки.

Крім того, інструменти ІІІ дають змогу частково автоматизувати рутинні

та трудомісткі процедури досудового розслідування. Наприклад, алгоритми розпізнавання обличчя можуть порівнювати зображення можливих підозрюваних із наявними базами даних, зменшуючи часові витрати слідчих на первинну ідентифікацію. Аналогічно, інструменти на базі ШІ можуть швидко аналізувати телефонні з'єднання або фінансові операції, допомагаючи виявляти підозрілі зв'язки та точніше встановлювати часову послідовність подій.

Опрацювання значного обсягу зображень і відеоматеріалів у стислі строки є трудомістким завданням, що супроводжується підвищеним ризиком помилок, зумовлених втомою, перевантаженням та іншими антропогенними чинниками. Алгоритмічні системи, на відміну від людини, можуть здійснювати безперервний аналіз мультимедійної інформації, що зумовлює їх потенційну ефективність у процесі масштабного опрацювання цифрових візуальних даних. Так, у межах ініціатив на кшталт «Intelligence Advanced Research» [406], включно з проєктами у сфері комп'ютерного зору (зокрема «Janus Activity»), проводяться випробування алгоритмів, здатних здійснювати ідентифікацію осіб за біометричними ознаками шляхом аналізу рис обличчя за моделлю, наближеною до роботи людського аналітика [310].

Окремі приклади аналітичних платформ на базі ШІ вже застосовуються в практиці правоохоронних органів. Так, за наведеними джерелами, у підрозділах поліції Великої Британії використовується Qlik Sense - програмне забезпечення, розроблене компанією Qlik Technologies [402], яке забезпечує інтеграцію понад 10 раніше розрізнених баз даних, включаючи журнали усіх екстрених викликів, реєстри зареєстрованих злочинів, інформацію про судимості, відомості про предмети й технічні засоби, пов'язані із правопорушеннями. Повідомляється, що система використовується на рівні патрульних підрозділів, може залучатися під час первинного реагування та перевірки відомостей на місці події, а також підтримує ухвалення превентивних рішень у сфері запобігання правопорушенням. За даними джерела, у 2024 році лондонська поліція розгорнула понад 117 точок застосування цієї технології [439], що позиціонується як підтвердження її результативності.

У Південній Кореї застосовується система розпізнавання облич Dejaview, розроблена ETRI, яка здійснює не лише моніторинг у режимі реального часу, а й аналізує потенційно криміногенні ситуації та може використовуватися для превенції окремих правопорушень [281]. Система використовує машинне навчання для аналізу ситуативних патернів і виявлення ознак потенційної протиправної поведінки, враховуючи такі фактори, як час доби, місце події та історію інцидентів [342].

Однією з найвідоміших технологій III у сфері біометричної ідентифікації осіб у правоохоронній практиці є Clearview AI [324] – американська система з розпізнавання облич, яка використовується, зокрема, правоохоронними органами.

Зазначена технологія позиціонується як інструмент підтримки розкриття злочинів у США [324] і дозволяє правоохоронним органам за фотографією особи здійснювати пошук збігів у базі даних, формувати посилання на відповідні зображення в мережі Інтернет та водночас опрацьовувати значні обсяги фото- і відеоданих, включаючи матеріали вебкамер. Технологія також застосовувалася для розшуку жертв злочинів [397].

Водночас твердження про «лише кілька» випадків помилкової ідентифікації потребують критичної оцінки з огляду на обмеженість публічних даних, різницю методик обліку та потенційну нерепрезентативність відомих випадків. У відкритих джерелах повідомлялося про окремі випадки помилкової ідентифікації за допомогою розпізнавання обличчя Clearview AI [324], але, за твердженням розробників, такі помилки пов'язані переважно з якістю аналізованих світлин [324], а не з недоліками функціонування самої технології.

У березні 2022 року компанія Clearview AI надала Україні доступ до своєї системи розпізнавання облич у межах підтримки оборони держави в умовах російської збройної агресії. Спочатку доступ було надано Міністерству оборони України, а згодом до проєкту приєдналися й інші відомства, зокрема Національна поліція України [304] з метою ідентифікації осіб, причетних до агресії та виявлення колаборантів. За наведеними даними, станом на 2023 рік

завдяки технології було опрацьовано понад 30 млрд фотографій із соцмереж та інформаційних стрічок [86, с. 151], а її використання в окремих джерелах оцінюється як результативне [412]. Повідомляється, що технологія застосовується для перевірки осіб на блоктах, ідентифікації загиблих військовослужбовців і військовополонених, а також пошуку зниклих безвісти. Водночас застосування технологій розпізнавання облич у воєнному контексті має відбуватися з дотриманням вимог законності, необхідності та пропорційності, а також процесуальних гарантій, зокрема під час розслідування воєнних злочинів.

Отже, потенціал використання ІІІ у правоохоронній діяльності пов'язаний насамперед із можливістю інтелектуального опрацювання інформації, виявлення прихованих взаємозв'язків та підтримки складних аналітичних процесів у стислі строки. Крім того, алгоритмічні системи можуть застосовуватися для оцінювання достовірності окремих відомостей або рівня довіри до джерел інформації – за умови чітко визначених критеріїв та обов'язкової верифікації результатів людиною.

Водночас ризик порушення прав людини з використанням ІІІ суттєво зростає, адже, працюючи з великими масивами даних, ІІІ самостійно формує закономірності та прогнозні оцінки, зокрема у сфері криміногенної активності, а в окремих конфігураціях – і для виявлення корупційних ризиків. За відсутності належних запобіжників (якість даних, контроль упереджень, підзвітність і можливість оскарження) це може посилювати дискримінаційні практики через непряме «профілювання» за формально об'єктивними ознаками (місце проживання, соціально-демографічні характеристики, типові маршрути тощо) в різних регіонах [33, с. 135].

Відомі випадки алгоритмічної дискримінації, пов'язані з машинною обробкою даних і ризик-стратифікацією груп населення. Зокрема, використання алгоритмічних інструментів оцінювання ризику (небезпеки особи) у деяких штатах США призводило до дискримінаційних наслідків щодо афроамериканців, які не мали попереднього кримінального досвіду: алгоритм

оцінював їх як «більш ризикових/небезпечних», ніж білих правопорушників, які мали суттєвий попередній кримінальний досвід [288], хоча за фактичними обставинами окремі з них могли становити більший реальний ризик [337]. Цей приклад демонструє, що «об'єктивність» автоматизованих оцінок може бути уявною: результати залежать від якості даних, обраних змінних та припущень, закладених у модель.

Окремим напрямом застосування ІІІ є аналітичне прогнозування злочинності шляхом опрацювання даних та виявлення закономірностей, що часто передують протиправній поведінці. Однак застосування таких інструментів є допустимим лише за наявності чіткої правової підстави та визначеної легітимної мети, із дотриманням вимог законності, необхідності й пропорційності, а також за умови принципу мінімізації даних і недопущення втручання в приватність. Ураховуючи такі фактори, як час, місцезнаходження та соціально-демографічні характеристики (лише настільки, наскільки це обґрунтовано метою та не створює дискримінаційного ефекту), алгоритми ІІІ можуть формувати прогнозні оцінки щодо потенційних зон підвищеного ризику та допомагати правоохоронним органам раціональніше розподіляти ресурси. Водночас такий підхід може мати подвійний ефект: поряд з потенційним зниженням рівня правопорушень і підвищенням суспільної безпеки він здатен посилювати профілювання та непряму дискримінацію, якщо моделі навчаються на упереджених даних або застосовуються без належного людського контролю, прозорості критеріїв і можливості оскарження [34, с. 9].

Системи ІІІ, здатні формувати оцінки щодо локальних «сплесків» злочинності, можуть бути корисними для планування розподілу ресурсів, формування кадрового і фахового складу, залучення необхідних фахівців, вибору систем захисту та спеціальних засобів тощо. Разом з тим рішення, що ґрунтуються на таких оцінках, мають залишатися підконтрольними людині та підлягати перевірці й процедурі оскарження, аби мінімізувати ризики порушення прав людини.

Інтелектуальні алгоритми, як вже зазначалось, можуть аналізувати великі

обсяги даних, виявляючи закономірності та тенденції, які можуть підтримувати дії правоохоронних органів, визначати потенційні осередки злочинності та групи, що перебувають у зоні ризику, а також виокремлювати типи правопорушень, що найчастіше трапляються у певних локаціях або сферах. Більше того, «предиктивна поліцейська діяльність» (predictive policing) – один із найбільш дискусійних прикладних напрямів ІІІ у правоохоронній діяльності – використовує можливості аналізу даних для прогнозування ймовірності злочинних подій у певних місцях/періодах, а не «злочинів до того, як вони відбудуться» у буквальному розумінні.

Як зазначає В. Г. Пядишев, «на відміну від традиційних методів, штучний інтелект пропонує динамічний підхід до розкриття злочинів, використовуючи можливості аналізу даних, машинного навчання та розпізнавання образів. Здатність систем штучного інтелекту швидко обробляти величезні обсяги інформації дозволяє правоохоронним органам виявляти закономірності, виявляти потенційних підозрюваних та активно запобігати злочинам» [220, с. 409]. Такі заходи можуть допомогти правоохоронним органам стати більш ефективними, зосередивши свої ресурси там, де вони найбільше потрібні.

Виклики, з якими стикається українська правоохоронна та судова системи у воєнний час, зокрема «блокування чи ускладнення роботи установ на деокупованих та прифронтових територіях, нестача кадрів, велика кількість справ та ін.», підвищують об'єктивну потребу технологічної підтримки та звернення до інструментів ІІІ у сфері кримінальної юстиції в Україні, однак через підвищені ризики для прав людини, вимоги до процесуальних гарантій та наслідки помилок для свободи та гідності особи її водночас називають «найменш перспективною для імплементації ІІІ» [172].

Зазначені обставини актуалізують питання про допустимий ступінь автономізації правозастосовчої діяльності та межі участі алгоритмічних систем у процесах ухвалення юридично значущих рішень. Саме у цьому контексті в науковій літературі пропонуються різні моделі класифікації рівнів залучення ІІІ у сферу кримінальної юстиції.

У сучасній доктрині одним із ключових критеріїв допустимості використання ІІІ у сфері правозастосування вважається ступінь збереження людського контролю над алгоритмічними системами. У зв'язку з цим поширення набули концепції human-in-the-loop, human-on-the-loop та human-out-of-the-loop [338], які відображають різні моделі співвідношення автономності систем ІІІ та участі людини у процесі ухвалення юридично значущих рішень. Саме в межах такого підходу формуються й більш деталізовані класифікації рівнів автономізації правозастосовчої діяльності. Зокрема, Л. Еліот, з метою оцінювання ступеня залученості ІІІ в правничу діяльність, запропонував таку класифікацію [335] рівнів автоматизації правозастосовчої діяльності:

- рівень 0 – повна відсутність автоматизації;
- рівень 1 – базова автоматизація (електронний документообіг, онлайн-сервіси нормативної інформації);
- рівень 2 – розширена автоматизація: використання систем машинного навчання для класифікації даних юридичної практики та інтелектуалізованого пошуку в юридичних базах даних із застосуванням методів обробки природної мови;
- рівень 3 – напіваавтономна автоматизація, що передбачає використання експертних систем підтримки ухвалення рішень і формулювання висновків у конкретних справах;
- рівень 4 – автономізація окремих галузей юридичної діяльності, за якої допускається ухвалення повністю автономних рішень у певних сегментах правозастосування (наприклад, частково автономний нотаріат або автономний адміністративний документообіг);
- рівень 5 – повна автономізація правозастосовчої діяльності на основі систем «сильного» ІІІ, здатних моделювати людський інтелект;
- рівень 6 – гіпотетична надлюдська автономність, заснована на використанні штучного інтелекту, який перевищує інтелект людини [335].

У правоохоронній діяльності така шкала особливо показова, адже зі

зростанням рівня автоматизації зростають і ризики для прав людини та вимоги до контролю.

Інтеграція ІІІ в оперативно-розшукову діяльність та діяльність органів досудового розслідування супроводжується ризиками *порушення конфіденційності, алгоритмічної упередженості та недотримання принципу пропорційності*. У світовій практиці застосування систем біометричної ідентифікації та алгоритмічного аналізу вже фіксувалися випадки арештів невинуватих осіб, зумовлені помилковою ідентифікацією, алгоритмічною упередженістю та іншими недоліками функціонування автоматизованих систем [415]. Наслідки подібних помилок ставали предметом судового розгляду та знаходили відображення у практиці ЄСПЛ [318; 305; 476].

Здійснений аналіз показує, що сучасні практики застосування ІІІ у сфері безпеки й правопорядку мають подвійний ефект. З одного боку, такі технології істотно підсилюють аналітичні можливості правоохоронних органів через інтеграцію інформаційних ресурсів, оперативне опрацювання значних обсягів даних, часткову автоматизацію окремих процедур та прогнозування ризиків. З іншого – надмірна довіра до алгоритмічних систем здатна спричиняти помилки, наслідком яких стають порушення прав людини [491]. Особливо небезпечними такі ризики є у випадках, коли алгоритмічні результати фактично перетворюються на підставу для управлінських або процесуальних рішень без належної перевірки, контролю та можливості ефективного оскарження.

За таких умов застосування ІІІ не може ґрунтуватися виключно на критеріях технологічної ефективності. Використання алгоритмічних систем у правоохоронній діяльності повинно здійснюватися в межах чітко визначених стандартів законності, необхідності, пропорційності, підзвітності та процесуального контролю. ІІІ може використовуватися лише як допоміжний інструмент аналітичної підтримки, не підміняючи юридичну оцінку обставин справи, індивідуалізацію рішень та дискреційні повноваження уповноваженої особи. Відповідно, застосування таких систем має супроводжуватися ефективними механізмами перевірки, постійного людського контролю та

можливістю оскарження наслідків використання алгоритмічних рішень.

Саме такі ризики зумовили потребу у формуванні диференційованого правового режиму та системи посилених запобіжників, закріплених у Регламенті (ЄС) 2024/1689 Європейського парламенту та Ради від 13 червня 2024 року, яким встановлюються гармонізовані правила щодо штучного інтелекту (AI Act).

Одним із ключових ризиків використання ШІ у правоохоронній сфері є *алгоритмічна упередженість*, здатна спричиняти дискримінаційні наслідки щодо окремих соціальних груп. Оскільки моделі ШІ навчаються на основі значних обсягів інформації, вони можуть успадковувати та посилювати статистичні перекося, закладені у вихідних даних і практиках їх формування. У результаті алгоритмічні системи здатні відтворювати вже наявні форми соціальної нерівності та впливати на правозастосовчу практику у спосіб, несумісний із принципами рівності та недискримінації.

Проблема полягає в тому, що системи ШІ, навчаючись на даних, які формально відображають соціальну реальність, але водночас містять елементи структурної нерівності, здатні надалі відтворювати й посилювати відповідні патерни [161]. Саме на такий ризик у контексті американської правоохоронної практики звертають увагу дослідники: «можуть бути злочини, скоєні в районах, де більшість становлять меншини. Тож, якщо ви дуже некритично прочитаєте дані, ви почнете зупиняти та обшукувати темношкірих та латиноамериканців» [491].

За таких умов аналітичні висновки ШІ повинні розглядатися виключно як допоміжний інструмент правозастосування, а не як самодостатня підстава для втручання у права людини без додаткової перевірки, належних процесуальних гарантій та можливості ефективного оскарження.

Одним із найбільш відомих прикладів алгоритмічної упередженості та расової дискримінації у сфері автоматизованого оцінювання ризиків є система COMPAS, яка використовувалася у судовій практиці США для прогнозування ризику рецидиву. У 2016 році журналістське розслідування ProPublica

встановило, що алгоритм суттєво частіше помилково відносив темношкірих осіб до групи підвищеного ризику повторного правопорушення (45 %), ніж білих осіб (23%) [288]. На проблему расової упередженості та алгоритмічної дискримінації у функціонуванні COMPAS також звертають увагу американські дослідники алгоритмічних помилок і bias-моделей [377; 527].

Недопустимість подібної логіки використання ШІ підкреслює риторичне питання Н. Руди, старшого аналітика ІТ-фірми Enterprise Strategy Group: «Якщо 90 відсотків згвалтувань скоюють чоловіки, чи повинні ми ув'язнювати всіх чоловіків? [491]. Цей приклад демонструє одну з ключових методологічних пасток алгоритмічного прогнозування: статистичні закономірності, виявлені на рівні груп, не можуть автоматично трансформуватися у підставу для індивідуалізованих правових наслідків щодо конкретної особи.

Ще одним ключовим ризиком використання ШІ у правоохоронній діяльності є проблема *конфіденційності та надмірного втручання у приватне життя*. Широке застосування систем спостереження на основі ШІ об'єктивно підвищує імовірність постійного або тривалого моніторингу переміщень і поведінки осіб без їх поінформованої згоди, особливо за відсутності чітких правових підстав, процедур отримання дозволів, часових і цільових обмежень обробки даних, а також ефективних механізмів контролю та підзвітності.

Якщо раніше подібне спостереження переважно розглядалося як похідний елемент ризиків алгоритмічної упередженості та дискримінації, то у новітній правовій і аналітичній доктрині його дедалі частіше виокремлюють як самостійний ризик використання ШІ у сфері безпеки та правопорядку [283].

У 2025 році видання Veritone зазначало, що масове впровадження систем відеоспостереження на основі ШІ, зокрема технологій розпізнавання облич, за відсутності належного правового регулювання та впорядкованих механізмів оскарження створює загрозу постійного нагляду за громадянами без їх згоди. Подібні практики можуть формувати сприйняття втручання у приватність як свавільного та підривати довіру до діяльності правоохоронних органів [282].

У звіті Diplomatic Courier (2025) «Law Enforcement Embraces AI Amid

Privacy Concerns» також підкреслюється, що використання систем біометричної ідентифікації створює серйозні виклики для захисту конфіденційності через недостатність людського контролю, непрозорість алгоритмів та ризики дискримінації [426]. У зв'язку з цим автори наголошують на необхідності посилення законодавчих рамок і залучення фахівців з етики до формування політики використання ІІІ у правоохоронній сфері.

Окрему проблему становить і *ризик витоку інформації*. При цьому йдеться не лише про безпеку окремої особи, а й про загрози для спільнот, держав та міждержавних об'єднань.

Витік інформації із систем ІІІ може бути наслідком недостатньої кіберзахищеності таких систем або цілеспрямованих атак з боку злоумисників. У випадках несанкціонованого доступу до баз персональних даних відповідна інформація може бути викрадена та використана для шахрайства, шантажу чи інших протиправних цілей. Додаткові загрози виникають під час міжвідомчого обміну інформацією, взаємодії з підрядниками, а також у процесі зберігання відомостей у хмарних сервісах без достатніх гарантій договірного захисту, сегментації доступу та журналювання дій користувачів.

На сьогодні вже зафіксовано випадки витоку персональних даних, пов'язані з помилками алгоритмічних систем або непередбачуваними технічними ситуаціями як в Україні, так і у світі [283; 174]. Водночас значна частина таких інцидентів не набуває широкого розголосу через *відсутність прозорості звітності, нерозкриття обставин інцидентів або складність встановлення причинно-наслідкового зв'язку між технологічним збоєм і порушенням прав людини*.

Показовим у цьому контексті є випадок 2018 року, пов'язаний із масовим збором та обробкою персональних даних користувачів Facebook. Унаслідок цього компанія Cambridge Analytica, яка спеціалізувалася на аналітиці даних для політичних кампаній, отримала доступ до персональної інформації мільйонів користувачів без їх належної згоди [231]. Хоча зазначений кейс не зводиться виключно до помилок ІІІ, він наочно демонструє, як аналітичні

технології та цифрові екосистеми обробки інформації здатні створювати масштабні ризики для приватності за відсутності ефективних правових і технічних запобіжників.

Використання ШІ для пошуку та аналітичного опрацювання приватної інформації неминуче пов'язане з роботою з Big Data та створює *ризик ненавмисного виявлення персональних даних*, якщо щодо них попередньо не були застосовані належні механізми захисту. Як зазначають К. Мартін та Дж. Зіммерман, аналізуючи екосистемну перспективу ШІ [435], такі ризики можуть бути зумовлені недостатньою точністю алгоритмів анонімізації та деідентифікації, а також можливістю деанонімізації особи шляхом повторного поєднання наборів даних і встановлення ідентифікаційних ознак за непрямыми атрибутами.

Загрозу приватності також становлять технології розпізнавання обличчя (Facial Recognition) [529; 531], які часто позиціонуються як одна з ключових технологічних переваг використання ШІ у розшуковій та ідентифікаційній діяльності [531; 484]. Водночас застосування таких систем без належної правової підстави та процесуальних гарантій, коли персональні дані збираються й обробляються без достатньої поінформованості та контролю з боку суб'єктів даних [142], створює високі ризики непропорційного втручання у приватне життя.

Практика правоохоронних органів у цій сфері неодноразово ставала предметом критики, а відповідні підходи держав зазнавали корекції під впливом судового контролю, зокрема у зв'язку з рішенням ЄСПЛ [315; 316], в яких втручання визнавалося непропорційним або недостатньо врегульованим законом. Окремого загострення набуває проблема збирання та використання зображень із соціальних мереж без згоди користувачів [25].

Крім систем оцінювання ризиків та розпізнавання облич, функціонують і системи ШІ, здатні підтримувати аналіз доказової інформації. Їх функціонал може охоплювати аналіз документальних доказів, виявлення закономірностей у доказовій базі, а також ідентифікацію потенційних суперечностей або помилок

у матеріалах досудового розслідування. Такі системи здатні аналізувати й зіставляти відеозаписи, фінансові транзакції, електронне листування, результати моніторингу соціальних мереж та інші цифрові відомості, виявляючи неочевидні взаємозв'язки, які можуть залишатися поза межами традиційного аналізу доказів [522]. Водночас результати подібного аналізу повинні мати виключно допоміжний характер і підлягати обов'язковій перевірці людиною, оскільки помилки алгоритмічної моделі або хибні кореляції можуть призводити до формування неправомірних слідчих версій та непропорційного втручання у права людини.

Починаючи з 2020 року Amnesty International закликає до прямої заборони використання технологій розпізнавання облич на основі ШІ у правоохоронній практиці [286]. Аналогічні застереження з 2023 року висловлює і Українська Гельсінська спілка з прав людини, досліджуючи ризики застосування таких технологій у Європі та в Україні [232].

Однак інтеграція ШІ у слідчу (розшукову) та оперативно-службову діяльність не позбавлена низки викликів, що постають на перетині оперативної доцільності, технічної спроможності та гарантій прав людини. Насамперед ідеться про конфіденційність і захист персональних даних, які опиняються в зоні підвищеного ризику за умов масового використання систем відеоспостереження, автоматизованого моніторингу комунікацій та аналітики великих масивів інформації про поведінку окремих осіб та груп. Забезпечення розумного балансу між суспільною потребою у превенції правопорушень і правом людини на приватність залишається складним правовим завданням. Водночас очікування, що такий баланс може бути автоматично гарантований алгоритмічною системою, видається ще більш проблематичним.

У цьому контексті використання ШІ у слідчій та оперативно-розшуковій діяльності постає одночасно як потужний інструмент підвищення ефективності та як джерело нових, іноді важкопрогнозованих, правових ризиків. Здатність інтелектуальних систем опрацьовувати значні обсяги даних, виявляти кореляції, які виходять за межі людського сприйняття, моделювати можливі

потенційні зони підвищеного криміногенного ризику та частково автоматизувати окремі етапи розслідування здатна істотно посилити спроможність правоохоронних органів. Однак без правових і технічних запобіжників такі інструменти можуть перетворитися на механізми масового спостереження, алгоритмічного профілювання та непрямой дискримінації окремих категорій осіб, що суперечить базовим цінностям демократичного суспільства.

Саме технології розпізнавання обличчя дедалі частіше опиняються в центрі фахових дискусій щодо допустимих меж застосування ШІ в публічному просторі [61; 5; 159] Guidelines on Facial Recognition (Council of Europe, 2021) підкреслює, що технології розпізнавання обличчя як різновид біометричних технологій можуть істотно впливати на право на приватність, захист персональних даних, людську гідність та інші фундаментальні права. Документ пропонує окремі рекомендації для законодавців, розробників і користувачів таких систем [336].

У EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement Європейська рада із захисту даних наголошує, що використання технологій розпізнавання обличчя правоохоронними органами повинно відповідати принципам законності, необхідності та пропорційності, а окремі форми їх застосування можуть бути несумісними з вимогами щодо захисту фундаментальних прав [361].

Для правоохоронної діяльності вони розглядаються як один із найбільш ефективних інструментів ідентифікації осіб, оскільки дають змогу оперативно встановлювати особу у публічному просторі, зіставляти отримані дані з наявними базами розшукуваних осіб, відстежувати маршрути пересування тощо. Проте за відсутності чітких правових критеріїв, часових і цільових обмежень щодо обробки персональних даних, а також ефективного зовнішнього контролю подібні практики неминуче трансформуються у приховані механізми масового нагляду, в межах яких згода суб'єкта даних фактично або ігнорується, або набуває суто формального характеру .

Очевидно, що «накопичений досвід та «критична» маса загроз неконтрольованого розширення сфери застосування систем штучного інтелекту зумовили появу законодавчих ініціатив, спрямованих на створення комплексної нормативно-правової бази для забезпечення відповідального розвитку штучного інтелекту, захисту основних прав і сприяння інноваціям» [98]. Одним із найбільш показових прикладів такого підходу стало прийняття AI Act [472]. Запровадження на рівні ЄС єдиних стандартів регулювання дозволяє мінімізувати ризики використання ШІ у правоохоронній діяльності та діяльності спецслужб, оскільки акт містить прямі заборони окремих небезпечних і маніпулятивних практик, а також спеціальні вимоги щодо застосування високоризикових систем.

AI Act ґрунтується на ризик-орієнтованому підході: він не забороняє ШІ у правоохоронній сфері загалом, а розмежовує (1) практики, несумісні з фундаментальними правами, які підлягають забороні, і (2) високоризикові системи, застосування яких допускається лише за умови дотримання спеціальних вимог і процедур відповідності. Пряма заборона стосується конкретних типів застосувань, у тому числі у діяльності поліції та спецслужб (AI Act, art. 5) , зокрема:

1) використання систем, що застосовують сублімінальні техніки, маніпулюють поведінкою осіб або експлуатують вразливість окремих груп населення (зокрема дітей та осіб з інвалідністю) з метою суттєвого викривлення поведінки, яке може спричинити шкоду;

2) системи соціального рейтингування (social scoring), що здійснюють оцінювання осіб на підставі їхньої соціальної поведінки або особистісних характеристик;

3) системи біометричної категоризації, які класифікують осіб за чутливими ознаками (зокрема расовим чи етнічним походженням, політичними поглядами, релігійними переконаннями або сексуальною орієнтацією);

4) окремі форми застосування систем віддаленої біометричної ідентифікації у публічно доступних місцях. Зокрема, використання технологій

«real-time» у правоохоронних цілях як загальне правило забороняється, однак допускається у виняткових випадках за наявності чітко визначених законом умов: належної правової підстави, вузько окресленої легітимної мети, дотримання принципів необхідності й пропорційності, а також попереднього дозволу чи контролю компетентного органу (зокрема судового контролю). Такі винятки можуть застосовуватися, наприклад, для розшуку окремих осіб, підозрюваних у вчиненні тяжких злочинів, або запобігання терористичним загрозам.

Таким чином, AI Act прямо виводить за межі допустимого для правоохоронних органів і спецслужб ті види застосування ІІІ, які визнаються несумісними з фундаментальними цінностями ЄС через їх непропорційний і системний вплив на права людини (приватність, свободу пересування, свободу зібрань, заборону дискримінації), а також через створення інфраструктурних ризиків масового нагляду та стигматизації окремих груп.

Системи ІІІ, що використовуються у правоохоронній діяльності, здебільшого класифікуються AI Act як високоризикові (high-risk). Для виробників і операторів таких систем встановлено комплекс спеціальних обов'язків (розд. ІІІ, гл. 2) [4]. AI Act вимагає не формального впровадження інтелектуальних технологій у чутливі сфери, а побудови повноцінної системи управління ризиками, орієнтованої насамперед на захист прав людини. Йдеться про безперервний процес виявлення, аналізу та мінімізації ризиків, пов'язаних з алгоритмічною упередженістю, непрямую дискримінацією, надмірним втручанням у приватність або створенням непропорційних загроз для окремих груп населення.

Така система ризик-менеджменту повинна функціонувати як реальний механізм превенції, здатний виявляти та усувати небезпечні конфігурації ще до впровадження відповідних технологій у правозастосовчу практику.

Окремий акцент AI Act робить на якості даних, на яких здійснюються навчання та тестування систем ІІІ. Навчальні, валідаційні й тестові набори даних повинні бути релевантними цілям функціонування системи,

репрезентативними щодо цільової популяції та максимально вільними від явних і прихованих упереджень. Якщо алгоритмічна модель некритично успадковує системні перекоси та структурні викривлення даних – етнічні, соціальні чи територіальні, – вона здатна не лише відтворювати, а й посилювати вже наявні форми несправедливості, що прямо суперечить логіці людиноцентричного регулювання ІІІ.

У зв'язку з цим вимоги до якості даних і систем управління ризиками мають супроводжуватися належною простежуваністю функціонування систем ІІІ та можливістю зовнішньої перевірки. Інакше навіть формально коректні процедури залишатимуться фактично недоступними для ефективного контролю.

Не менш важливими елементами регулювання є вимоги до технічної документації та забезпечення прозорості функціонування систем ІІІ. Алгоритми, джерела даних, параметри навчання, умови та режими застосування мають бути задокументовані таким чином, щоб компетентний орган, аудитор або суд могли здійснити змістовну перевірку відповідності системи вимогам права, а не покладатися виключно на запевнення виробника. Чим чутливішою є сфера застосування ІІІ (зокрема діяльність правоохоронних органів і спецслужб), тим більш обмеженою стає можливість посилення на «комерційну таємницю» як підставу для непрозорості алгоритмічних рішень.

Обов'язковим елементом архітектури високоризикових систем ІІІ є також логування – автоматична фіксація ключових подій і рішень системи у формі журналів подій. Це необхідно не лише для технічного аудиту, а й для відновлення причинно-наслідкового ланцюга функціонування системи: хто, коли і на підставі яких даних ініціював її запуск, які вихідні результати згенерував алгоритм, до яких правових наслідків це призвело, а також чи були своєчасно виявлені та усунуті помилки. За відсутності такого «цифрового сліду» ефективний контроль, незалежний аудит і притягнення до юридичної відповідальності істотно ускладнюються.

Нарешті, ключовою гарантією безпечного використання високоризикових

систем ШІ є людський нагляд (human oversight). У цьому контексті AI Act фактично орієнтується на моделі «людина в контурі управління» (human-in-the-loop) та «людина над контуром управління» (human-on-the-loop), водночас обмежуючи допустимість повної автономізації правозастосування за моделлю «людина поза контуром управління» (human-out-of-the-loop). Такі системи повинні проектуватися у спосіб, за якого людина залишається не формальним спостерігачем, а реальним суб'єктом контролю, здатним призупинити функціонування алгоритму, перевірити та за потреби відхилити його висновок, поставити під сумнів запропоноване рішення й ухвалити інше, керуючись правовими та етичними критеріями.

Таким чином, AI Act закріплює модель, за якої допустимість використання ШІ у правоохоронній діяльності визначається не рівнем технологічної ефективності системи, а ступенем забезпечення прав людини, процесуального контролю та можливості реального людського втручання у функціонування алгоритмічних механізмів.

3.5. Правове регулювання обмеження використання штучного інтелекту в правосудді

У сфері правосуддя вимога людського контролю набуває особливого значення, оскільки судові рішення є не лише результатом формального застосування норми права, а й актом юридичної оцінки, що передбачає інтерпретацію, внутрішнє переконання судді, оцінку доказів, дотримання принципів справедливості та пропорційності. У зв'язку з цим повна автономізація судового розсуду суперечила б самій природі правосуддя як форми реалізації державної влади, заснованої на принципі верховенства права.

Цифровізація судової системи та впровадження технологій штучного інтелекту у сферу правосуддя поступово трансформують не лише технічні механізми здійснення судочинства, а й саму природу судового розгляду та ухвалення юридично значущих рішень. Якщо на початкових етапах

алгоритмічні системи використовувалися переважно для автоматизації документообігу, пошуку судової практики чи аналітичної підтримки судді, то сучасні моделі штучного інтелекту дедалі активніше інтегруються у процеси оцінки доказів, прогнозування судових рішень та формування рекомендацій щодо правозастосування. За таких умов проблема меж допустимого використання ШІ у сфері правосуддя набуває не лише технологічного, а насамперед аксіологічного та конституційно-правового значення.

У статті 6 Європейської конвенції про захист прав людини і основоположних свобод закріплено право на розгляд справи незалежним і «безстороннім судом» [113], однак прямої вказівки на те, що таким суддею має бути саме людина, цей міжнародно-правовий акт не містить. Водночас конституції багатьох держав, зокрема й України (ст. 127 Конституції України [115]), прямо визначають, що правосуддя здійснюють судді, а відповідний правовий статус у сучасних правових системах належить виключно людині [483]. Відповідно до чинних засад сучасного законодавства на ШІ не може бути покладено функцію здійснення правосуддя.

Попри це, у сучасному правничому дискурсі активно тривають наукові дискусії щодо допустимих меж і доцільності використання ШІ у сфері правосуддя в різних формах та функціональних моделях. Як показує практика, сучасні проєкти нормативно-правових актів дедалі частіше розробляються з урахуванням можливості їх автоматизованого сприйняття та застосування цифровими системами, зокрема системами ШІ, на що прямо звертають увагу відповідні проєктні групи [341].

ШІ завдяки своєму потенціалу, швидкості обробки інформації, точності та очікуваній доступності відкриває значні перспективи для підвищення ефективності функціонування системи правосуддя. Проте саме у сфері судочинства переваги алгоритмічної обробки даних найгостріше стикаються з вимогами справедливого суду, суддівської незалежності, мотивованості рішення та збереження людського контролю над актом правосуддя. Отже, використання ШІ у сфері правосуддя поряд із потенційними перевагами

зумовлює виникнення низки ризиків, які потребують належного правового осмислення та врахування.

У зв'язку з цим доцільним є окремий аналіз як потенційних переваг інтеграції систем ІІІ у процес здійснення правосуддя, так і ризиків, пов'язаних із таким використанням.

Як уже зазначалося, ІІІ слід розглядати як високошвидкісний та ефективний технологічний інструмент, здатний здійснювати складну обробку значних масивів інформації, виявляти закономірності, формувати інформаційно-аналітичні моделі та синтезувати відповідні висновки на основі закладених алгоритмів функціонування. Такі можливості потенційно можуть бути корисними і для системи правосуддя, насамперед у частині аналітичної, інформаційно-пошукової та допоміжної процесуальної діяльності.

До переваг використання ІІІ у сфері правосуддя, як і в інших галузях суспільної діяльності, слід віднести можливість автоматизації складних і тривалих рутинних процесів, виконання яких потребує значних часових ресурсів та високої концентрації уваги. Саме під час монотонної обробки великих масивів інформації людина найбільш схильна до втоми та допущення помилок. У цьому контексті системи ІІІ здатні ефективно аналізувати значні обсяги нормативно-правових актів, судової практики, наукових джерел та інших інформаційних масивів з метою пошуку релевантної правової інформації або доказових матеріалів, у тому числі з відкритих джерел [25; 486].

Разом із тим стаття 16 Кодексу суддівської етики прямо визначає, що «використання суддею технологій штучного інтелекту є допустимим, якщо це не впливає на незалежність та неупередженість судді, не стосується оцінки доказів і процесу ухвалення рішень та не порушує вимог законодавства» [110]. Такий підхід відображає сучасну правову модель взаємодії судочинства і ІІІ, відповідно до якої носієм функції правосуддя може бути виключно людина, тоді як ІІІ розглядається лише як допоміжний технологічний інструмент, використання якого повинно здійснюватися під повним людським контролем та відповідно до вимог законодавства.

Безумовно, ІІІ може бути корисним для покращення доступу до правосуддя, зокрема шляхом надання первинних довідково-інформаційних послуг та виконання окремих допоміжних адміністративних функцій. Так, віртуальні помічники, чат-боти та онлайн-платформи здатні надавати користувачам інформацію щодо порядку й умов звернення до суду, особливостей підсудності справ, переліку необхідних документів, а також допомагати у зборі та систематизації публічно доступної інформації. За умови належної міжвідомчої цифрової інтеграції такі системи потенційно можуть сприяти й оперативному отриманню окремих офіційних відомостей, необхідних для здійснення судочинства [38].

Здатність алгоритмів ІІІ обробляти значні масиви даних, виявляти закономірності, здійснювати аналітичне співставлення інформації та формувати відповідні моделі створює потенційні можливості для їх використання під час підготовки проєктів процесуальних документів, у тому числі проєктів судових рішень. Однак у такому випадку йдеться виключно про допоміжні інформаційно-аналітичні заготовки, а не про самостійне формування юридично значущих актів, ухвалення яких потребує людської оцінки, внутрішнього переконання судді та інтерпретації правових норм.

Не виключається також використання спеціалізованих систем ІІІ для автоматизованої перевірки окремих фактичних обставин справи, співставлення дат, часу, геолокаційних даних, погодних умов, логіки послідовності подій чи узгодженості показань із наявними доказами. Проте навіть у такому разі результати діяльності подібних систем можуть мати виключно рекомендаційний та допоміжний характер, звертаючи увагу судді на потенційні неузгодженості, суперечності або розбіжності, але не підміняючи його дискреційні повноваження у процесі оцінки доказів.

Уже сьогодні застосування ІІІ у сфері правосуддя пов'язане з низкою ризиків, на які звертають увагу дослідники, що критично осмислюють можливості та межі алгоритмізації судочинства. При цьому подальший розвиток і ускладнення інтелектуальних систем можуть лише посилити

відповідні загрози у майбутньому.

Одним із ключових ризиків використання ШІ у сфері правосуддя є проблема алгоритмічної упередженості та дискримінації [36, с. 459]. Парадоксально, однак саме здатність ШІ обробляти значні масиви інформації, здійснювати їх систематизацію та кластеризацію потенційно може призводити до відтворення дискримінаційних моделей щодо окремих соціальних груп. Наслідком цього можуть ставати упереджені результати, поглиблення існуючої соціальної нерівності та відтворення дискримінаційних практик у системі правосуддя.

А. Шрілата та Г. Чоудхарі зазначають: «Упередження може проявлятися в різних проявах, включаючи расову упередженість, гендерну упередженість, соціально-економічну упередженість або упередженість, що корениться в інших юридично захищених ознаках. Наприклад, якщо історичні дані, що використовуються для навчання системи штучного інтелекту, відображають системні упередження або дискримінаційну практику, система штучного інтелекту може ненавмисно підтримувати ці упередження під час прийняття рішень» [486].

Таким чином, ризики використання ШІ значною мірою зумовлені статистичною природою алгоритмічних моделей, які здатні відтворювати та масштабувати наявні соціальні перекося й дискримінаційні практики [403]. Саме тому проблема алгоритмічної упередженості набуває особливого значення у сфері правосуддя, де однією з базових засад є вимога неупередженості та рівності всіх перед законом і судом.

Оскільки функціонування систем ШІ у сфері правосуддя через складність алгоритмічних процесів фактично залишається для пересічного користувача, а нерідко й для самих працівників правничої системи, своєрідною «чорною скринькою», виникають суттєві проблеми з розумінням та інтерпретацією механізмів формування алгоритмічних висновків. Відсутність прозорості процесу прийняття рішень, неможливість простежити логіку оцінки даних та брак людського елементу у здійсненні правосуддя потенційно здатні

породжувати недовіру до таких систем, а також сумніви щодо дотримання принципів належної правової процедури та справедливого суду. За таких умов особа, не розуміючи механізму формування відповідного рішення чи рекомендації, фактично позбавляється можливості повноцінно оцінити його обґрунтованість та справедливість.

Особливе місце серед ризиків використання ШІ у сфері правосуддя посідають етичні проблеми алгоритмізації судочинства. У цьому контексті особливого значення набуває проблема пошуку балансу між технологічною ефективністю та людяністю судочинства. Попри те, що алгоритмізація процесу прийняття рішень теоретично може зменшувати вплив емоційного чинника та окремих проявів людської упередженості, надмірна технологізація правосуддя водночас здатна створювати загрози для таких фундаментальних засад судочинства, як справедливість, гуманізм, індивідуалізація підходу та морально-ціннісна оцінка обставин справи.

Крім того, функціонування систем ШІ, пов'язаних з обробкою значних масивів інформації, потенційно пов'язане з ризиками витоку даних, у тому числі персональних. Для сфери правосуддя ця проблема набуває особливої чутливості, оскільки судочинство безпосередньо пов'язане з обробкою великого обсягу персональних даних не лише обвинувачених чи підсудних, а й свідків, потерпілих, третіх осіб та інших учасників процесу. У відповідних інформаційних масивах можуть міститися конфіденційні відомості, інформація з обмеженим доступом або навіть дані, що становлять охоронювану законом таємницю. За таких умов функціонування систем ШІ об'єктивно пов'язане з ризиком несанкціонованого доступу, витоку, неправомірного накопичення чи використання інформації, яку відповідні системи збирають, обробляють та зберігають

Наведений перелік ризиків не є вичерпним, а подальший розвиток і практичне застосування систем ШІ у сфері правосуддя можуть виявити й інші, менш очевидні на сучасному етапі загрози. Саме на запобігання таким ризикам має бути спрямоване міжнародне та національне правове регулювання

використання ІІІ, однак без ігнорування тих технологічних можливостей, які здатні сприяти підвищенню ефективності та якості здійснення правосуддя.

Отже, інтеграція ІІІ у систему правосуддя відкриває значні перспективи для підвищення ефективності, доступності та якості судочинства. Водночас допустимість використання ІІІ у цій сфері можлива лише за умови належного врахування основних ризиків, обмеження його застосування у найбільш чутливих аспектах здійснення правосуддя та збереження визначальної ролі людини у процесі ухвалення юридично значущих рішень. За таких умов ІІІ може розглядатися як допоміжний технологічний інструмент, а не як автономний суб'єкт здійснення правосуддя.

Саме на забезпечення такого підходу спрямовані п'ять принципів використання штучного інтелекту у судовій системі, закріплені в Етичній хартії Ради Європи щодо використання штучного інтелекту в судових системах та їхньому середовищі 2018 р. [332] (далі – CEPEJ Ethical Charter):

- принцип поваги до основних прав людини під час використання ІІІ;
- принцип недискримінації, спрямований на запобігання будь-яким формам дискримінації між окремими особами чи групами осіб;
- принцип якості та безпеки, що передбачає обробку судових рішень і даних у надійному та безпечному технологічному середовищі;
- принцип прозорості, неупередженості та справедливості;
- принцип «під контролем користувача» (under user control) [428].

Принцип поваги до основних прав людини під час використання ІІІ передбачає необхідність забезпечення сумісності процесів розробки, впровадження та застосування інтелектуальних систем із фундаментальними правами і свободами людини.

Відповідно до цього принципу обробка судових рішень і даних повинна здійснюватися виключно для чітко визначених правомірних цілей та у повній відповідності до основних прав [346], гарантованих Європейською конвенцією про захист прав людини і основоположних свобод, а також Конвенцією про захист осіб у зв'язку з автоматизованою обробкою персональних даних [331].

У межах зазначеного принципу особливого значення набуває забезпечення рівності сторін та змагальності судового процесу. Як підкреслюється у CEPEJ Ethical Charter, «коли інструменти штучного інтелекту використовуються для вирішення спору або як інструмент для допомоги в ухваленні судових рішень чи надання вказівок громадськості, важливо переконатися, що вони не підривають гарантії права на доступ до судді та право на справедливий суд» [298].

CEPEJ Ethical Charter передбачає, що у разі використання інструментів ШІ для вирішення спорів, як засобу допомоги в ухваленні судових рішень або для надання вказівок громадськості, вкрай важливо забезпечити, щоб такі системи не підривали гарантії права на доступ до судді та права на справедливий суд, зокрема принципи рівності сторін і змагальності судового процесу (абз. 1 Principle of respect for fundamental rights).

Також документ акцентує на необхідності використання ШІ з належною повагою до принципів верховенства права та незалежності суддів у процесі ухвалення рішень (абз. 3 Principle of respect for fundamental rights). У зв'язку з цим пріоритет повинен надаватися підходам, заснованим на дотриманні етичних стандартів та фундаментальних прав людини. Зокрема, ще на етапах проєктування, навчання та функціонального налаштування інтелектуальних систем до їхньої архітектури мають інтегруватися обмеження, спрямовані на недопущення прямих або опосередкованих порушень фундаментальних цінностей, гарантованих міжнародно-правовими актами у сфері захисту прав людини.

Виходячи зі змісту CEPEJ Ethical Charter [332], принцип поваги до основних прав людини під час використання ШІ передбачає необхідність первинного інтегрування вимог щодо дотримання фундаментальних прав і свобод людини безпосередньо в архітектуру та алгоритмічну логіку інтелектуальних систем, які розробляються для використання у сфері правосуддя. Аналогічним чином уже на етапах проєктування та навчання таких систем повинні закладатися механізми забезпечення захисту персональних

даних, конфіденційної інформації та інших відомостей з обмеженим доступом.

Принцип недискримінації зобов'язує запобігати розвитку чи посиленню будь-яких форм дискримінації щодо окремих осіб або соціальних груп під час використання ІІІ у сфері правосуддя. CEPEJ Ethical Charter виходить із того, що системи ІІІ в процесі обробки значних масивів інформації здатні виявляти та відтворювати вже існуючі закономірності, у тому числі такі, що містять дискримінаційні практики або соціальні перекося. Саме тому на суб'єктів, зацікавлених у впровадженні інтелектуальних систем, покладається обов'язок гарантувати, що відповідні алгоритмічні моделі не відтворюватимуть і не посилюватимуть дискримінацію та не призводитимуть до детерміністичного підходу під час аналізу конкретної справи (абз. 1 Principle of non-discrimination).

CEPEJ Ethical Charter також акцентує увагу на тому, що принцип недискримінації повинен забезпечуватися як на етапі розробки інтелектуальних систем, так і під час їх практичного впровадження та функціонування, особливо у випадках, коли обробка інформації прямо чи опосередковано пов'язана з так званими «чутливими» даними. У зв'язку з цим інтелектуальні системи мають бути побудовані таким чином, щоб виключати дискримінаційні підходи, пов'язані з расовим чи етнічним походженням, соціально-економічним становищем, політичними поглядами, релігійними або філософськими переконаннями, членством у професійних спілках, генетичними та біометричними даними, станом здоров'я, сексуальним життям чи сексуальною орієнтацією особи (абз. 2 Principle of non-discrimination).

Документ також передбачає, що у разі виявлення подібних дискримінаційних ризиків повинні застосовуватися заходи щодо їх мінімізації або, за можливості, нейтралізації, а також здійснюватися належне інформування й підвищення обізнаності зацікавлених суб'єктів. Водночас CEPEJ Ethical Charter підтримує використання методів машинного навчання та міждисциплінарного наукового аналізу з метою виявлення й подолання дискримінаційних практик.

Таким чином, CEPEJ Ethical Charter не допускає перенесення

дискримінаційних алгоритмічних моделей або систематизованих упереджених даних у процес здійснення правосуддя. Водночас документ не заперечує можливості використання узагальнених даних, отриманих у процесі судової діяльності, для кримінологічних досліджень, вивчення закономірностей злочинності та моделювання детермінаційних зв'язків у межах наукового аналізу, у тому числі щодо окремих соціальних груп.

Принцип якості та безпеки, закріплений у CEPEJ Ethical Charter, передбачає необхідність використання під час обробки судових рішень і даних перевірених джерел інформації та надійних моделей, розроблених на міждисциплінарній основі у безпечному технологічному середовищі (Принцип 3. Principle of quality and security). Фактично йдеться про практичну реалізацію принципів прозорості, неупередженості та справедливості під час використання ІІІ у сфері правосуддя.

CEPEJ Ethical Charter підкреслює, що у випадках застосування інструментів ІІІ, здатних породжувати юридичні наслідки або суттєво впливати на життя людини, відповідні гарантії повинні поширюватися на весь цикл функціонування інтелектуальної системи – від етапу проєктування та відбору даних до навчання, тестування, впровадження й практичної експлуатації. Особливого значення при цьому набувають якість, репрезентативність та організація інформаційних масивів, оскільки саме вони безпосередньо впливають на процес навчання алгоритмічних моделей і, відповідно, на результати їх функціонування.

У цьому форматі принцип поваги до прав людини під час використання ІІІ вимагає не лише формального посилання на положення Європейської конвенції про захист прав людини і основоположних свобод [331], а й первинного інтегрування відповідних правових приписів у саму архітектуру інтелектуальних систем. Ідеться про те, що алгоритмічні моделі, призначені для функціонування у сфері правосуддя, мають із самого початку проєктуватися таким чином, щоб унеможливлювати прямі чи опосередковані порушення фундаментальних прав людини, а також містити вбудовані механізми захисту

персональних даних і конфіденційної інформації.

У цьому аспекті особливого значення набуває проблема прозорості алгоритмічних систем та можливості їх зовнішнього аудиту. Як зазначається у відповідних дослідженнях, «надання цілих алгоритмів або основного програмного коду громадськості є мало ймовірним рішенням у цьому контексті, оскільки приватні компанії розглядають свій алгоритм як ключове пропрієтарне програмне забезпечення, яке захищено. Однак може існувати можливість вимагати, щоб ключові підмножини інформації про алгоритми були надані громадськості, наприклад, які змінні використовуються, для яких цілей алгоритми оптимізовані, навчальні дані та середні значення та стандартні відхилення отриманих результатів або кількість і тип даних, які обробляються алгоритмом».

Подібні підходи простежуються і у звіті С. Віллані «AI for Humanity», де звертається увага на необхідність проведення незалежного аудиту інтелектуальних систем. Зокрема, зазначається, що аудитори можуть перевіряти чесність і недискримінаційність функціонування програм шляхом моделювання різних типів вхідних даних та створення множинних профілів користувачів відповідно до спеціально визначених критеріїв. Аналогічні підходи щодо забезпечення прозорості та підзвітності інтелектуальних систем відображені також у звіті Палати лордів Сполученого Королівства «AI in the UK: ready, willing and able?» (§§ 92–99) [391].

У зазначеній доповіді Палати лордів серед ключових засобів наближення алгоритмічних систем до вимог нейтральності та недискримінаційності називається використання більш різноманітних і репрезентативних масивів даних. Зокрема, акцентується увага на необхідності уникнення упереджених «тренувальних наборів даних» («training datasets») та забезпечення належної репрезентативності різних груп користувачів під час тестування систем ШІ на предмет виявлення можливих дискримінаційних ефектів (§§ 93–95 звіту).

Водночас міждисциплінарний підхід до розробки інтелектуальних систем, а також посилений аудит процедур обробки даних і самої архітектури

алгоритмічних моделей розглядаються як необхідні умови забезпечення прозорості, підзвітності та суспільної довіри до алгоритмічних рішень (§§ 96–99 звіту).

Центральне значення для забезпечення людського контролю над алгоритмізацією судочинства у CEPEJ Ethical Charter має Принцип 5 – «Під контролем користувача» («Principle ‘under user control’») [332]. У його основі лежить підхід, відповідно до якого використання інструментів ШІ у сфері правосуддя повинно розширювати можливості автономного й усвідомленого прийняття рішень людиною, а не перетворювати користувача на пасивного виконавця алгоритмічних приписів. Саме тому професійні учасники системи правосуддя повинні зберігати можливість у будь-який момент перевірити дані та логіку міркувань, покладених в основу алгоритмічного висновку, співвіднести їх з обставинами конкретної справи та, за необхідності, відмовитися від використання такого висновку, не сприймаючи його як автоматично обов’язковий (абз. 2 Principle ‘under user control’) [332].

Для сторін судового процесу принципово важливим є забезпечення прозорості та зрозумілої комунікації щодо характеру і ролі ШІ у відповідному провадженні. Особі має бути чітко роз’яснено, чи мають рекомендації інтелектуальної системи виключно допоміжний характер, які альтернативні процесуальні можливості існують, а також гарантовано право на юридичну допомогу й безпосередній доступ до суду у розумінні статті 6 ЄКПЛ. Крім того, особа повинна бути поінформована про факт попередньої алгоритмічної обробки її справи та мати процесуальну можливість заперечити проти такого підходу, наполягаючи на безпосередньому розгляді справи людиною-суддею (абз. 3 Principle ‘under user control’) [332].

У ширшому вимірі впровадження інформаційних систем на базі ШІ у сферу правосуддя потребує розвитку програм цифрової грамотності для суддів, адвокатів, прокурорів та інших учасників процесу, а також формування постійного професійного міждисциплінарного діалогу щодо меж і наслідків алгоритмізації судочинства [503]. Лише за умови належної обізнаності та

критичної компетентності користувачів можливо уникнути ситуації, за якої технологія фактично підмінятиме суддівський розсуд, зберігаючи при цьому лише зовнішні ознаки формальної законності.

Керуючись зазначеними принципами, держави, розробники інтелектуальних систем та суб'єкти нормотворчої діяльності повинні співпрацювати над формуванням надійних правових механізмів і рамок обмежень використання ШІ у сфері правосуддя, спрямованих на мінімізацію відповідних ризиків. Такі обмеження мають забезпечувати реалізацію принципів, закріплених у CEPEJ Ethical Charter, з урахуванням європейського розуміння верховенства права та права людини на справедливий суд.

Практика ЄСПЛ щодо застосування статті 6 Конвенції у справах, де на процес ухвалення рішень прямо чи опосередковано впливають алгоритмічні системи, фактично формує змістовні межі допустимого використання ШІ у сфері правосуддя. ЄСПЛ послідовно виходить із того, що право на справедливий суд охоплює не лише формальне існування «суду, встановленого законом», а й право особи на зрозуміле, мотивоване та таке, що підлягає ефективному оскарженню і публічному контролю, судові рішення. Саме тому подібні стандарти вкрай складно узгоджуються з використанням непрозорих алгоритмічних моделей типу з закритою логікою функціонування, зокрема у питаннях оцінки доказів, прогнозування поведінки чи призначення покарання [447].

У подальшій правовій доктрині, присвяченій проблематиці алгоритмізації правосуддя, положення, сформульовані ЄСПЛ у справі «Руїс Торіха проти Іспанії» (*Ruiz Torija v. Spain*) [316], набули нового осмислення в контексті використання непрозорих алгоритмічних систем під час постановлення вироків або визначення міри покарання. Акцентується увага на тому, що застосування таких систем потенційно здатне порушувати одразу декілька складових права на справедливий суд, гарантованого статтею 6 ЄКПЛ. Йдеться, зокрема, про право бути вислуханим, право на мотивоване судові рішення та принцип «рівності озброєнь» між стороною обвинувачення і стороною захисту. Якщо ані

суд, ані учасники процесу не можуть зрозуміло пояснити механізм формування алгоритмічного висновку щодо ризику рецидиву, рівня небезпечності особи чи запропонованої санкції, це ставить під сумнів вимоги передбачуваності, контрольованості та перевірюваності правозастосування [293].

АСМ Code of Ethics, хоча й адресований насамперед розробникам та фахівцям у сфері інформаційних технологій, формує важливі етичні орієнтири, що безпосередньо кореспондують із сучасними підходами до обмеження використання ШІ у сфері правосуддя. Кодекс вимагає мінімізувати потенційну шкоду, забезпечувати справедливість і недискримінаційність алгоритмічних систем, уникати проєктування моделей, здатних відтворювати або посилювати упередженість, а також гарантувати підзвітність і пояснюваність алгоритмічних рішень, особливо у випадках, коли вони можуть істотно впливати на права та свободи людини.

У контексті ШІ у сфері права це означає, що системи, здатні впливати на судові рішення, оцінку особи чи прогнозування її поведінки, повинні проєктуватися таким чином, щоб їхні висновки могли бути зрозумілими, пояснюваними та придатними для оскарження. За таких умов алгоритмічна система не може функціонувати як непояснювана модель, висновки якої формально мають рекомендаційний характер, але фактично визначають зміст судового рішення [495].

Подібні підходи до забезпечення прозорості, підзвітності та недискримінаційності алгоритмічних систем простежуються і в діяльності національних регуляторних органів держав Європейського Союзу. Зокрема, важливе значення у цьому контексті мають рекомендації французької Національної комісії з інформатики та свобод – Commission Nationale de l'Informatique et des Libertés (CNIL) – щодо використання ШІ у судових системах [329] (далі – рекомендації CNIL).

Рекомендації CNIL зосереджені насамперед на питаннях захисту персональних даних та мінімізації дискримінаційних ефектів, що безпосередньо кореспондує з обмеженнями AI Act щодо високоризикових систем у сфері

правосуддя. Так само, як в інших проаналізованих документах, CNIL наголошує на необхідності проведення обов'язкової оцінки впливу на захист даних у випадках використання судових систем ШІ, особливо коли обробляються чутливі категорії інформації, пов'язані з расовим чи етнічним походженням, станом здоров'я, політичними поглядами або іншими sensitive data. Крім того, передбачається необхідність регулярного аудиту алгоритмічної упередженості, перевірки якості даних та контролю інформаційних масивів, на яких здійснюється навчання відповідних моделей.

Аналізуючи зазначені рекомендації, науковці та практики підкреслюють, що підходи CNIL фактично конкретизують положення AI Act щодо управління даними, оцінки ризиків та запобігання алгоритмічній дискримінації у сфері правосуддя. Водночас AI Act і рекомендації CNIL збігаються у принциповому підході, відповідно до якого судові алгоритмічні системи не можуть вважатися легітимними без попередньої оцінки ризиків для прав людини, контролю за використанням sensitive data та наявності процедурних механізмів виявлення, перевірки й усунення алгоритмічної упередженості. За таких умов обмеження, закріплені в AI Act, фактично формують наднаціональний нормативний каркас для розвитку національних моделей регулювання використання ШІ у сфері правосуддя, у тому числі таких, як французькі рекомендації CNIL [354].

Подібну логіку обмежень демонструють і Принципи Міністерства юстиції США щодо використання ШІ у системі кримінального правосуддя [330], зокрема у контексті рішень і дій, заснованих на прогнозуванні ризиків, подібних до практик, пов'язаних із використанням COMPAS [515]. Хоча зазначений документ функціонує поза межами правового поля Європейського Союзу, його підходи концептуально збігаються з європейськими моделями регулювання алгоритмічних систем.

Зокрема, документ забороняє покладатися виключно на автоматизовані системи під час ухвалення рішень, здатних впливати на свободу особи, зокрема щодо обрання запобіжного заходу чи умовно-дострокового звільнення (Розділ V). Одночасно наголошується на необхідності збереження людського розсуду,

проведення регулярної перевірки алгоритмічних моделей на предмет расової та соціальної упередженості, а також забезпечення прозорості критеріїв, що використовуються для оцінки ризиків (Розділ VI).

Такий підхід концептуально кореспондує з моделлю AI Act, відповідно до якої подібні системи класифікуються як високоризикові, а практика «виключно автоматизованого прийняття рішень» («sole decision-making») без змістовного людського контролю розглядається як неприйнятна для сфери правосуддя. Таким чином, навіть поза межами юрисдикції AI Act сучасні американські підходи підтверджують універсальність базової ідеї: алгоритмічні інструменти у кримінальному правосудді можуть використовуватися виключно як допоміжні [378], підзвітні та прозорі системи, але не як самодостатні «судді-алгоритми», здатні самостійно визначати юридичну долю людини.

AI Act щодо використання ШІ у сфері правосуддя виходить із презумпції неприпустимості повної автономізації процесу ухвалення юридично значущих рішень та необхідності жорсткого обмеження найбільш ризикованих алгоритмічних практик. Як уже зазначалося, AI Act прямо забороняє системи ШІ, які шляхом застосування маніпулятивних технік або використання вразливості людини здатні суттєво викривлювати її поведінку. У контексті правосуддя це означає недопустимість використання алгоритмічних систем, призначених для впливу на волевиявлення сторін процесу, свідків чи суддів, зокрема через спеціальний добір інформації, інтерфейсні рішення або інші механізми психологічного впливу.

Особливим об'єктом обмежень у межах AI Act виступають біометричні та суміжні системи, здатні опосередковано впливати на результати здійснення правосуддя. Зокрема, AI Act забороняє практики соціального скорингу – оцінювання осіб на підставі їхньої поведінки, соціального статусу або особистісних характеристик, а також біометричну категоризацію за чутливими ознаками, пов'язаними з расою, етнічним походженням, політичними поглядами, релігійними переконаннями чи сексуальною орієнтацією. Подібні обмеження фактично унеможливають імплементацію у сферу правосуддя

моделей, побудованих за логікою «рейтингів довіри», прогнозування соціальної небезпечності або формування «ризикових профілів» підсудних.

Водночас AI Act не встановлює повної заборони використання систем III у сфері правосуддя, однак відносить відповідні системи до категорії високоризикових із комплексом спеціальних обмежень і обов'язкових вимог (п. 8 Додаток III AI Act). Зокрема, системи, що застосовуються для оцінювання ризиків, прогнозування рецидиву, формування рекомендацій щодо міри покарання або аналізу доказів, допускаються лише за умови функціонування повноцінної системи управління ризиками, забезпечення належної якості та репрезентативності даних, запобігання алгоритмічній упередженості, а також документування логіки функціонування відповідних моделей.

Ключовим нормативним обмеженням у межах AI Act виступає вимога забезпечення осмисленого людського контролю над високоризиковими системами III. Регламент виходить із того, що жодне рішення, здатне породжувати юридично значущі наслідки для особи, не може ґрунтуватися виключно на автоматизованій обробці даних без можливості для людини втрутитися у процес ухвалення рішення, перевірити підстави алгоритмічного висновку та змінити або відхилити його. Фактично це означає нормативне заперечення моделей, у межах яких людина усувається з контуру управління («human out of the loop»), та закріплення підходу, відповідно до якого III у сфері правосуддя може виконувати виключно допоміжну функцію.

У цьому контексті слушно зазначається, що «алгоритмічна упередженість виникає тоді, коли системи, навчені на історичних даних, що відображають соціальну нерівність, відтворюють і підсилюють дискримінацію щодо маргіналізованих груп» [328]. За таких умов навіть формальний людський нагляд, який не супроводжується критичним аналізом джерел даних, принципів їх відбору та логіки функціонування алгоритмічної моделі, не здатний повною мірою нейтралізувати структурну несправедливість.

Таким чином, алгоритмічна упередженість становить безпосередню загрозу праву на справедливий суд, оскільки здатна породжувати

дискримінаційні результати, підривати вимогу неупередженості суду та знижувати рівень довіри до судових процедур. Наприклад, якщо модель оцінки ризику рецидиву або інший інструмент прогнозування ґрунтується на історичних даних правоохоронних органів і судової практики, вона потенційно здатна відтворювати вже існуючі структурні перекоси та дискримінаційні патерни, подаючи їх при цьому як «нейтральну» статистичну закономірність. Саме тому теза про те, що «людина й алгоритм однаково упереджені», не враховує принципової особливості алгоритмічних систем: «алгоритм масштабує упередженість – помилки моделі стають масовими, послідовними і менш помітними для процесуального контролю» [341].

Крім того, проблема через незрозумілі алгоритми (проблема «чорної скринки») полягає в тому, що такі алгоритми роблять процес ухвалення рішень незбагненим для користувачів, що унеможливлює ефективне оскарження відповідно до принципу рівності сторін за ст. 6 ЄКПЛ. На практиці це означає, що у разі коли результати, згенеровані AI, фактично визначають хід провадження, але залишаються недоступними для розуміння і перевірки, це підриває як принцип змагальності, так і гарантії справедливого суду у сенсі ст. 6 ЄКПЛ. Типовим прикладом є «алгоритм візового скринінгу Міністерства внутрішніх справ Великої Британії», який «сортував заяви за національністю, системно маркуючи заявників із «ісокоризикових» країн, що на практиці означало расизовану сегрегацію доступу до міграційних процедур» [483] – саме такі практики демонструють, до чого призводить поєднання непрозорості, автоматизації та відсутності ефективних засобів оскарження.

Крім того, серйозну проблему становить використання алгоритмічних моделей із закритою логікою функціонування. У подібних системах процес формування висновків залишається фактично незрозумілим для користувачів, що істотно ускладнює або навіть унеможливлює ефективне оскарження відповідних результатів у контексті принципу рівності сторін, гарантованого статтею 6 ЄКПЛ.

На практиці це означає, що у випадках, коли результати, сформовані

системою ШІ, фактично впливають на перебіг провадження, але залишаються недоступними для розуміння, перевірки чи критичного аналізу, під загрозою опиняються як принцип змагальності, так і гарантії справедливого суду у розумінні статті 6 ЄКПЛ.

Показовим прикладом у цьому контексті є алгоритм візового скринінгу Міністерства внутрішніх справ Великої Британії, який «сортував заяви за національністю, системно маркуючи заявників із “високоризикових” країн, що на практиці означало расизовану сегрегацію доступу до міграційних процедур» [483]. Подібні практики наочно демонструють ризики, що виникають у результаті поєднання алгоритмічної непрозорості, автоматизації процедур та відсутності ефективних механізмів оскарження.

З огляду на це використання непрозорих алгоритмічних моделей здатне перетворювати право на мотивоване рішення на суто формальну гарантію, оскільки сторони отримують лише кінцевий результат, не маючи можливості зрозуміти, які саме дані, критерії та логіка були покладені в основу відповідного висновку. У межах змагального процесу невідоме джерело даних, закрита модель функціонування та непрозорість вагових коефіцієнтів алгоритму фактично унеможливають повноцінне спростування або критичне оскарження відповідної позиції, що підриває принцип рівності сторін.

У результаті замість посилення гарантій, передбачених статтею 6 ЄКПЛ, непрозора алгоритмічна оцінка ризику, доказів чи правової позиції може підміняти публічно контрольоване судове міркування прихованою технічною оптимізацією моделі, яка не піддається належній перевірці та процесуальному контролю.

У відповідь на зазначені ризики сучасна правова доктрина наполягає на тому, що «судові системи АІ можуть вважатися прийнятними лише за умови, що їхня роль у прийнятті рішень є прозорою, а результати – пояснюваними в обсязі, необхідному для оскарження та публічного контролю» [489]. Аналогічно підкреслюється, що «алгоритмічні інструменти в суді мають оцінюватися крізь призму ст. 6 ЄКПЛ: чи зберігається право бути вислуханим,

отримати мотивоване рішення та доступ до ефективного засобу правового захисту» [489].

Особливого значення ці вимоги набувають щодо онлайн-механізмів вирішення спорів та систем ШІ, які здатні пропонувати сторонам готові варіанти врегулювання конфлікту або фактично спрямовувати їх до певного результату спору. Подібні системи не можуть позбавляти особу права на звернення до суду та вимоги повноцінного людського перегляду справи. Саме тому для забезпечення відповідності статті 6 ЄКПЛ алгоритмічні механізми онлайн-вирішення спорів повинні гарантувати добровільність прийняття запропонованих рішень, збереження доступу до суду та можливість повноцінного перегляду справи людиною-суддею.

Як підкреслюється в сучасних дослідженнях, «право на справедливий суд вимагає, щоб сторони мали доступ не лише до результату алгоритмічної оцінки, а й до інформації про її основу – релевантні фактори, ваги й обмеження моделі – в обсязі, достатньому для процесуального заперечення», а «недостатня пояснюваність алгоритмічних інструментів підриває «рівність озброєнь», оскільки одна зі сторін може користуватися технологічною перевагою, яку інша не здатна ні зрозуміти, ні ефективно оскаржити» [287].

Подібні підходи безпосередньо підсилюють висновок про те, що «для відповідності стандартам справедливого суду жодна особа не повинна зазнавати істотних юридичних наслідків виключно на підставі автоматизованого рішення без змістовного людського контролю. Саме тому сучасна правова доктрина виходить із концепції «людини-судді у контурі прийняття рішень», відповідно до якої ШІ повинен виступати допоміжним інструментом судді, підсилюючи можливості аналізу доказів, систематизації інформації та забезпечення послідовності судової практики, але не замінюючи людську інтерпретацію, дискрецію та оцінку обставин конкретної справи. У цьому контексті цілком слушно зазначається, що «навіть найрозвинутіші системи ШІ можуть лише доповнювати судову діяльність; вони не здатні взяти на себе нормативну відповідальність за балансування цінностей та етичне

зважування, яке є серцевиною справедливого суду» [473].

У цьому сенсі сама концепція повністю автоматизованого «цифрового судді» суперечить базовим компонентам права на справедливий суд, зокрема праву бути вислуханим людиною, вимозі мотивованого судового рішення та можливості його ефективного оскарження, зорієнтованого саме на людський судовий розсуд. Не випадково у сучасних дослідженнях підкреслюється, що «якщо учасники процесу сприймають алгоритм як фактичного вирішувача спору, а суддю – лише як формального підписанта, це руйнує легітимність правосуддя та довіру до судової системи навіть за формального збереження людської «присутності у рішенні».

Для збереження суспільної довіри до правосуддя недостатньо лише технічної точності алгоритмічної системи. Необхідно, щоб учасники процесу могли розуміти, яку саме роль ШІ відігравав під час формування відповідного рішення, а також мали гарантії того, що остаточне рішення ухвалюється людиною-суддею.

Узгоджено з цим концепція збереження судді-людини у контурі управління («human judge in the loop»), що у CEPEJ Ethical Charter відповідає принципу «під контролем користувача» («under user control»), виходить із того, що ШІ може використовуватися лише як допоміжний інструмент судового аналізу, але не як заміна людського судового розсуду та відповідальності за остаточне рішення. У цьому контексті цілком обґрунтовано підкреслюється, що «суддя не повинен перетворюватися на пасивного ратифікатора алгоритмічних висновків», а збереження автономного судового міркування (пп. 25, 55–58, 60 CEPEJ) виступає ключовою умовою легітимності правосуддя [332].

Таким чином, CEPEJ Ethical Charter ще з 2018 р. не лише проголошує загальні етичні орієнтири, а фактично формує нормативний каркас для розробки та впровадження судових систем ШІ, у межах якого принципи поваги до прав людини, недискримінації, якості, прозорості та «підконтрольності користувачу» повинні інтегруватися вже на етапі проєктування інтелектуальних систем. При цьому, як підкреслюється у сучасних

дослідженнях, «практика імплементації показує, що найскладнішим є перетворення принципу “під контролем користувача” на реальні процедурні гарантії: судді мають зберігати можливість відхиляти алгоритмічні рекомендації й пояснювати, чому людський розсуд у конкретній справі відрізняється від пропозиції системи» [280].

На цьому тлі AI Act становить спробу юридичної конкретизації та нормативної матеріалізації зазначених етичних орієнтирів, зокрема через віднесення судових систем ШІ до категорії високоризикових. Такий підхід означає покладення на держави та розробників інтелектуальних систем обов’язку забезпечувати належну якість, репрезентативність та актуальність даних, на яких здійснюється навчання алгоритмічних моделей. Не випадково у сучасній доктрині наголошується, що «без механізмів очищення даних від історичної дискримінації і регулярних аудитів упередженості будь-які гарантії «недискримінаційності» алгоритмічних систем залишаються декларативними» (ст. 10 AI Act) [472].

Так само, як і інші проаналізовані міжнародні акти та рекомендації, AI Act виходить із необхідності проведення попередньої оцінки впливу судових систем ШІ на права людини та захист персональних даних ще до початку їх практичного використання [347], а не лише реагування на можливі порушення вже після їх виникнення.

Таким чином, п’ять принципів CEPEJ Ethical Charter – повага до прав людини, недискримінація, якість і безпека, прозорість та справедливість, а також «підконтрольність користувачу» – формують мінімальний етичний стандарт допустимого використання ШІ у сфері правосуддя. Водночас AI Act фактично здійснює юридичну імплементацію зазначених принципів через віднесення судових систем ШІ до категорії високоризикових, встановлюючи обов’язкові вимоги щодо логування, пояснюваності алгоритмічних рішень, оцінки ризиків та забезпечення змістовного людського контролю. У цьому сенсі саме з ухваленням AI Act у 2024 р. принципи, закладені в CEPEJ Ethical Charter ще у 2018 р., починають переходити зі сфери м’якого права (soft law) у

площину обов'язкових регуляторних стандартів.

Зазначені підходи знаходять відображення і в позиції Генерального секретаря ООН, який у 2024 р. наголошував, що використання ШІ у сфері правосуддя повинно не замінювати, а зміцнювати верховенство права, а будь-яке впровадження інтелектуальних систем має «посилювати, а не підривати» право на справедливий суд. Практика держав – членів Ради Європи також свідчить про те, що найбільш ефективними виявляються ті проекти використання ШІ у судових системах, які обмежуються допоміжною технічною підтримкою, супроводжуються належною підготовкою суддів та відкритою комунікацією щодо потенційних ризиків, а не орієнтовані на створення повністю автоматизованих механізмів ухвалення рішень [347].

Отже, обмеження, встановлені AI Act щодо високоризикових систем ШІ, разом із вимогами прозорості, пояснюваності та підконтрольності користувачу логічно впливають із уже сформованих міжнародних стандартів у сфері захисту права на справедливий суд. Їхнє основне призначення полягає у недопущенні ситуації, за якої алгоритмічна упередженість, непрозорість моделей або системи з прихованою логікою функціонування підмінятимуть собою людський судовий розсуд під час ухвалення юридично значущих рішень [506].

Використання ШІ у сфері правосуддя демонструє виразний «подвійний ефект»: з одного боку, інтелектуальні системи здатні істотно підвищувати ефективність аналізу доказів, сприяти уніфікації підходів до подібних категорій справ та зменшувати рутинне навантаження на суддів, а з іншого – створюють нові, складно контрольовані ризики для реалізації права на справедливий суд. Такі ризики пов'язані не лише з можливими технічними помилками, а насамперед із непрозорістю алгоритмічних рішень, небезпекою відтворення структурної дискримінації, втручанням у приватність та потенційним витісненням людського судового розсуду алгоритмічними моделями, механізм функціонування яких є складним для пояснення, перевірки та ефективного оскарження.

За таких умов обмеження, встановлені щодо використання судових систем ІІІ, слід розглядати не як перешкоду технологічному розвитку, а як необхідний інструмент захисту фундаментальних гарантій права на справедливий суд та підтримання суспільної довіри до системи правосуддя.

Нормативна модель, закріплена у Регламенті (ЄС) 2024/1689, Європейській етичній хартії CEREJ, національних рекомендаціях, зокрема французьких настанов CNIL, а також принципах Міністерства юстиції США, свідчить про формування спільного міжнародного підходу, відповідно до якого використання ІІІ у сфері правосуддя повинно залишатися допоміжним, підзвітним та прозорим для людини.

Класифікація судових систем ІІІ як високоризикових, вимоги щодо якості, репрезентативності та недискримінаційності даних, обов'язкове проведення аудитів алгоритмічної упередженості, забезпечення людського нагляду та заборона виключно автоматизованого ухвалення юридично значущих рішень формують базове нормативне ядро обмежень, спрямованих на нейтралізацію найбільш небезпечних ризиків використання ІІІ у сфері правосуддя – від расової та соціальної дискримінації до втрати людиною реального контролю над алгоритмічними процесами.

У цьому сенсі відповідні обмеження є не випадковими регуляторними бар'єрами, а закономірним продовженням уже сформованих стандартів ЄСПЛ, Ради Європи та професійних етичних кодексів у сфері розробки й використання інтелектуальних систем.

З огляду на це перспективна модель використання ІІІ у сфері правосуддя передбачає не створення «цифрового судді», а функціонування розумно обмеженого технічного помічника, інтегрованого у процесуальні механізми та підпорядкованого принципам верховенства права, незалежності суду й поваги до людської гідності [481; 519]. Сутність чинних обмежень полягає у перенесенні акценту з безумовного технологічного ентузіазму на необхідність управління ризиками, що, своєю чергою, вимагає проєктування та використання судових систем ІІІ таким чином, щоб вони підсилювали, а не

підривали гарантії справедливого суду, прозорості та відповідальності.

Відмова від повністю автономних моделей ухвалення рішень, встановлення жорстких вимог до прозорості, пояснюваності та контролю, а також збереження пріоритету людського судового розсуду слід розглядати не як перешкоду технологічному розвитку, а як необхідну умову збереження людського змісту правосуддя в умовах поширення інтелектуальних технологій.

Ця теза набуває особливої ваги з огляду на сучасні тенденції до автоматизації окремих процесуальних рішень – від автоматизованого розподілу справ і визначення порядку їх розгляду до підготовки проєктів судових рішень та використання алгоритмічних систем для оцінки ризиків і небезпечності особи. Міжнародний досвід, зокрема практика застосування подібних систем у США, демонструє, що непрозорі алгоритмічні моделі здатні не лише відтворювати, а й посилювати системні упередження, порушуючи принципи рівності перед законом та недискримінації.

У європейських документах, присвячених використанню ШІ у сфері правосуддя, дедалі чіткіше простежується підхід, відповідно до якого алгоритмічні системи не можуть підміняти собою судові розсудження, а повинні залишатися виключно допоміжним інструментом підтримки судової діяльності.

З позицій верховенства права це означає, що будь-які системи ШІ, які застосовуються у судочинстві, повинні відповідати щонайменше трьом базовим вимогам:

1. такі системи мають бути достатньо пояснюваними у тій частині, в якій їх результати впливають на зміст судового рішення. Суддя повинен мати можливість зрозуміти логіку алгоритмічної рекомендації та оцінити її у співвідношенні з матеріалами конкретної справи, а не сприймати алгоритмічний висновок як модель із прихованою логікою функціонування;

2. повинна забезпечуватися реальна можливість оскарження рішень, у формуванні яких відігравали роль алгоритмічні інструменти. Сторони процесу мають отримувати доступ до інформації про характер такого впливу та

можливість ставити під сумнів як фактичні дані, так і правові висновки, сформовані із використанням ШІ;

3. застосування алгоритмічних систем у сфері правосуддя повинно бути чітко врегульоване законом, а не залишатися на рівні внутрішніх інструкцій судових органів або розробників програмного забезпечення.

Український контекст надає цій проблематиці додаткового виміру, пов'язаного з кризою суспільної довіри до судової системи.

О. Я. Ковальчук у своєму дисертаційному дослідженні пропонує визначення «цифровий судовий процес» як форми здійснення правосуддя, що передбачає використання інформаційно-комунікаційних технологій та електронних систем на всіх стадіях судового процесу, включаючи подання документів, проведення судових засідань, збір і аналіз доказів, ухвалення та оприлюднення судових рішень, з метою забезпечення ефективного, об'єктивного, прозорого та доступного правосуддя при дотриманні всіх процесуальних прав і гарантій учасників судового процесу [107, с. 457].

Незважаючи на значний потенціал ШІ для автоматизації окремих процесів, домінуючою залишається позиція, відповідно до якої алгоритми не можуть підміняти суддівський розсуд, оскільки здійснення правосуддя пов'язане з оцінкою доказів, тлумаченням норм права та забезпеченням принципів верховенства права і справедливості [272].

Показовою у цьому контексті є ухвала Київського апеляційного суду від 30 липня 2025 року у справі № 11-кп/824/1818/2025, якою було скасовано вирок суду першої інстанції через використання під час його підготовки текстів, згенерованих ChatGPT. Суд дійшов висновку, що включення до мотивувальної частини теоретичних положень, сформованих системою штучного інтелекту, ставить під сумнів самотійність суддівського розсуду та не відповідає вимогам кримінального процесуального законодавства. Таким чином, суд фактично підтвердив, що використання технологій штучного інтелекту не повинно підміняти інтелектуальну діяльність судді та впливати на незалежність здійснення правосуддя [257].

В ухвалі Касаційного господарського суду у складі Верховного Суду від 8 лютого 2024 року у справі № 925/200/22 вперше на рівні ВС безпосередньо оцінено використання ChatGPT у судовому процесі. Суд дійшов таких висновків: відповіді ChatGPT не є джерелом достовірної науково доведеної інформації; посилання на «позицію» ChatGPT не може спростовувати правові висновки, викладені у судовому рішенні; використання відповідей ChatGPT як аргументу проти остаточного судового рішення ставить під сумнів суддівський розсуд та авторитет судової влади; апелювання до згенерованих відповідей ІІІ у цій справі було оцінено як прояв неповаги до суду [258].

У постанові Верховного Суду від 8 липня 2025 року у справі № 925/496/24 сторона намагалася використати відповіді **ChatGPT** та **Grok** як докази для тлумачення умов договору. ВС відмовився враховувати такі матеріали та сформулював важливу правову позицію: відповіді генеративного ІІІ не відповідають вимогам належності, допустимості та достовірності доказів; ІІІ може використовуватися лише як допоміжний інформаційний інструмент; технології штучного інтелекту не можуть підміняти суддівський розсуд або процедуру доказування; використання ІІІ повинно бути спрямоване на підтримку верховенства права, а остаточні юридично значущі рішення має приймати виключно суддя [181].

І. В. Гловюк зауважує: «Визначення меж реагування судами на недоліки процесуальних документів, ідентифіковані як випадки невідповідального використання ІІІ потребує урахування таких аспектів: чи мало місце повідомлення про використання ІІІ (що не є обов'язковим та і взагалі передбаченим станом на день підготовки статті); урахуванням можливостей галюцинацій ІІІ у тому числі у контексті викривленого змісту нормативних актів, судової практики, та вигадкування норм права та судової практики; обережності констатації неналежного виконання професійних обов'язків правником та неповаги до суду чи зловживанням у процесі через ризики стигматизації правника неправильною ідентифікацією використання ІІІ» [56].

Слід підкреслити, що сьогодні розгортається надзвичайно активна

дискусія щодо меж використання ІІІ і у цій сфері. Про що свідчать багаточисленні публікації українських науковців [270; 134; 103; 268], які мають бути концептуально оцінені в окремому галузевому дослідженні.

Попри те, що використання ІІІ потенційно здатне мінімізувати окремі прояви людського фактора, зокрема корупційні ризики, та викликати позитивне суспільне сприйняття, впровадження непрозорих алгоритмічних систем у сферу судочинства в умовах низького рівня інституційної довіри може, навпаки, посилювати суспільні підозри та формувати уявлення про появу додаткового «цифрового прошарку» між громадянином і судом. Саме тому будь-які експериментальні моделі використання ІІІ в українському правосудді повинні супроводжуватися максимальною відкритістю, пілотними проєктами, незалежною експертизою та широкою професійною дискусією, а також реалізовуватися з урахуванням європейських стандартів і вимог у контексті євроінтеграційних процесів України.

З урахуванням викладеного правова політика України у сфері застосування ІІІ в судочинстві повинна базуватися на таких засадах:

- заборона повністю автоматизованого ухвалення судових рішень у справах, що стосуються прав, свобод та обов’язків людини і громадянина;
- визнання систем ІІІ виключно допоміжними інструментами, які не позбавляють суддю обов’язку самостійно оцінювати докази та формувати правові висновки;
- встановлення законодавчих вимог щодо пояснюваності, прозорості та можливості оскарження рішень, ухвалених із використанням ІІІ;
- запровадження процедур незалежної оцінки алгоритмічних систем, що використовуються у судовій діяльності, включно з аудитом алгоритмічної упередженості та перевіркою відповідності правам людини;
- забезпечення особливих гарантій захисту даних учасників судового процесу, які використовуються для навчання та функціонування відповідних систем.

3.6. Правове регулювання обмеження використання штучного інтелекту в освіті та науці

Сфера освіти є одним із найпоширеніших і водночас найбільш дискусійних напрямів інтеграції технологій штучного інтелекту. Відповідно до результатів аналізу, представлених у підрозділі 1.3 та висновках до розділу 1, цей сектор характеризується високим рівнем поляризації суспільних запитів, що виявляється навіть на рівні індивідуального сприйняття (див. додаток Г). Емпірично встановлена парадоксальність ставлення респондентів до ШІ полягає у своєрідному когнітивному дисонансі: визнання його беззаперечної користі для розвитку освіти й науки поєднується з високим рівнем занепокоєння щодо загроз академічній доброчесності.

Освітній сектор є одним із ключових напрямів практичного розгортання штучного інтелекту (ШІ). Попри значну кількість застережень та очевидне зростання ризиків недоброчесного використання відповідних технологій, конструктивний потенціал ШІ залишається вагомим і багатовимірним. Інтеграція інтелектуальних систем дозволяє автоматизувати рутинні процеси, зокрема оцінювання та адміністрування, оптимізувати використання людських ресурсів, забезпечити персоналізацію навчання, а також впроваджувати інноваційні форми поширення й дисемінації знань.

Провідною перевагою ШІ є індивідуалізація освітнього процесу шляхом адаптації навчальних матеріалів до рівня підготовки, темпу сприйняття та індивідуальних потреб кожного здобувача освіти. Технології ШІ виступають ефективним інструментом моделювання й моніторингу індивідуальних освітніх траєкторій, проєктування навчальних планів, а також прогнозування результатів професійної атестації. Крім того, алгоритмічні системи суттєво спрощують пошук інформації та аналіз великих масивів даних, що набуває особливого значення для сучасної освітньої й наукової діяльності [37, с. 140].

Автоматизація рутинних завдань, зокрема перевірки письмових робіт і тестових завдань, вивільняє часовий ресурс педагогічних працівників для

наукової, методичної та творчої діяльності. У контексті дистанційного навчання ІІІ також відкриває перспективи створення інтерактивних платформ, адаптивних курсів, а також інтеграції віртуальних викладачів, цифрових помічників і чат-ботів.

Зазначені переваги трансформують професійну діяльність викладачів, оптимізують роботу здобувачів освіти та адміністративного персоналу, формуючи якісно новий рівень організації освітнього процесу. Делегація алгоритмічним системам рутинних завдань, які раніше потребували значних часових ресурсів, мінімізує технічне навантаження на людину та сприяє підвищенню ефективності освітньої діяльності. Високий рівень суспільного запиту визначає освітню систему як одну з провідних платформ інтеграції штучного інтелекту (ІІІ). За умови відповідального впровадження таких технологій із урахуванням потенційних ризиків їх використання можливе суттєве підвищення ефективності, доступності, адаптивності та гнучкості освітніх процесів.

На практиці в освітнє середовище вже інтегровано прикладне програмне забезпечення з елементами ІІІ, призначене для розпізнавання мовлення, машинного навчання та комп'ютерного зору. До репрезентативних прикладів належать адаптивні системи управління навчанням (Learning Management Systems, LMS)³, які здатні коригувати дидактичний контент і темп засвоєння навчального матеріалу залежно від академічних результатів здобувачів освіти. Функціональні можливості таких платформ додатково розширюються за рахунок інтеграції інтелектуальних чат-ботів і цифрових помічників, що забезпечують оперативне консультування та координацію взаємодії між суб'єктами освітнього процесу.

Поряд із цим сервіси генерації та аналізу текстового й графічного

³ **Ellis R. K.** Learning Management System - це програмне забезпечення для адміністрування, документування, відстеження, звітності, автоматизації та надання навчальних курсів, навчальних програм, матеріалів або програм навчання та розвитку [Ellis, Ryann K. (2024), Field Guide to Learning Management. American Society for Training & Development (ASTD). 2009. URL: https://web.archive.org/web/20140824102458/http://www.astd.org/~/media/Files/Publications/LMS_fieldguide_20091]

контенту виступають ефективними асистивними інструментами у професійній діяльності викладача, зокрема у процесах підготовки методичних матеріалів, створення навчального контенту та верифікації результатів тестування.

Попри очевидні дидактичні переваги, інтеграція штучного інтелекту супроводжується високим рівнем ризиків, ключовими серед яких є загрози академічній доброчесності [521]. Деструктивний потенціал таких процесів виходить за межі локальних порушень освітньої етики, оскільки нівелювання принципів доброчесності на етапі підготовки фахівців безпосередньо впливає на якість людського капіталу, професійної компетентності та функціонування майбутнього експертного середовища. У цьому контексті ризики недоброчесного використання ШІ набувають системного характеру та формують довгострокові суспільні наслідки.

Стрімке поширення генеративних платформ (зокрема, ChatGPT, Perplexity та інших) актуалізувало появу феномену своєрідної академічної «антикультури», у межах якої алгоритмічні системи використовуються не як допоміжний інструмент навчання, а як механізм імітації інтелектуальної діяльності. Практика неконтрольованого використання ШІ охоплює широкий спектр порушень – від автоматизованого виконання поточних навчальних завдань до генерації кваліфікаційних і наукових робіт без належного рівня осмислення, засвоєння та рефлексії навчального матеріалу здобувачами освіти.

За таких умов інтенсифікація використання ШІ зумовлює необхідність формування комплексної системи правових, етичних та організаційних механізмів контролю, що мають базуватися на принципах прозорості, верифікації авторства, цифрової етики, захисту персональних даних і відповідального використання інтелектуальних технологій.

Інституціоналізація правових стандартів академічної доброчесності, втілена у Законі України «Про академічну доброчесність», формує важливі нормативні засади забезпечення безпеки освітнього середовища, однак окремі положення акта можуть ускладнювати формування єдиної правозастосовної практики. Однією з проблем залишається недостатня визначеність критеріїв

кваліфікації окремих порушень академічної доброчесності, що створює ризики суб'єктивного тлумачення відповідних норм.

Інституціоналізація правових стандартів безпеки в освітньому середовищі, втілена у Законі України «Про академічну доброчесність» [187], наразі не забезпечує повною мірою досягнення покладених на неї регуляторних цілей. Однією з ключових проблем акта є розмитість правових меж академічного правопорушення, зумовлена відсутністю чіткого алгоритму фіксації та кваліфікації відповідних девіацій. Нормативна дефініція, закріплена у п. 1 ст. 17 Закону, визначає порушення як будь-яку дію або бездіяльність суб'єкта, що суперечить внутрішнім чи загальним правилам і цінностям академічної доброчесності [187], що, своєю чергою, створює значний простір для суб'єктивного тлумачення та неоднорідної правозастосовної практики

Окрему юридичну специфіку документа становить поширення механізмів академічної відповідальності на здобувачів освіти, які досягли 14-річного віку. Водночас практична реалізація окремих положень Закону може ускладнюватися значною диференціацією видів порушень академічної доброчесності та складністю їх чіткого розмежування у правозастосовній діяльності.

У вітчизняному науковому дискурсі однією з найбільш актуальних проблем, пов'язаних із використанням штучного інтелекту, є академічний плагіат у контексті застосування контенту, згенерованого алгоритмічними системами. Дослідження українських учених засвідчують тенденцію до розширення меж традиційного розуміння плагіату шляхом включення до нього результатів алгоритмічної генерації. Зокрема, В. Явір та Д. Макішев відносять до проявів академічного плагіату використання «текстів та/або результатів, згенерованих комп'ютерною програмою в автоматичному режимі» [275], наголошуючи на неможливості визнання фізичної особи автором академічного твору, фактичним творцем якого виступає система штучного інтелекту.

Поряд із проблемою недоброчесного авторства окремим ризиком у площині академічної етики є інтеграція ШІ-технологій у процеси моніторингу

та оцінювання знань. Використання алгоритмічних систем для перевірки творчих, аналітичних чи проєктних завдань обмежується відсутністю емоційного інтелекту, недостатньою здатністю до глибокого контекстуального аналізу, а також неспроможністю повною мірою враховувати соціокультурні, вікові та інклюзивні особливості комунікації здобувачів освіти.

За таких умов алгоритмічні похибки можуть призводити до викривлення об'єктивності оцінювання, формування у здобувачів освіти відчуття несправедливого ставлення та зростання конфліктності в межах освітнього процесу. У довгостроковій перспективі подібні практики створюють ризики для інституційної довіри та репутації закладів вищої освіти.

Автоматизація контролю знань є ще одним критично важливим аспектом, який у сучасній науковій літературі розглядається як сфера підвищених ризиків при застосуванні технологій штучного інтелекту. Дослідженню цієї проблематики присвячено значний масив актуальних міжнародних наукових розвідок, серед яких праці К. Мегалоконому, С. Гуласа та Р. Сотіракопулоса (2025) [444], М. Воткінса (2025) [528], а також Т. Вентінг Лі зі співавторами (2023) [427].

Особливе значення для цього дослідження мають результати емпіричного експерименту Майкла Г. Вагнера (2025) [525], у межах якого здійснювався порівняльний аналіз оцінювання студентських робіт викладачем та алгоритмічними системами ШІ, попередньо налаштованими відповідно до критеріїв максимальної об'єктивності. Попри позитивні результати експерименту, що проявилися у деталізації зворотного зв'язку та здатності системи виявляти окремі помилки, не завжди помітні для викладача, автоматизоване оцінювання продемонструвало низку суттєвих обмежень і алгоритмічних похибок:

1. Висока ресурсомісткість процесів прекофігурації та верифікації даних. Налаштування систем ШІ для забезпечення належного рівня об'єктивності оцінювання потребує від викладача спеціалізованих цифрових компетентностей, а також значних часових витрат на формулювання промптів,

завантаження критеріїв і моделювання параметрів перевірки. При цьому навіть незначні інженерні або логічні помилки на етапі налаштування системи здатні суттєво деформувати підсумкові результати контролю знань.

2. Надмірна технізація процесу оцінювання та дефіцит емоційного інтелекту. Алгоритмічний аналіз позбавлений емпатійного компонента, що обмежує можливість глибокої інтелектуальної взаємодії між суб'єктами освітнього процесу. М. Вагнер характеризує цю проблему таким чином: «У способі взаємодії системи з ідеями студентів бракувало теплоти, інтуїтивного розуміння процесу навчання, а також здатності розпізнавати й підтримувати автентичну інтелектуальну допитливість».

Руйнування фундаментальної дидактичної цінності освітнього процесу. Будучи прихильником етичної інтеграції інтелектуальних технологій в освіту, дослідник порушує концептуальне питання: «Якщо здобувачі використовують штучний інтелект для написання есе, а викладачі застосовують його для їх оцінювання, то в чому полягає стрижнева освітня цінність такої справи?» [525].

Репрезентативним підтвердженням першого з окреслених ризиків є валідні емпіричні дані дослідження вчених Вашингтонського університету (США), проведеного серед педагогів початкової та середньої ланок освіти (від закладів дошкільної освіти до 12-х класів). Згідно з висновками дослідників: «Понад 60% вчителів зазначили, що вони можуть використовувати рубрики, згенеровані штучним інтелектом, у своїх класних завданнях. Більшість зазначили, що вони внесли незначні зміни до рубрики, що свідчить про їхню неготовність повністю прийняти контент, згенерований штучним інтелектом, без перегляду та коригування. Цікаво, що жоден вчитель не вказав, що він вніс суттєві зміни до рубрики, згенерованої штучним інтелектом. Лише 7% вчителів зазначили, що рубрики не можуть бути використані в їхньому класі – або тому, що вони потребували суттєвого перегляду, або тому, що вони просто не застосовні. Приблизно чверть вчителів повідомили, що вони взагалі не намагалися використовувати рубрики, згенеровані штучним інтелектом. Слід зауважити, що окремі вчителі подавали декілька форм відповідей для різних

навчальних класів, однак підсумкові результати були статистично скориговані таким чином, щоб кожен респондент мав однакову питому вагу у вибірці» [498].

Наведені статистичні показники демонструють необхідність постійного критичного моніторингу, додаткової верифікації алгоритмічно згенерованого контенту та суттєвих часових витрат з боку педагогічних працівників у процесі використання систем ІІІ для оцінювання результатів навчання.

Суб'єкти освітнього простору в демократичних державах одностайно наголошують на необхідності збереження антропоцентричного контролю (human-in-the-loop) над технологіями штучного інтелекту (ІІІ) з метою мінімізації алгоритмічних похибок та забезпечення об'єктивності оцінювання. Паралельно актуалізується потреба у розробці етичних кодексів і регламентів, що визначають чіткі межі та превентивні обмеження щодо застосування ІІІ у педагогічній практиці. Поки такі механізми формуються на загальнодержавному рівні, заклади вищої освіти (ЗВО) здатні автономно впроваджувати внутрішні інструменти превенції академічних девіацій. Світовий університетський досвід засвідчує ефективність подібного підходу в умовах масового поширення інтелектуальних систем, а відповідні практики поступово інтегруються й в освітній простір України.

Водночас критично важливим аспектом інтеграції ІІІ в освітнє середовище є ризик несанкціонованого доступу алгоритмічних систем до персональних даних здобувачів освіти та працівників освітніх інституцій. Оскільки функціонування моделей ІІІ базується на обробці значних масивів персоналізованої інформації, недостатній рівень кіберзахисту може призвести до витоку конфіденційних відомостей, несанкціонованого розголошення результатів навчання або компрометації даних з обмеженим доступом. Особливої чутливості ця проблема набуває для закладів вищої освіти військового профілю, а також інституцій, що здійснюють підготовку кадрів для сектору безпеки і оборони та правоохоронних органів

Системна інтеграція ІІІ в освітню інфраструктуру супроводжується

масштабною обробкою персональних даних здобувачів освіти та науково-педагогічних працівників. Недостатній рівень захищеності систем обробки інформації може призвести до витоку академічних реєстрів, компрометації персональних даних або несанкціонованого доступу до службової інформації, що становить особливу загрозу для закладів вищої освіти військового профілю та інституцій, які здійснюють підготовку фахівців для сектору безпеки і оборони та правоохоронних органів.

Ефективна мінімізація таких кіберризиків можлива лише за умови впровадження надійних механізмів захисту конфіденційності та переходу до архітектури безпечних цифрових освітніх платформ. Вказані вимоги узгоджуються з положеннями Закону України «Про захист персональних даних» [197] та підзаконними нормативно-правовими актами, що регулюють правовідносини у сфері автоматизованої обробки інформації.

З метою узагальнення досліджуваних аспектів правового регулювання ШІ в освітньому середовищі доцільно звернутися до концептуальних засад Регламенту Європейського Парламенту і Ради про штучний інтелект (EU AI Act), ухваленого у 2024 році.

Зазначений документ запроваджує уніфікований ризико-орієнтований підхід до регулювання систем штучного інтелекту в різних суспільних сферах. Освітній сектор перебуває під безпосереднім впливом положень цього акта, оскільки некоректне або деструктивне застосування інтелектуальних технологій у цій галузі здатне створювати загрози фундаментальним правам людини.

Відповідно до п. 56 преамбули Регламенту до категорії високоризикових (High-Risk AI Systems) віднесено системи ШІ, що використовуються у сфері освіти та професійної підготовки, зокрема для:

- визначення доступу або перевірки умов вступу здобувачів освіти;
- зарахування осіб до закладів освіти чи освітніх програм різних рівнів;
- оцінювання результатів навчання та визначення рівня підготовки особи, якщо це суттєво впливає на її подальшу освітню чи професійну траєкторію;

– прокторингу, моніторингу та виявлення заборонених форм поведінки під час екзаменів [369].

Концептуальна основа безпекової архітектури Регламенту ґрунтується на тому, що системи високого ризику можуть створювати суттєві загрози для здоров'я, безпеки та фундаментальних прав людини. Саме тому їх виведення на ринок передбачає обов'язкове проходження процедури оцінки відповідності, а подальше використання регулюється спеціальним правовим режимом. Європейський законодавець обґрунтовує таку класифікацію тим, що інструменти ШІ у сфері освіти «можуть визначати освітній і професійний курс життя людини і, таким чином, впливати на її здатність забезпечувати собі засоби до існування».

Крім того, у п. 56 Регламенту акцентується увага на ризиках, пов'язаних із неналежним проєктуванням або практичним використанням систем ШІ, що здатне призводити до надмірного втручання у приватне життя суб'єктів освітнього процесу, а також до порушення права на освіту, принципу недискримінації та відтворення історичних моделей упередженості щодо окремих соціальних груп, зокрема за ознаками статі, віку, інвалідності, расового чи етнічного походження.

Нормативне закріплення зазначеної класифікації міститься у Додатку III до Регламенту («Системи штучного інтелекту високого ризику, про які йдеться у статті 6(2)»), де до категорії високоризикових у сфері освіти та професійної підготовки віднесено системи ШІ, призначені для:

- визначення доступу, умов вступу або розподілу фізичних осіб між освітніми та професійно-технічними закладами різних рівнів (пп. «а»);
- оцінювання результатів навчання, зокрема у випадках, коли такі результати використовуються для управління освітнім процесом (пп. «b»);
- верифікації рівня освіти, який особа вже здобула або до якого може отримати доступ у межах освітніх інституцій (пп. «с»);
- прокторингу, моніторингу та виявлення заборонених форм поведінки здобувачів освіти під час екзаменаційних або тестових процедур (пп. «d»).

Подібна жорсткість правового регулювання зумовлена застереженнями, закріпленими у п. 44 преамбули Регламенту. Європейський законодавець акцентує увагу на наявності «серйозних занепокоєнь щодо наукового підґрунтя систем штучного інтелекту, призначених для ідентифікації або формування висновків про емоції» [369]. Вразливість таких технологій пов'язана з тим, що зовнішні прояви емоційного стану істотно варіюються залежно від соціокультурного контексту, конкретної ситуації та індивідуальних психофізіологічних особливостей людини.

Відповідно, системи ШІ, що здійснюють розпізнавання емоцій або намірів осіб на основі аналізу біометричних даних, можуть створювати дискримінаційні наслідки та порушувати фундаментальні права і свободи суб'єктів освітнього процесу.

Важливим орієнтиром для формування європейської політики у сфері цифрової освіти є звіт Європейської асоціації університетів «Майбутнє цифрового навчання та викладання в європейських закладах вищої освіти» (The Future of Digital Learning and Teaching in European Higher Education Institutions) [386]. У документі комплексно проаналізовано перспективи та ризики інтеграції інтелектуальних систем, а також сформульовано базові рекомендації для університетів щодо забезпечення прозорості, доброчесності та відповідального використання технологій штучного інтелекту.

Окремим напрямом сучасних наукових дискусій є проблема потенційного впливу ШІ на ринок праці у сфері освіти. Водночас наявні дослідження свідчать про те, що такий вплив має переважно трансформаційний, а не деструктивний характер. З огляду на офіційне віднесення освітніх ШІ-технологій до категорії високоризикових, їх використання передбачає обов'язкове збереження антропоцентричного контролю та постійної участі «людини у контурі управління» (*human-in-the-loop*).

Відповідно до концепції цифрової трансформації освіти, ключова роль у дидактичному процесі має залишатися за професійним педагогом як основним суб'єктом освітньої взаємодії. За таких умов інтелектуальні системи здатні

автоматизувати переважно технічні, рутинні або адміністративні завдання, що оптимізує структуру робочого часу, однак не створює передумов для масштабного витіснення викладача з освітнього процесу чи суттєвого скорочення професорсько-викладацького складу.

Трансформація професійної діяльності освітян під впливом штучного інтелекту (ШІ) має комплексний і нелінійний характер та не створює однозначно деструктивних наслідків для кадрового потенціалу галузі. Інтеграція інтелектуальних систем дозволяє оптимізувати освітній процес шляхом автоматизації контрольних-оцінювальних, адміністративних і технічних функцій, що вивільняє інтелектуальний ресурс суб'єктів викладання та знижує навантаження у сфері рутинної діяльності. Водночас ШІ виступає каталізатором модернізації дидактики, забезпечуючи індивідуалізацію навчання, супровід педагогічної діяльності та відкриваючи нові форми поширення й дисемінації знань.

Подібні трансформації стимулюють диверсифікацію ринку праці через появу нових професійних профілів, зокрема фахівців з інтеграції ШІ в освітній простір, розробників адаптивних навчальних програм та аналітиків великих освітніх даних. Зрештою, характер впливу інтелектуальних технологій на сферу зайнятості залежатиме від моделі імплементації ШІ, дотримання принципу антропоцентричного контролю та здатності суспільних інститутів адаптуватися до цифрових трансформацій.

Аналізуючи світові тенденції розгортання ШІ у вищій школі, дослідники акцентують увагу на безальтернативності ролі «викладача, наставника, наукового керівника тощо. Адже навчальний процес багатогранний і не обмежується лише розв'язанням поставлених завдань. Людська взаємодія в освіті незамінна і має безліч соціальних задач» [4]. Повноваження педагога виходять далеко за межі механічної трансляції інформації, охоплюючи аксіологічні, виховні та соціалізаційні аспекти, які залишаються недоступними для алгоритмічних систем.

Таким чином, застереження щодо деструктивного впливу штучного

інтелекту (ШІ) на ринок праці педагогічних працівників видаються перебільшеними. Ключова трансформація полягатиме не у скороченні робочих місць, а в модернізації професійного профілю викладача та набутті ним специфічних цифрових компетентностей для ефективного використання ШІ-технологій. Репрезентативним прикладом такої синергії є інтелектуальні системи навчання, що забезпечують індивідуалізацію дидактичного процесу та оперативний зворотний зв'язок, виступаючи інтенсифікатором, а не сурогатом професійної діяльності педагога.

Делегування алгоритмічним системам рутинних, трудомістких і масштабованих операцій дозволяє оптимізувати робочий час людини та зосередити увагу на складніших формах педагогічної взаємодії. Водночас викладач безальтернативно зберігає за собою концептуальні функції наставника, ментора, модератора освітнього процесу та суб'єкта академічної відповідальності. Такий розподіл функцій узгоджується з ризико-орієнтованою логікою Регламенту ЄС про штучний інтелект, який обмежує автономію високоризикових систем у гуманітарній сфері та зберігає визначальну роль людини у процесі ухвалення рішень.

Узагальнюючи вищезазначене, можна дійти висновку, що домінуючими ризиками інтеграції штучного інтелекту (ШІ) в освітній простір є: академічний плагіат (експлуатація генеративних моделей для створення текстів), механістичне й потенційно упереджене оцінювання, витік великих масивів персональних даних, а також загроза скорочення робочих місць викладачів. При цьому три з чотирьох окреслених деструктивних чинників уже мають превентивні механізми нівелювання, тоді як побоювання щодо масового безробіття освітян позбавлені об'єктивних передумов. Логіка розв'язання цих проблем базується на таких засадах:

1. Регулювання академічної доброчесності: подолання негативних проявів використання ШІ має здійснюватися у контексті класичного розуміння плагіату з акцентом на локальну нормативну регламентацію в межах конкретних інституцій. Доцільним є чітке унормування випадків припустимого

застосування ШІ для певних типів навчальних завдань за умови обов'язкового розкриття (декларування) обсягів його використання здобувачами.

2. Обмеження автоматизованого оцінювання: алгоритмічний контроль знань позбавлений емпативного компонента та здатності враховувати соціокультурний контекст творчих робіт. Відтак, делегування функцій оцінювання ШІ є валідним виключно для чітко структурованих, алгоритмізованих завдань (зокрема, тестових форм). Такий підхід повністю узгоджується зі стандартами Регламенту ЄС про штучний інтелект, який класифікує системи освітнього оцінювання як високоризикові.

3. Захист від дискримінаційних практик: відповідно до положень Регламенту ЄС, оцінювальна діяльність не може бути повністю автономізована через загрозу репродукування алгоритмами узагальнених моделей упередженості. Забезпечення фундаментальних прав учасників освітнього процесу вимагає обов'язкового збереження антропоцентричного (людського) контролю на всіх етапах експертизи.

4. Стабілізація кадрового потенціалу: синергія попередніх чинників доводить, що інтеграція ШІ не зумовить тотального скорочення робочих місць у вищій школі. Провідна та регулююча роль педагога визнана на міжнародному рівні як ключова безпекова гарантія, що перетворює ШІ з конкурента на допоміжний дидактичний інструмент.

Європейська доктрина правового регулювання штучного інтелекту (ШІ) не містить прямих заборон щодо застосування штучного інтелекту (ШІ) в освітній сфері, проте загальні обмеження щодо використання недопустимих ШІ-технологій є релевантними й для інститутів освіти. Зокрема, Регламент ЄС про штучний інтелект обмежує можливість повної автономізації систем оцінювання знань, відносячи цю сферу до категорії високого ризику через її безпосередній вплив на забезпечення фундаментальних прав людини.

Зазначені обставини зумовлюють формування прозорих і валідних правил використання ШІ в освітньому процесі. Здобувачі освіти, викладачі та науковці потребують чіткої нормативної диференціації між допустимим застосуванням

ШІ-інструментів – для інформаційного пошуку, технічного асистування, лінгвістичного редагування, візуалізації даних тощо – та неправомірним використанням алгоритмів, що призводить до симуляції авторства, заміщення самостійної когнітивної діяльності або фальсифікації результатів дослідження.

Відсутність подібної нормативної визначеності створює ризик формування своєрідної інституційної аномії у закладах вищої освіти, що може проявлятися у двох протилежних формах: або у надмірно рестриктивному підході, який провокує розрив між формальними вимогами та реальною освітньою практикою, або у безконтрольній лібералізації, що поступово нівелює аксіологічний зміст освіти як процесу формування компетентностей і самостійного мислення.

Окремого теоретико-правового осмислення потребує проблема потенційного обмеження професійної автономії викладачів і дослідників. Використання освітніх платформ із вбудованими ШІ-модулями, які генерують стандартизовані навчальні програми, форми контролю та шаблони зворотного зв'язку, здатне створювати ризики алгоритмічного патерналізму та поступового звуження педагогічної творчості. У науково-дослідній сфері алгоритмічні системи ранжування видань, авторів та індексів цитування можуть стимулювати методологічний конформізм, орієнтуючи дослідників на кон'юнктурні теми на шкоду міждисциплінарним і нетривіальним науковим пошукам.

За таких умов завдання правового регулювання полягає не лише у формальному закріпленні статусу викладача й науковця, а й у створенні ефективних інституційних гарантій академічної свободи, здатних запобігти її технологічному знеціненню в умовах цифрової трансформації освіти.

В українських реаліях зазначені виклики додатково екстраполюються на умови воєнного стану, масштабний перехід до дистанційного та змішаного форматів навчання, а також перманентні трансформації сфер вищої освіти й науки. З одного боку, це інтенсифікує потребу в цифрових та, зокрема, ШІ-інструментах для оптимізації дидактичного процесу, моніторингу знань і

підтримки суб'єктів освітнього процесу, особливо тих, які перебувають у прифронтових регіонах або мають статус внутрішньо переміщених осіб. З іншого боку, зазначені чинники створюють передумови для розгортання систем тотального цифрового контролю та прокторингу, здатних порушувати права здобувачів освіти й викладачів на приватність, свободу вираження поглядів та академічну автономію.

Відтак будь-які рестрикції щодо застосування ІІІ в освітній та науковій сферах мають бути векторизовані виключно на захист людської суб'єктності в академічному середовищі – як здобувачів освіти, так і професорсько-викладацького та дослідницького складу. У цьому контексті особливого значення набуває необхідність формування збалансованої правової політики, здатної поєднати потреби цифрової модернізації освіти із гарантіями фундаментальних прав людини та збереженням академічних свобод.

З огляду на необхідність подальшої модернізації законодавства про освіту та академічну доброчесність, для вітчизняної правової політики доцільно сформулювати такі стратегічні орієнтири:

1. **Нормативна імплементація** – закріплення на рівні законів та локальних актів закладів вищої освіти диференційованих правил використання ІІІ в освітній і науково-дослідній діяльності, включно з обов'язком декларування фактів використання генеративних платформ.

2. **Процедурна верифікація** – розробка спеціалізованих механізмів виявлення та реагування на порушення академічної доброчесності із застосуванням ІІІ, що поєднуюватимуть превентивні, просвітницькі та санкційні інструменти.

3. **Алгоритмічна транспарентність** – встановлення вимог до прозорості та підзвітності інтелектуальних систем, які використовуються для оцінювання, селекції чи моделювання освітніх траєкторій, із гарантуванням права на апеляційне оскарження автоматизованих рішень.

4. **Захист академічних свобод** – забезпечення того, щоб інституціоналізація ІІІ виступала фасилітатором, а не деструктором

академічної свободи й автономії закладів освіти та наукових установ.

5. Посилення кібербезпеки – удосконалення механізмів захисту персональних даних здобувачів освіти та дослідників, які інтегруються в операційні середовища освітніх ІІІ-платформ.

Окреслені орієнтири можуть слугувати концептуальним підґрунтям для подальшого вдосконалення Законів України «Про освіту» та «Про академічну доброчесність» у частині комплексного правового регулювання використання технологій штучного інтелекту в освітній та науковій сферах.

Висновки до розділу 3

1. В межах трансгуманістичної парадигми оцінювання екзистенційних загроз цифровізації обґрунтовано правову природу машинного навчання як ключової специфічної ознаки систем штучного інтелекту, що кардинально змінює класичні підходи до створення програмного забезпечення. Доведено, що перехід від лінійного алгоритмічного програмування конкретного результату до автономного навчання системи на масивах даних трансформує систему юридичних ризиків. Встановлено, що заснований на прецедентах та емпіричних прикладах характер формування «поведінки» штучного інтелекту позбавляє розробника можливості повного прогнозування фінальних алгоритмічних рішень (явище алгоритмічної нелінійності). Обґрунтовано, що така особливість підриває традиційні інститути деліктного права, засновані на принципі передбачуваності шкоди, та вимагає впровадження нових механізмів етико-правового обмеження у високоризикових сферах суспільних відносин.

2. Систематизація новітніх трансгуманістичних та філософсько-правових концепцій (Х. Дрейфуса, Н. Бострома, С. Рассела, М. Тегмарка, Р. Курцвейла) дозволила типологізувати сучасні доктринальні застереження щодо використання штучного інтелекту у чотири фундаментальні блоки ризиків:

- аксіологічний (ціннісний) ризик – дефіцит узгодженості алгоритмічних рішень із людськими цінностями, етичними принципами та деонтологічними

засадами права;

- інституційно-безпековий ризик – екзистенційна загроза втрати суверенного людського контролю над автономними системами та виникнення нерегульованої військово-технологічної конкуренції;

- антропологічний ризик – підрив особистої автономії, конфіденційності, автентичності людського потенціалу та свободи волі;

- соціально-економічний ризик – загроза глобальної дестабілізації, поглиблення соціальної нерівності та неконтрольованої мілітаризації суспільства.

Консолідація зазначених ризиків формує єдине філософсько-методологічне підґрунтя для переходу від ліберальної парадигми невтручання до моделі керованого та проактивного державного регулювання.

3. На основі детального дослідження прецедентних і нормативних обмежень у найбільш соціально-чутливих сферах суспільного життя обґрунтовано універсальний регуляторний потенціал воєнної класифікації автономних систем озброєння (AWS) за критерієм інтенсивності людського контролю. Систематизовано та юридично верифіковано три базові моделі суб'єктної взаємодії:

- «людина в контурі управління» (*human in the loop*), що передбачає безперервний операційний контроль та можливість поточного коригування дій системи людиною;

- «людина над контуром управління» (*human on the loop*), за якої система функціонує в автономному режимі під стратегічним наглядом оператора з правом втручання (*override*) у разі алгоритмічних аномалій;

- «людина поза контуром управління» (*human out of the loop*), що характеризується повною автономністю машини на етапах детекції, селекції та ураження цілей без подальшого людського втручання.

Доведено, що екстраполяція вказаної тріади за межі мілітарного сектору дозволяє сформуванню уніфіковану міжгалузеву модель правового регулювання, яка забезпечує диференціацію нормативних обмежень, визначення ступенів

ризиків та фіксацію суб'єктів деліктної відповідальності на різних етапах життєвого циклу систем штучного інтелекту.

4. Обґрунтовано правове значення психо-когнітивного феномену надмірної довіри до автоматизації (automation bias) як одного з ключових деструктивних чинників, що підриває ефективність нормативно-правового обмеження штучного інтелекту у високоризикових сферах (воєнній, медичній та правоохоронній). Доведено, що беззастережне підпорядкування оператором власного критичного судження алгоритмічним висновкам трансформує юридично закріплені режими людського контролю (human-in/on-the-loop) у формальні процедури, позбавлені реального змісту. З погляду теорії права така деформація кваліфікується як порушення стандарту належної професійної обачності (due diligence) та прояв професійної недбалості.

Встановлено, що подолання ефекту automation bias вимагає не лише імперативної заборони систем абсолютної алгоритмічної автономії, а й запровадження комплексних інституційно-правових запобіжників, зокрема нормативного закріплення процедур обов'язкової людської верифікації критичних даних, спеціальних професійно-психологічних вимог до операторів та підвищених стандартів юридичної відповідальності у випадках сліпого слідування помилковим рекомендаціям алгоритмічних систем.

5. Концептуалізовано проблему наднаціонального правового вакууму у сфері регулювання автономних систем озброєння (AWS) з елементами штучного інтелекту та Інтернету речей (ІоТ), зумовлену виключенням мілітарного сектору з предмета регулювання Регламенту ЄС 2024/1689 (AI Act).

Доведено, що єдиною легітимною нормативною основою регулювання у цій сфері залишається система імперативних принципів міжнародного гуманітарного права (МГП). На основі аналізу офіційних доктринальних позицій Міжнародного комітету Червоного Хреста (МКЧХ) обґрунтовано методологічну неможливість повної алгоритмізації воєнних рішень, оскільки сучасний ШІ нездатний до повноцінного моделювання оціночних категорій МГП – принципів розрізнення, пропорційності та запобігання надмірним

стражданням. Доведено, що системи класу «human out of the loop» мають розглядатися як різновид зброї невибіркової дії, що потребує кодифікації міжнародно-правової заборони на їх розроблення, виробництво та накопичення.

6. Обґрунтовано закономірності формування сучасної моделі правового регулювання штучного інтелекту у сферах медицини та фармакології. Доведено, що еволюція нормативного нагляду відображає системний перехід від дескриптивних етичних орієнтирів (Звіт ВООЗ 2021 р.) до комплексних юридичних механізмів регулювання (Регламент (ЄС) 2017/745 про медичні вироби (MDR), Регламент (ЄС) 2024/1689 (AI Act), План дій FDA SaMD, Настанови ICH E6(R3)). Сформульовано авторський концепт багаторівневого алгоритмічного контролю та запропоновано модель двокомпонентного комплаєнсу, відповідно до якої функціонування технічних підсистем у режимі «людина поза контуром управління» (*human out of the loop*) допускається виключно для первинного скринінгу, аналізу зображень і тріажу, тоді як безпосередня діагностика, вибір планів лікування та біоетична валідація клінічних випробувань мають здійснюватися в режимах «людина над контуром управління» (*human on the loop*) або «людина над контуром управління» (*human on the loop*). Такий підхід забезпечує збереження виключної професійної дискреції лікаря. Доведено доктринальну потребу в модернізації інституту інформованої згоди пацієнта шляхом упровадження моделі розширеної інформованої згоди (*extended informed consent*), яка передбачає обов'язок розкриття особі регуляторного статусу алгоритму, ступеня його експериментальності, специфічних ризиків та конвенційних альтернатив лікування.

7. На основі узагальнення прецедентів дискримінаційного та неправомірного втручання у приватне життя громадян (зокрема при масовому біометричному розпізнаванні облич у публічному просторі) концептуалізовано доктринальні засади обмеження штучного інтелекту у правоохоронній діяльності та діяльності спецслужб. Відповідно до положень AI Act обґрунтовано необхідність чіткого розмежування поліцейських систем на

категорію абсолютно заборонених технологій (дистанційна біометрична ідентифікація в реальному часі, системи предиктивного профайлінгу злочинності) та категорію систем високого ризику, використання яких допускається лише за умов суворого процесуального контролю. Сформульовано принцип остаточного людського арбітражу, відповідно до якого використання моделі «людина поза контуром управління» (*human out of the loop*) у правоохоронному секторі є безумовно протиправним, тоді як єдиним легітимним процесуальним стандартом визнається модель «людина в контурі управління» (*human in the loop*), що гарантує право уповноваженої особи на скасування будь-якого автоматизованого висновку.

8. Концептуалізовано правові ризики непрозорості функціонування штучного інтелекту, відомої як «ефект чорної скриньки» (*black box effect*), у сфері сучасного судочинства. Доведено, що технічна неможливість інтерпретації логіки алгоритмічних розрахунків створює пряму загрозу нівелювання конституційного принципу належної правової процедури (*due process*) та права на справедливий суд (стаття 6 ЄКПЛ). Установлено, що віднесення наднаціональним законодавцем судових ШІ-систем до категорії високого ризику за Регламентом (ЄС) 2024/1689 перевело етичні принципи Хартії СЕРЕJ у площину конкретних процесуальних гарантій: обов'язкового логування (*traceability*), пояснюваності (*explainability*) та безперервного людського нагляду (*human oversight*). Спростовано теоретичну обґрунтованість концепції «цифрового судді» та запропоновано модель ШІ як функціонально обмеженого технічного помічника, підпорядкованого принципам верховенства права, незалежності суду та збереження виключної компетенції людського судового розсуду.

9. Концептуалізовано специфіку правового регулювання штучного інтелекту в освітній та науковій сферах, визначених як простори парадоксального сприйняття цифрових інновацій. Обґрунтовано доцільність віднесення систем ШІ для оцінювання рівня знань і профайлінгу здобувачів освіти до категорії високого ризику за AI Act, оскільки повне усунення

людського контролю у цій сфері створює загрозу алгоритмічного впливу на майбутню професійну траєкторію особи. Доведено, що мінімізація етико-деонтологічних ризиків (зокрема академічного плагіату) має здійснюватися шляхом модернізації локального нормативного регулювання академічної доброчесності через упровадження принципу прозорості авторства (disclosure). Обмежено сферу самостійного «машинного оцінювання» виключно лінійними та формалізованими завданнями (тестуванням), тоді як оцінювання творчих робіт вимагає імперативного закріплення режиму «human in the loop». Доведено, що участь педагога залишається ключовою міжнародно визнаною гарантією безпечного використання ШІ в освіті, що мінімізує ризики депрофесіоналізації та масового скорочення робочих місць.

10. Сформульовано методологічну модель «карти ризиків», відповідно до якої різні форми використання штучного інтелекту потребують диференційованих правових режимів та неоднакового ступеня нормативних обмежень залежно від потенційного впливу на фундаментальні права людини, суспільну безпеку та рівень автономності алгоритмічної системи. У межах цієї моделі:

- у сфері автономної зброї – обґрунтовано необхідність імперативної міжнародно-правової заборони систем, позбавлених змістовного людського контролю, а також обов'язкового аудиту на відповідність нормам міжнародного гуманітарного права;

- у сфері медицини – доведено потребу нормативного закріплення розширеної інформованої згоди, захисту великих медичних даних та субсидіарної відповідальності розробників;

- у правоохоронному секторі – обґрунтовано необхідність заборони практик масового нагляду, соціального скорингу та предиктивного профайлінгу;

- у сфері правосуддя – доведено неприпустимість автономного ухвалення судових рішень із гарантуванням права на оскарження та пояснюваність алгоритмічних висновків;

- в освіті і науці – обґрунтовано доцільність локального нормативного регулювання засад академічної свободи, доброчесності та захисту конфіденційності даних здобувачів освіти.

11. Виявлено та теоретично узагальнено спільну ціннісну основу правових обмежень штучного інтелекту в усіх досліджених сферах суспільних правовідносин. Доведено, що людська гідність, право на життя і здоров'я, особиста свобода та безпека, недоторканність приватності, недискримінація, доступ до справедливого суду й академічна свобода виступають первинними аксіологічними критеріями допустимості алгоритмізації суспільних відносин. Саме ця система фундаментальних цінностей визначає межу, за якою штучний інтелект може розглядатися як легітимний інструмент оптимізації суспільних процесів або ж як потенційна загроза, що потребує жорсткого нормативного контролю чи повної юридичної заборони.

12. Доведено, що обмеження використання штучного інтелекту в сучасному правовому полі не можуть зводитися виключно до технічних стандартів чи інженерних регламентів кодування. Обґрунтовано, що регулювання алгоритмічного середовища становить комплексне політико-правове завдання суверенної держави та вимагає формування цілісної національної цифрової правової політики. Така політика має поєднувати імперативні заборони неприйнятних цифрових практик, спеціальні жорсткі режими для високоризикових сфер та гнучкі «м'які» механізми регулювання для технологій із мінімальним або обмеженим ступенем ризику.

Установлено, що легітимність використання систем штучного інтелекту у демократичній правовій державі безпосередньо залежить від забезпечення принципів прозорості, пояснюваності, підзвітності алгоритмічних рішень та збереження реального людського контролю. Відповідні регуляторні рішення мають ухвалюватися насамперед на стратегічному рівні державної правової політики з урахуванням ризик-орієнтованого підходу, галузевої специфіки застосування високих технологій та необхідності пріоритетного захисту людської суб'єктності.

РОЗДІЛ 4. ФОРМУВАННЯ СУЧАСНОЇ ІНСТИТУЦІЙНОЇ МОДЕЛІ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ В УМОВАХ ЄВРОІНТЕГРАЦІЇ

Проведене у попередніх розділах дослідження дає підстави стверджувати, що формування правової моделі використання штучного інтелекту в Україні не може зводитися до механічного перенесення окремих положень іноземного законодавства або до доповнення чинних законів поодинокими згадками про алгоритмічні системи. Відсутність законодавчої класифікації ризиків, єдиної процедури оцінювання впливу на основоположні права і спеціальних гарантій для осіб свідчать про необхідність переходу від фрагментарного стратегічного регулювання до цілісної державної правової політики.

Така політика повинна одночасно виконувати три функції. По-перше, правозахисну, оскільки використання систем ШІ органами публічної влади та приватними суб'єктами може впливати на гідність, приватність, рівність, свободу вираження поглядів, доступ до публічних послуг і право на ефективний засіб юридичного захисту. По-друге, безпекову, адже алгоритмічні системи стають складовою критичної інформаційної інфраструктури, оборони, кібербезпеки та управління кризовими ситуаціями. По-третє, інноваційно-стимулюючу, тому що надмірно невизначені або непропорційні обмеження можуть перешкоджати технологічному розвитку, доступу українських розробників до європейського ринку та впровадженню суспільно корисних рішень.

Конституційним ядром такої політики мають бути положення ст. ст. 3, 8, 19, 32, 34 і 55 Конституції України, з яких випливають пріоритет людини та її безпеки, вимога законності діяльності органів публічної влади, захист приватності й інформаційних прав, а також гарантованість судового захисту. У сфері ШІ ці положення набувають процедурного значення: чим істотніше алгоритмічний результат впливає на права та законні інтереси особи, тим вищими мають бути вимоги до нормативної визначеності, обґрунтування мети,

якості даних, людського контролю, документування та можливості оскарження [115].

4.1. Ризик-орієнтована правова політика та адміністративні процедури обмеження використання штучного інтелекту в Україні

О. Є. Користін та Н. П. Свиридюк справедливо зауважують, що в умовах невизначеності ризик-орієнтований підхід є найбільш ефективним інструментом управління, що забезпечує системне виявлення, аналіз та оцінку потенційних загроз і визначення пріоритетів державної політики. На основі ризик-орієнтованого підходу може бути проведено стратегічний аналіз: ідентифікацію та ранжування загроз; аналіз і оцінку ризиків їх поширення; а також оцінювання спроможності та вразливості певних галузей щодо мінімізації таких ризиків і забезпечення ефективної реалізації державної політики [121, с. 195].

І. А. Нечаєва та А. Ю. Панкова, характеризуючи цей підхід в управлінні вказують: «...відповідно до сучасної теорії антикрихкості та ризик-орієнтованого підходу, замість того, щоб мінімізувати ризик, протистоячи змінам, організаціям необхідно змінюватися так часто, щоб система в цілому та її підсистеми змушені були робити свої речі стійкими» [166, с. 26].

В. Некрасов та Г. Катамадзе підкреслюють, що ризик-орієнтований підхід спрямований на формування системної методології оцінки ризиків (загроз, вразливостей, наслідків) шляхом комплексного аналізу статистичних даних, експертних оцінок, результатів правозастосовної діяльності, міжнародного досвіду та інших релевантних джерел інформації. Його призначення полягає у структуризації інформації про загрози, вразливості та можливі наслідки їх реалізації, що забезпечує прийняття обґрунтованих управлінських рішень, вибір пропорційних заходів реагування та адаптацію найкращих міжнародних практик до національних умов [165, с. 312 – 313].

Вчені розвивають концепцію трирівневої моделі аналітичної діяльності передбачає системний підхід до організації аналітичного забезпечення, що ґрунтується на інтеграції аналітичних функцій на всіх рівнях управління – від безпосередньої практичної діяльності до стратегічного планування. Відповідно до цієї моделі, перший рівень аналітичної роботи полягає у застосуванні аналітичних інструментів уповноваженими суб'єктами під час планування та здійснення заходів у межах їх компетенції. На цьому етапі здійснюються виявлення первинних ознак потенційних загроз, їх попередній аналіз, оперативний пошук інформації та забезпечується своєчасне реагування з метою попередження або мінімізації можливих ризиків [264, с. 191; 120; 114].

Група з розробки фінансових заходів протидії відмиванню коштів (FATF) розробила власну методику, яка лежить в основі ризик-орієнтованих підходів правового регулювання та управління у різних сферах відносин. Найважливіша ідея FATF полягає в тому, що державне регулювання не повинно бути однаковим для всіх об'єктів. Інтенсивність державного впливу має визначатися рівнем ризику. Саме тому заходи державного нагляду, контрольні процедури та ресурси концентруються насамперед на сферах із найбільшою ймовірністю настання негативних наслідків, тоді як щодо низькоризикових об'єктів застосовуються менш інтенсивні механізми регулювання. FATF виходить із того, що ефективне регулювання починається з визначення, оцінки та розуміння ризиків. Лише після цього визначаються форма, частота та інтенсивність наглядових заходів. Таким чином, оцінка ризиків є первинним елементом, а контроль – похідним. FATF наголошує, що ризики не є статичними. Наглядовий орган повинен постійно здійснювати їх моніторинг, переглядати оцінки та оперативно реагувати на появу нових загроз. Заходи контролю повинні відрізнятися залежно від характеру, масштабу та інтенсивності ризиків. Це означає, що однакові регуляторні вимоги не можуть застосовуватися до всіх суб'єктів або систем без урахування рівня потенційної небезпеки [376].

На нашу думку, задля дослідження ризик-орієнтованої правової політики використання ШІ та побудови її теоретико-методологічної моделі доцільно використовувати ці чотири методологічні положення, визначені FATF: пріоритет попередньої оцінки ризиків перед вибором адміністративно-правових засобів реагування; принцип пропорційності державного впливу рівню ризику; динамічний (безперервний) характер оцінки ризиків; циклічність ризик-орієнтованого регулювання: ідентифікація ризиків → їх оцінка → вибір регуляторних заходів → постійний моніторинг і коригування [376].

Вчені підкреслюють, що українська практика впровадження ризик-орієнтованої моделі державного управління свідчить про поступовий перехід від застосування окремих ризик-орієнтованих інструментів у визначених сферах до формування комплексної національної системи управління ризиками, заснованої на європейських стандартах і кращих міжнародних практиках їх ідентифікації, оцінки та мінімізації. Виявлення ризиків здійснюється шляхом комплексного моніторингу, який проводять уповноважені державні органи, з метою подальшого розроблення та реалізації заходів щодо їх мінімізації на макро- та мікрорівнях. Нормативно-правова база України забезпечує правові засади застосування ризик-орієнтованого підходу, визначає механізми його реалізації, критерії оцінки ризиків і розподіляє повноваження щодо їх оцінювання між відповідними суб'єктами [58, с. 170 – 171].

Ризик-орієнтовану правову політику у сфері ШІ пропонується розуміти як системну, науково обґрунтовану діяльність держави з формування та реалізації диференційованих правових режимів, за яких зміст і інтенсивність заборон, обов'язків, процедур контролю та юридичних гарантій визначаються імовірністю, масштабом, тяжкістю й оборотністю негативного впливу конкретної системи ШІ на права людини, демократію, верховенство права, публічну та національну безпеку. Її відмінність від традиційного реагування на вже заподіяну шкоду полягає у пріоритеті превентивних засобів: попередній класифікації, оцінці впливу, тестуванні, оцінці відповідності, реєстрації,

аудиту, моніторингу та своєчасному припиненні використання небезпечної системи.

Потреба саме в ризик-орієнтованій моделі зумовлена неоднорідністю систем ШІ. Одна й та сама технологічна архітектура може використовуватися для автоматичного сортування звернень громадян, медичної діагностики, біометричної ідентифікації, прогнозування криміногенних ризиків або підтримки військового рішення. Тому правове значення має не абстрактна наявність «штучного інтелекту», а функціональне призначення системи, середовище її використання, види даних, коло осіб, рівень автономності, можливість помилки, характер юридичних наслідків і реальна спроможність людини запобігти шкоді.

Методологічним орієнтиром для України є ризикоорієнтована конструкція Регламенту (ЄС) 2024/1689, який поєднує заборону визначених практик неприйнятного ризику, спеціальні вимоги до високоризикових систем, обов'язки прозорості для окремих систем і моделей загального призначення та переважно вільне використання рішень із мінімальним ризиком. Регламент не встановлює універсальної заборони автоматизації, а диференціює вимоги залежно від функцій системи та потенційного впливу на захищені цінності [472]. Водночас, ця модель не повинна бути єдиним орієнтиром, що ми спробуємо довести у цій частині дослідження.

Правозахисний вимір європейського підходу був сформований не лише AI Act. Рекомендація CM/Rec(2020)1 Комітету Міністрів Ради Європи закріпила орієнтири пропорційності, прозорості, недискримінації, відповідальності, оцінювання впливу та доступу до ефективного засобу захисту при застосуванні алгоритмічних систем [228]. Подальшим етапом стала Рамкова конвенція Ради Європи про штучний інтелект, права людини, демократію та верховенство права, яка вимагає забезпечувати протягом життєвого циклу систем ШІ людську гідність, автономію, рівність, приватність, прозорість, нагляд, підзвітність, надійність і безпечні інновації, а також

запроваджувати процедури оцінювання ризиків, запобігання шкоді, оскарження та, за необхідності, заборони або мораторії щодо окремих застосувань [333].

Підписання Україною Рамкової конвенції та євроінтеграційний курс означають, що національна політика повинна враховувати не лише вимоги доступу продуктів до внутрішнього ринку ЄС, а й окрему правозахисну логіку Ради Європи. Водночас адаптація не повинна бути механічним копіюванням AI Act. Європейський регламент створений передусім як акт внутрішнього ринку ЄС, тоді як українська модель має додатково врахувати правовий режим воєнного стану, потреби оборони і розвідки, стан державних реєстрів, спроможність контролюючих органів, обмежені фінансові ресурси та необхідність швидкого відновлення держави.

З огляду на це до основних принципів національної ризикоорієнтованої політики доцільно віднести: 1) людиноцентризм і пріоритет основоположних прав; 2) законність і правову визначеність; 3) необхідність та пропорційність втручання; 4) превентивність і обачність; 5) технологічну нейтральність; 6) прозорість і пояснюваність у межах, сумісних із захистом таємниці та безпеки; 7) недискримінацію і якість даних; 8) змістовний людський контроль; 9) підзвітність і персоніфіковану відповідальність; 10) кіберстійкість і захист даних за проєктуванням; 11) участь зацікавлених сторін; 12) адаптивність та періодичний перегляд правових режимів; 13) підтримку безпечних інновацій.

Запропонований перелік не є декларативною етичною рамкою. Кожен принцип повинен мати процедурне продовження. Так, законність реалізується через визначену нормативну підставу та компетенцію органу; пропорційність - через перевірку мети, придатності, необхідності та менш обмежувальних альтернатив; прозорість - через документацію, повідомлення та доступ до значущої інформації; недискримінація - через аналіз репрезентативності даних і тестування упередженості; людський контроль - через право компетентної посадової особи відхилити, змінити або зупинити алгоритмічний результат; підзвітність - через журналювання, аудит і юридичну відповідальність.

Узгодження принципів із майбутньою інституційною моделлю, обґрунтованою у підрозділі 4.2, потребує функціонального розмежування трьох груп діяльності: формування державної політики, незалежного контролю за конкретними системами та розгляду індивідуальних спорів. Один і той самий орган може брати участь у кількох процесах, однак не повинен поєднувати несумісні ролі таким чином, щоб суб'єкт, який ініціював або фінансував впровадження системи, одноосібно оцінював її безпечність і вирішував скарги на власні рішення. Отже, ризикоорієнтована політика має включати не тільки матеріальні критерії допустимості, а й гарантії функціональної неупередженості адміністративних процедур.

З цієї позиції принципи правової політики доцільно перетворювати на перевірювані правила прийняття рішень. Наприклад, принцип пропорційності повинен завершуватися письмовим висновком про законну мету, придатність засобу, відсутність менш обмежувальної альтернативи та співмірність залишкового ризику; принцип прозорості – визначенням обсягу інформації для особи, аудитора і регулятора; принцип підзвітності – встановленням конкретного відповідального підрозділу та посадової особи. Така операціоналізація унеможливорює ситуацію, коли правозахисна термінологія використовується декларативно, але не впливає на допуск системи до експлуатації.

О. А. Баранов, досліджуючи правові ризики Інтернету речей, обґрунтовує необхідність переходу від реагування на наслідки до попереднього виявлення й оцінювання небезпек цифрових технологій [18, с. 47 – 49, 201 – 205]. Цей висновок повною мірою поширюється на ІІІ, оскільки автономність, масштабованість і здатність до адаптації можуть збільшувати не лише корисний ефект, а й масштаб помилки. Відтак адміністративні процедури мають охоплювати весь життєвий цикл системи - від формулювання мети та підготовки даних до виведення з експлуатації.

Ризик у запропонованій моделі слід оцінювати як поєднання щонайменше п'яти груп критеріїв. Перша група характеризує об'єкт впливу: життя і

здоров'я, свобода, приватність, рівність, майнові та соціальні права, демократичні процеси, критична інфраструктура. Друга - інтенсивність впливу: масштаб охоплення, тривалість, систематичність, можливість прихованого спостереження. Третя - технологічні властивості: рівень автономності, непрозорість, адаптивність, залежність від великих масивів даних. Четверта - процесуальний контекст: можливість людини перевірити результат, якість оскарження, оборотність рішення. П'ята - характеристики суб'єктів: вразливість дітей, пацієнтів, затриманих, отримувачів соціальної допомоги, військовослужбовців та інших осіб, які перебувають у відносинах владної або фактичної залежності.

Для уніфікації оцінювання доцільно запровадити паспорт ризику системи ІІІ як обов'язкову частину її адміністративного дос'є. У паспорті повинні фіксуватися призначення системи, правова підстава використання, суб'єкти життєвого циклу, категорії даних, потенційно зачеплені права, групи підвищеної вразливості, рівень автономності, можливі сценарії шкоди, контрольні показники, засоби людського втручання та попередня категорія ризику. Паспорт не замінює HRIA/FRIA чи оцінку відповідності, а забезпечує єдину вихідну інформацію для всіх наступних процедур і для взаємодії органів, визначених у підрозділі 4.2.

Оцінка ризику не повинна зводитися до механічного числового бала. Кількісна шкала корисна для порівняння і пріоритезації перевірок, проте окремі фактори мають характер юридичних меж, які не можуть бути компенсовані високою очікуваною ефективністю. Зокрема, імовірність порушення може бути невисокою, але незворотність позбавлення свободи, шкоди здоров'ю або дискримінаційного виключення з публічної послуги вимагає посиленого режиму. Тому матриця ризику має поєднувати кількісні показники з якісною правовою оцінкою тяжкості, незворотності та системності наслідків.

Категорія ризику повинна мати динамічний характер. Система, яка на стадії пілотування виконувала допоміжну функцію, може стати високоризиковою після масштабування, інтеграції з реєстрами, зміни моделі

або фактичного використання її результату як визначального для владного рішення. Закон доцільно доповнити обов'язком повторної класифікації після істотної модифікації, зміни мети, розширення кола осіб, підключення нових джерел даних або виявлення раніше невідомої закономірності шкоди. Невиконання такого обов'язку має розглядатися як самостійне порушення правил експлуатації.

На законодавчому рівні доцільно закріпити п'ять взаємопов'язаних категорій: 1) заборонені практики неприйнятного ризику; 2) високоризикові системи; 3) системи обмеженого ризику, для яких встановлюються спеціальні вимоги прозорості; 4) системи мінімального ризику, щодо яких діють загальні норми та добровільні стандарти; 5) моделі ШІ загального призначення, включаючи моделі із системним ризиком. Такий поділ відтворює функціональну логіку європейського регулювання, але має бути конкретизований українськими критеріями та секторальними додатками.

До неприйнятних необхідно відносити не технологію як таку, а практики, які за своєю метою або способом використання несумісні з Конституцією, правами людини та демократичним порядком. У підготовленому авторському проєкті Закону України «Про безпечне та відповідальне використання систем штучного інтелекту» (Додаток Е) запропоновано заборонити маніпулятивне або оманливе застосування ШІ, що істотно спотворює поведінку особи та спричиняє або створює реальну загрозу значної шкоди; експлуатацію вразливості особи; соціальне оцінювання громадян органами публічної влади поза чітко визначеними законом процедурами; створення баз біометричних даних шляхом невибіркового збирання зображень; категоризацію за чутливими ознаками з метою дискримінації; оцінювання ризику вчинення правопорушення виключно на підставі профілю або рис особистості; окремі форми дистанційної біометричної ідентифікації у публічному просторі без установлення законом підстави та незалежного контролю.

Формулювання законодавчої заборони повинно відповідати принципу правової визначеності, який є фундаментальною складовою верховенства права

і означає, що закони та правові акти повинні бути ясними, передбачуваними й доступними для розуміння громадянами [143]. Недостатньо назвати практику «небезпечною» або «неетичною». Закон має визначити суб'єкта, мету, спосіб обробки даних, коло винятків, процесуальні умови їх застосування, компетентний орган і правові наслідки порушення. Винятки з заборон, особливо для правоохоронної діяльності та національної безпеки, не можуть встановлюватися загальною бланкетною формулою; вони повинні бути необхідними, пропорційними, часово й предметно обмеженими та підлягати незалежному контролю.

Особливої деталізації потребує режим винятків, пов'язаних із національною безпекою, обороною та правоохоронною діяльністю. Законодавча конструкція має виходити не з презумпції повного вилучення відповідної сфери з регулювання, а з можливості застосування спеціальної закритої процедури. Рішення про виняток повинно містити посилання на конкретну норму закону, визначати мету, строк, територіальні й функціональні межі, категорії даних, відповідального суб'єкта, порядок незалежного контролю та умови припинення. Загальні формули про «інтереси держави» або «службову необхідність» не відповідають вимогам правової визначеності.

В умовах невідкладної загрози може застосовуватися прискорений порядок допуску, однак він не повинен означати відмову від документування. До початку або невідкладно після початку використання необхідно зафіксувати законну мету, доступні альтернативи, мінімальний набір тестів, модель людського контролю і строк дії рішення. Продовження експлуатації після завершення первинного строку має залежати від повної оцінки. Така конструкція дозволяє поєднати оперативність із наступним контролем і запобігає перетворенню тимчасового винятку на постійний нерегульований режим.

Високоризиковою доцільно визнавати систему, якщо вона є компонентом безпеки продукції або самостійним продуктом, що підлягає обов'язковій оцінці відповідності, або використовується у сфері, де її результат може істотно

вплинути на права, безпеку чи доступ особи до життєво важливої послуги. До таких сфер належать біометрія, критична інфраструктура, освіта, працевлаштування, соціальний захист, охорона здоров'я, правоохоронна, міграційна та прикордонна діяльність, правосуддя, виборчі процеси, а також окремі оборонні й безпекові застосування.

Водночас секторальна належність не повинна автоматично означати однаковий режим для всіх систем. Автоматичний розподіл внутрішньої кореспонденції медичного закладу не створює такого самого ризику, як алгоритмічна діагностика; система обліку навчальних матеріалів відрізняється від автоматизованого оцінювання вступника; пошук технічних помилок у судовому документі не тотожний прогнозуванню винуватості. Тому закон має передбачати можливість обґрунтованого виключення системи з високоризикової категорії, якщо вона не формує профілю особи, не приймає і не визначає зміст юридично значущого рішення та не створює істотного ризику для прав.

Рішення про віднесення системи до певної категорії ризику в публічному секторі має оформлюватися окремим мотивованим адміністративним документом або бути складовою рішення про її придбання чи введення в експлуатацію. У ньому слід зазначати фактичні характеристики системи, застосовані критерії, позиції секторальних експертів, відхилені альтернативи і правові наслідки класифікації. Такий документ необхідний не лише для внутрішнього управління, а й для подальшої перевірки регулятором, судом, органом державного фінансового контролю або Уповноваженим Верховної Ради України з прав людини.

У випадках, коли система одночасно належить до кількох сфер, наприклад поєднує медичну діагностику, обробку біометричних даних і надання адміністративної послуги, класифікація повинна здійснюватися за найбільш інтенсивним із застосовних режимів. Компетенційні розбіжності між органами не можуть використовуватися як підстава для відкладення оцінки або введення системи без контролю. До врегулювання спору має діяти тимчасовий

запобіжний режим, а центральний координатор, модель якого розкрита у підрозділі 4.2, повинен забезпечувати узгодження позицій без підміни повноважень секторальних органів.

Для систем обмеженого ризику основним регуляторним інструментом є прозорість. Особа повинна бути поінформована, що взаємодіє з ШІ; синтетичний контент має позначатися у випадках, коли його штучне походження може ввести в оману або вплинути на суспільно значущу поведінку; емоційне розпізнавання чи біометрична категоризація, якщо вони допустимі, потребують окремого повідомлення. Водночас вимоги прозорості не повинні перетворюватися на формальне повідомлення, яке не дозволяє зрозуміти роль системи та можливі наслідки.

Системи мінімального ризику доцільно залишити під дією загального законодавства про інформацію, захист даних, споживачів, авторське право, кібербезпеку та договірні відносини, доповнивши добровільними кодексами поведінки й стандартами. Такий підхід узгоджується з позицією М. В. Карчевського про недоцільність абсолютної заборони розвитку ШІ та необхідність поєднання стимулювання соціально корисного використання з мінімізацією ризиків зловживання [100].

Окремого правового режиму потребують моделі ШІ загального призначення. Їхня універсальність означає, що ризик нерідко виникає не на стадії створення базової моделі, а під час її інтеграції у конкретний продукт або публічну процедуру. Тому постачальник моделі повинен забезпечувати технічну документацію, інформацію про можливості й обмеження, політику дотримання авторського права та належну взаємодію з розробниками наступних ланок. Для моделей із системним ризиком необхідні додаткові обов'язки щодо оцінювання, тестування, кіберстійкості та повідомлення про інциденти.

Для моделей загального призначення важливо розмежовувати обов'язки постачальника базової моделі, розробника прикладної системи та розгортувача. Постачальник не завжди може передбачити всі майбутні застосування, але

зобов'язаний надати інформацію про навчання, відомі обмеження, допустимі сценарії використання, результати тестування й умови безпечної інтеграції. Розробник прикладного рішення повинен оцінити ризик конкретної функції, а розгортавав – перевірити її відповідність правовому контексту й фактичному середовищу. Розподіл ролей не повинен створювати прогалин, за яких кожен суб'єкт посилається на дії іншої ланки.

У разі системного ризику необхідним є механізм передачі інформації вздовж усього ланцюга створення й використання. Виявлений інцидент у конкретному секторі може свідчити про дефект базової моделі, актуальний для багатьох розгортавачів. Тому рамковий закон має встановити обов'язок повідомляти не лише компетентний орган, а й контрагентів наступних та попередніх ланок, забезпечувати доступ до оновлень безпеки, зберігати сумісність документації і не приховувати критичні зміни архітектури під виглядом звичайного оновлення сервісу.

Ризик-орієнтована класифікація набуває практичного значення лише через належну адміністративну процедуру. Закон України «Про адміністративну процедуру» закріплює принципи законності, обґрунтованості, пропорційності, відкритості, своєчасності, права особи бути заслуханою та обов'язок мотивувати адміністративний акт. Ці вимоги повинні застосовуватися і тоді, коли ШІ використовується для підготовки, рекомендації або фактичного визначення змісту владного рішення [186].

Перша процедура - інвентаризація та попередня класифікація. Орган публічної влади або інший розгортавач до придбання чи початку розроблення системи повинен визначити мету, функції, категорії даних, коло осіб, очікуваний рівень автономності, юридичні наслідки й попередню категорію ризику. Для органів влади інвентаризація має охоплювати також наявні системи, включаючи аналітичні модулі, які формально не називаються ШІ, але здійснюють профілювання, прогнозування або ранжування.

Друга процедура - перевірка законної мети та альтернатив. Необхідно встановити, чи має орган нормативно визначену компетенцію для використання

відповідного інструменту, чи є втручання придатним для досягнення легітимної мети, чи неможливо досягти її менш обмежувальним способом і чи не переважає ризик для особи очікувану суспільну користь. Така перевірка особливо важлива для біометричного спостереження, профілювання, прогностичної аналітики та використання даних, зібраних з іншою первинною метою.

Результати перевірки мети та альтернатив доцільно включати до єдиного адміністративного дос'є системи. У ньому мають бути пов'язані між собою обґрунтування потреби, паспорт ризику, документи закупівлі, оцінка впливу, висновок про відповідність, опис людського контролю, відомості реєстру, результати аудитів і повідомлення про інциденти. Формування єдиного дос'є не означає створення одного відкритого файлу: режим доступу до його частин може відрізнятися, але компетентний орган повинен мати можливість відновити повний ланцюг прийняття рішення.

У публічному адмініструванні обов'язок довести необхідність використання високоризикової системи має покладатися на орган, який ініціює її впровадження. Особа не повинна доводити існування менш обмежувальної альтернативи, якщо відповідна інформація перебуває виключно у володінні органу чи постачальника. За відсутності належного обґрунтування, документації або перевірюваних показників ефективності рішення про впровадження не може вважатися достатньо мотивованим. Це особливо важливо, коли аргументація зводиться до загальних посилань на економію часу чи інноваційність.

Третя процедура - оцінювання впливу високоризикової системи на основоположні права (HRIA/FRIA). Вона має передувати першому використанню системи органом публічної влади, суб'єктом, який надає публічні послуги, або іншим розгортувачем, якщо алгоритмічний результат здатний істотно вплинути на права. Оцінювання повинно бути повторним після суттєвої модифікації, зміни мети, категорій даних, масштабу використання або виявлення серйозного інциденту. Методичний матеріал Офісу Омбудсмана та

Мінцифри вже орієнтує розробників і користувачів на попередні консультації, тестування, системний моніторинг, аналіз точності, якості даних, відповідальності та захисту персональних даних [182].

Порядок проведення HRIA/FRIA доцільно затвердити постановою Кабінету Міністрів України. Розроблений проєкт такого порядку передбачає: опис системи та контексту; перевірку законної мети; аналіз менш обмежувальних альтернатив; визначення потенційно зачеплених прав і груп; оцінку якості, походження й репрезентативності даних; тестування дискримінаційного впливу; визначення людського контролю; консультації із зацікавленими сторонами; план запобігання та мінімізації ризиків; висновок про допустимість, умовну допустимість або неприпустимість використання; реєстрацію результатів та періодичний перегляд.

Участь зацікавлених сторін не повинна мати декоративного характеру. У чутливих сферах до консультацій слід залучати представників потенційно зачеплених груп, професійні об'єднання, Уповноваженого Верховної Ради України з прав людини, фахівців із захисту даних, кібербезпеки, етики, адміністративного права та відповідної галузі. Відомості, що становлять державну чи іншу охоронювану законом таємницю, можуть розглядатися у закритому режимі, але це не усуває обов'язку незалежної оцінки та документування.

Незалежність оцінювання передбачає врегулювання конфлікту інтересів. Працівники, які брали участь у розробленні технічного завдання, виборі постачальника або керуванні проєктом, можуть надавати інформацію, але не повинні одноосібно затверджувати прийнятність залишкового ризику. Для найбільш чутливих систем необхідна зовнішня експертиза або погодження секторального регулятора і правозахисного суб'єкта. Водночас залучення зовнішнього консультанта не звільняє адміністративний орган від відповідальності за остаточне рішення.

Підсумок HRIA/FRIA має містити не лише перелік виявлених ризиків, а й чітку правову кваліфікацію: допустиме використання, допустиме за визначених

умов, необхідність додаткового тестування або неприпустимість. Для умовно допустимого використання повинні визначатися строк, обмеження масштабу, контрольні показники, відповідальні особи й дата повторного перегляду. Публічна версія висновку може бути скороченою, проте має дозволяти зрозуміти мету системи, зачеплені права, основні ризики та заходи їх мінімізації.

Четверта процедура стосується управління даними. Якість системи ІІІ безпосередньо залежить від законності походження, повноти, актуальності та репрезентативності навчальних, тестових і валідаційних даних. Закон України «Про захист персональних даних» регулює автоматизовану обробку, однак не встановлює повного набору вимог до високоризикових моделей, профілювання, синтетичних даних, повторного використання масивів та алгоритмічного тестування [197]. Тому в рамковому законі і спеціальному законодавстві необхідно закріпити мінімізацію даних, визначення мети, розмежування ролей, строки зберігання, ведення документації, оцінку впливу на захист даних і право суб'єкта на ефективне заперечення.

Для органів влади особливе значення мають дані публічних електронних реєстрів. Їх використання для навчання або функціонування ІІІ має відповідати меті реєстру, правилам інформаційної взаємодії, вимогам до якості та достовірності відомостей, а також передбачати журналювання доступу. Закон України «Про публічні електронні реєстри» створює загальну інфраструктурну основу, але потребує доповнення нормами про алгоритмічне опрацювання, формування похідних профілів, виправлення помилок і незалежний аудит [208].

П'ята процедура - оцінка відповідності. Для високоризикової системи до її введення в експлуатацію необхідно перевіряти функціонування системи управління ризиками, якість даних, технічну документацію, журналювання, прозорість, людський нагляд, точність, надійність і кібербезпеку. Оцінювання може здійснюватися постачальником у випадках, визначених законом, або із залученням незалежного органу для найбільш чутливих застосувань. За

відсутності належної документації чи можливості перевірити модель система не повинна допускатися до високоризикової публічної функції.

Шоста процедура - публічна закупівля системи ІІІ. Орган влади не може переносити всі ризики на приватного постачальника або посилатися на комерційну таємницю як на підставу відмови від контролю. Тендерна документація повинна містити вимоги до класифікації ризику, доступу до технічної документації, тестування, захисту даних, кібербезпеки, сумісності, аудиту, оновлення, повідомлення про інциденти, перенесення даних і безпечного припинення використання. Договір має чітко розподіляти обов'язки постачальника та органу-розгортувача, встановлювати право на перевірку і забороняти односторонню зміну критичних параметрів без повторної оцінки.

Правове регулювання закупівлі має враховувати, що відповідно до законодавства про публічні закупівлі замовник визначає предмет, технічні специфікації та умови договору, дотримуючись принципів добросовісної конкуренції, недискримінації, відкритості й об'єктивності [209]. Для систем ІІІ ці принципи вимагають уникати специфікацій, які без об'єктивної потреби прив'язують орган до закритої платформи або конкретного постачальника. Водночас вимога відкритості не означає обов'язкового оприлюднення інформації, розкриття якої створює реальну кібербезпекову загрозу; обмеження має бути конкретним і не перешкоджати контролю уповноважених органів.

У договорі на створення або постачання високоризикової системи необхідно визначати права на технічну документацію, доступ до журналів, порядок незалежного тестування, обов'язок повідомляти про зміни моделі та вразливості, строки виправлення, умови оновлення, відповідальність за приховані дефекти, можливість перенесення даних і порядок безпечного завершення співпраці. Окремою умовою має бути заборона використовувати дані органу або осіб для додаткового навчання моделі без самостійної правової підстави та документованого погодження.

До оцінки пропозиції доцільно включати вартість усього життєвого циклу, а не тільки початкову ціну. Система з нижчою закупівельною вартістю

може створювати значні витрати на ліцензії, обчислювальні ресурси, оновлення, аудит, навчання персоналу або вихід із платформи. Такий аналіз знижує ризик технологічної залежності й дозволяє ще до укладення договору перевірити, чи спроможний замовник виконувати обов'язки розгортувача, передбачені рамковим законопроектом.

Сьома процедура - державна реєстрація. Публічний реєстр високоризикових систем має забезпечувати суспільну прозорість, не розкриваючи даних, що створюють реальну загрозу безпеці або порушують права третіх осіб. До відкритої частини доцільно включати назву та мету системи, постачальника і розгортувача, сферу використання, категорію ризику, правову підставу, статус оцінки відповідності та стислий опис людського контролю. Закрита частина може містити технічну документацію, моделі загроз, дані про вразливості та системи оборони, розвідки й національної безпеки. Розроблений проєкт урядової постанови (Додаток Е) передбачає також строки оновлення відомостей і аудит операцій із реєстром.

Державний реєстр має функціонувати не як ізольована база даних, а як інформаційна основа координації між центральним компетентним органом, секторальними регуляторами, Уповноваженим Верховної Ради України з прав людини та органами державного фінансового контролю. Внесення або зміна відомостей повинні автоматично формувати повідомлення тим органам, компетенція яких пов'язана зі сферою використання, видом даних чи характером ризику. Водночас сам факт реєстрації не створює дозволу і не перешкоджає подальшій перевірці.

Обсяг відкритої інформації має визначатися з урахуванням Закону України «Про доступ до публічної інформації» та трискладового тесту обмеження доступу [190]. Необхідно розмежовувати відомості про існування системи, її мету, правову підставу та суб'єктів, які становлять суспільний інтерес, і технічні деталі, здатні створити загрозу безпеці. Навіть якщо повна документація є закритою, суспільство повинно отримувати узагальнену

інформацію про категорію ризику, проведені оцінки, серйозні інциденти й застосовані коригувальні заходи.

Восьма процедура - забезпечення змістовного людського контролю. Людина в контурі прийняття рішення не повинна бути формальним підтверджувачем автоматичного результату. Вона має володіти достатньою компетентністю, мати доступ до релевантної інформації, розуміти можливості й обмеження системи, бути здатною виявити автоматизаційне упередження, не врахувати, змінити або скасувати результат та безпечно зупинити систему. Відповідальність за адміністративний акт або інше юридично значуще рішення залишається за уповноваженою особою чи органом, а не перекладається на алгоритм.

У публічному управлінні ця вимога кореспондує з обов'язком адміністративного органу самотійно дослідити обставини, вислухати особу, мотивувати рішення та діяти в межах дискреції. Науковці адміністративно-правової спрямованості справедливо наголошують, що впровадження ІІІ у публічне управління може підвищувати ефективність, але створює ризики дискримінації, непрозорості та неправомірного втручання в приватність [238]. Отже, алгоритмічний результат має використовуватися як доказове або аналітичне джерело, а не як суб'єкт владного волевиявлення.

Змістовний людський контроль має бути закріплений не лише як властивість системи, а і як організаційна функція. Орган повинен визначити посади, які мають право підтверджувати, відхиляти чи зупиняти алгоритмічний результат, вимоги до їх компетентності, порядок заміщення та межі персональної відповідальності. Неприпустимою є модель, за якої працівник формально відповідає за рішення, але не має доступу до пояснення, часу для перевірки або повноваження відступити від рекомендації системи.

Позиція М. В. Карчевського про конвергенцію юридичних і технічних компетентностей та необхідність технологічно нейтрального законодавства підтверджує, що підготовка персоналу має бути постійним елементом правової політики, а не одноразовим навчанням перед запуском системи [94]. Програма

підготовки повинна охоплювати правову підставу використання, межі точності, типові помилки, автоматизаційне упередження, захист даних, фіксацію відхилення від алгоритмічної рекомендації та порядок ескалації інциденту.

Дев'ята процедура - постійний моніторинг після введення в експлуатацію. Постачальник і розгортувач повинні збирати дані про точність, відмови, зміни в середовищі, дрейф моделі, скарги, дискримінаційні наслідки та інші відхилення. Правовий моніторинг не зводиться до технічного спостереження: він має оцінювати, чи зберігається законна мета, чи не змінився фактичний спосіб використання, чи є ефективним людський контроль і чи відповідають реальні наслідки результатам початкової HRIA/FRIA.

Десята процедура - повідомлення про серйозні інциденти. Попереднє повідомлення має подаватися без невиправданої затримки після виявлення події, що спричинила смерть, значну шкоду здоров'ю, істотне порушення прав, серйозну кібербезпекову подію, дискримінацію значної кількості осіб або збій критичної інфраструктури. Повний звіт повинен містити причини, масштаби, постраждалих, ужиті заходи, план усунення та висновок щодо повторного використання. Уповноважений орган повинен мати право вимагати зупинення, обмеження, відкликання або повторної оцінки системи.

Єдина процедура повідомлення про інциденти повинна бути узгоджена з кібербезпековими, персонально-даними, медичними та іншими секторальними режимами. Одне порушення може одночасно становити витік даних, дефект високоризикової системи та підставу для перегляду адміністративних актів. Тому первинне повідомлення має надходити до єдиного контактного пункту або бути автоматично маршрутизоване компетентним органам, а суб'єкт не повинен подавати суперечливі звіти за різними формами без об'єктивної необхідності.

Класифікація серйозності інциденту має враховувати не тільки кількість постраждалих, а й характер права, тривалість наслідків, повторюваність, прихованість та можливість поширення дефекту на інші системи. Після інциденту необхідно забезпечити збереження журналів, версії моделі, наборів

вхідних даних і рішень посадових осіб, щоб уникнути втрати доказів через автоматичне оновлення. Особи, права яких могли бути істотно зачеплені, повинні отримувати повідомлення в обсязі, необхідному для звернення за захистом, якщо таке інформування не створює конкретної й переважаючої загрози.

Одинадцята процедура - застосування коригувальних заходів. Реагування має бути пропорційним: від припису усунути недоліки, обмежити функцію або провести повторний аудит до тимчасового зупинення, відкликання з експлуатації, заборони практики та застосування фінансової санкції. Для органів публічної влади додатково мають наставати дисциплінарні й адміністративно-правові наслідки, а незаконний адміністративний акт, істотно зумовлений дефектною системою ШІ, підлягає скасуванню або перегляду.

Дванадцята процедура - забезпечення індивідуальних прав. Особа повинна мати право знати про істотне використання ШІ, отримати зрозумілу інформацію про роль системи та основні фактори рішення, вимагати перегляду компетентною людиною, подавати заперечення, виправляти некоректні дані та оскаржувати як кінцеве рішення, так і неправомірне використання системи. Рамкова конвенція Ради Європи прямо пов'язує документування та доступ до інформації з реальною можливістю оскаржити рішення або саме використання системи [333].

Реалізація права на пояснення не означає обов'язкового розкриття вихідного коду або всієї комерційно чутливої документації. Змістовним є пояснення, яке дозволяє зрозуміти мету, роль системи, основні категорії даних, вирішальні фактори, межі точності, можливі наслідки та порядок перегляду. Баланс із державною таємницею, таємницею досудового розслідування, комерційною таємницею і кібербезпекою повинен досягатися через диференційований доступ, незалежний контроль і закриті процедури, а не через повне усунення підзвітності.

У процедурах адміністративного та судового оскарження алгоритмічна документація повинна розглядатися як частина матеріалів справи. Якщо орган

посилається на результат системи, він має надати достатні відомості для перевірки його релевантності, достовірності та способу використання. Комерційна закритість системи не може погіршувати становище особи: у разі неможливості розкрити інформацію безпосередньо учаснику необхідно забезпечити її дослідження судом, незалежним експертом або уповноваженим органом у закритому режимі. Ризик недоведеності належного функціонування системи повинен нести суб'єкт, який обрав її для здійснення владної функції.

Окремим інструментом має бути регуляторне експериментальне середовище. Українська Біла книга передбачає поетапний bottom-up підхід: формування культури саморегулювання, рекомендацій, оцінювання ризиків, адаптацію HUDERIA та Sandbox із подальшим ухваленням закону, наближеного до AI Act [153]. Важливо акцентувати, що значення HUDERIA полягає у тому, що вона виступає інструментом реалізації міжнародних стандартів, закріплених у Рамковій конвенції Ради Європи про штучний інтелект, Рекомендації CM/Rec(2020)1 та інших актах, які передбачають необхідність оцінювання впливу систем штучного інтелекту на права людини, демократію і верховенство права [153]. У цьому контексті HUDERIA слід розглядати як процедурний інструмент механізму адміністративно-правового регулювання, що забезпечує практичну реалізацію встановлених законом обов'язків щодо оцінювання ризиків та прийняття адміністративних рішень. Стрімке впровадження технологій штучного інтелекту у сферу публічного управління зумовлює необхідність формування цілісної та науково обґрунтованої системи управління пов'язаними ризиками, заснованої на ризик-орієнтованому та людиноцентричному підходах. Методологія HUDERIA є однією з найбільш комплексних моделей оцінювання ризиків штучного інтелекту, оскільки інтегрує правові, етичні й технологічні аспекти в єдину аналітичну систему та забезпечує оцінювання впливу AI-систем на права людини, демократію і верховенство права протягом усього їх життєвого циклу [334].

У цьому контексті HUDERIA слід розглядати як процедурний інструмент механізму адміністративно-правового регулювання, що забезпечує практичну реалізацію встановлених законом обов'язків щодо оцінювання ризиків та прийняття адміністративних рішень. Стрімке впровадження технологій штучного інтелекту у сферу публічного управління зумовлює необхідність формування цілісної та науково обґрунтованої системи управління пов'язаними ризиками, заснованої на ризик-орієнтованому та людиноцентричному підходах. Методологія HUDERIA є однією з найбільш комплексних моделей оцінювання ризиків штучного інтелекту, оскільки інтегрує правові, етичні й технологічні аспекти в єдину аналітичну систему та забезпечує оцінювання впливу AI-систем на права людини, демократію і верховенство права протягом усього їх життєвого циклу.

Попри існування різних міжнародних підходів до оцінювання ризиків штучного інтелекту, саме модель HUDERIA вирізняється системністю, високим рівнем інтеграції правозахисних стандартів та адаптованістю до застосування у сфері публічного управління. Водночас в Україні наразі відсутні інституціоналізовані механізми використання таких моделей, що зумовлює дисбаланс між темпами цифрової трансформації та спроможністю держави забезпечити безпечне, етичне й правомірне використання систем штучного інтелекту.

У зв'язку з цим доцільна імплементація методології HUDERIA до національної системи публічного управління як одного з ключових елементів формування сучасної моделі AI governance, що відповідає європейським стандартам.

Такий підхід є виправданим для підготовки індустрії та регулятора, але не може замінити обов'язкові правила щодо неприйнятності й високого ризику.

Розроблений автором проєкт Порядку функціонування регуляторного експериментального середовища (Додаток Е) передбачає добровільність, обмеженість строку, індивідуальний план випробування, попередню оцінку ризику, визначення метрик, нагляд, захист персональних даних і публічний

звіт. До Sandbox не повинні допускатися проекти, метою або неминучим результатом яких є заборонена практика, а також випробування без належної згоди чи правової підстави. Участь у середовищі не звільняє від відповідальності та не створює презумпції законності подальшого масового використання.

Управління регуляторним експериментальним середовищем має відповідати інституційній моделі. Мінцифри може забезпечувати методичну координацію та взаємодію з інноваційними суб'єктами, однак рішення про допустимість ризику, зупинення випробування або необхідність повідомлення про інцидент повинно прийматися за участю функціонально незалежного наглядового органу і відповідного секторального регулятора. Це усуває конфлікт між завданням підтримки інновацій та обов'язком захисту прав.

Вихід із Sandbox має завершуватися стандартизованим звітом про перевірені гіпотези, фактичні ризики, точність, виявлені групові відмінності, ефективність людського контролю та виконання умов випробування. Знеособлені висновки доцільно оприлюднювати, щоб результати експерименту використовувалися для вдосконалення методик і не залишалися приватною перевагою окремого учасника. Негативний результат випробування є правомірним результатом регуляторного експерименту і не повинен приховуватися або автоматично тлумачитися як заборона будь-яких подальших розробок.

План заходів з реалізації Концепції розвитку ІІІ на 2025–2026 роки підтверджує перехід державної політики до практичної фази: до IV кварталу 2026 року передбачено розроблення законопроекту щодо правового врегулювання у сфері ІІІ, підготовку рекомендацій із кібербезпеки, оцінювання захищеності систем, методичних рекомендацій для вищої освіти, використання ІІІ у державному управлінні, прийняття міжнародних стандартів як національних та заходи у сфері оборони [194]. Водночас План не визначає завершеної системи правових режимів і процедур, тому його реалізація має бути узгоджена з рамковим законом та підзаконними актами.

Концепція розвитку штучного інтелекту 2020 року залишається стратегічним вихідним документом, проте її переважно стимулюючий характер і відсутність законодавчої класифікації ризиків не відповідають сучасному етапу [215]. Доцільним є її оновлення через включення окремого розділу про загальні обмеження, принципи, заборонені практики, високоризикові сфери, людський контроль, оцінку впливу та систему моніторингу. При цьому стратегічний документ має визначати цілі й напрями, а конкретні права, обов'язки, процедури та санкції - встановлюватися законом і актами, прийнятими на його виконання.

Для практичної реалізації ризикоорієнтованої політики запропоновано багаторівневий пакет нормативно-правових актів. Його перший рівень становить рамковий Закон України «Про безпечне та відповідальне використання систем штучного інтелекту», який має закріпити терміни, принципи, категорії ризику, заборонені практики, вимоги до високоризикових систем, обов'язки постачальників і розгортувачів, права осіб, державний нагляд, заходи реагування та особливості воєнного стану. Другий рівень - зміни до законів про адміністративну процедуру, персональні дані, доступ до публічної інформації, публічні електронні реєстри, адміністративні послуги, закупівлі та кібербезпеку. Третій - урядові порядки проведення HRIA/FRIA, ведення реєстру і повідомлення про інциденти, а також функціонування Sandbox.

Узгодженість трирівневого пакета потребує чіткого розмежування предмета закону і підзаконного регулювання. Рамковий закон повинен визначати права та обов'язки, категорії ризику, заборонені практики, основні повноваження органів, види заходів реагування, права на оскарження і межі делегування. Постанови Кабінету Міністрів можуть деталізувати послідовність дій, форми документів, строки, технічні параметри інформаційної взаємодії та методики, але не створювати нові підстави для обмеження прав або нові санкції.

Розподіл повноважень має узгоджуватися із Законом України «Про центральні органи виконавчої влади», який розмежовує формування державної політики міністерствами та виконання окремих функцій з її реалізації іншими центральними органами виконавчої влади [219]. Тому в законопроекті доцільно відмежувати стратегічну й методичну роль Мінцифри від функцій незалежної перевірки, застосування приписів і санкцій. Така конструкція не применшує координаційної ролі міністерства, а запобігає конфлікту між стимулюванням впровадження ІІІ та контролем за законністю конкретних систем.

Пакет актів має містити правила вирішення колізій. Загальні положення рамкового закону застосовуються до всіх систем, тоді як секторальне законодавство встановлює додаткові вимоги, обумовлені характером сфери. Виконання технічного регламенту не звільняє від HRIA/FRIA; дотримання правил захисту даних не замінює перевірки дискримінаційного впливу; реєстрація не замінює оцінки відповідності; участь у Sandbox не усуває відповідальності. Ці правила доцільно прямо закріпити, щоб уникнути конкуренції режимів і вибіркового застосування найбільш зручного набору вимог.

Зазначена система має особливе значення для спеціальності 12.00.07. Інформаційно-правовий компонент охоплює режими даних, доступ до інформації, прозорість, журналювання, кібербезпеку, конфіденційність і якість інформаційних ресурсів. Адміністративно-правовий - компетенцію, процедури допуску, оцінку відповідності, реєстрацію, контроль, приписи, зупинення системи, адміністративне оскарження та відповідальність. Їх поєднання дозволяє розглядати обмеження ІІІ не як окрему заборону, а як функціонуючий механізм публічного адміністрування.

Положення про рівні правової політики, сформульовані І. В. Арістовою у дослідженні державної інформаційної політики, підтверджують необхідність поєднання концептуально-доктринального, нормативно-правового, інституційно-організаційного та правозастосовного компонентів [8, с. 90 – 116]. Подібну логіку простежує П. Л. Фріс, який розмежовує науковий, законодавчий

та правореалізаційний рівні правової політики [261, с. 18 – 20]. Для сфери ІІІ ця модель означає, що наукові критерії ризику мають бути трансформовані в норми, а норми - забезпечені процедурами, компетентними суб'єктами та практикою контролю.

На науковому рівні необхідно виробити уніфікований понятійний апарат, критерії неприйнятності, високого та системного ризику, методологію HRIA/FRIA, стандарти змістовного людського контролю й оцінки алгоритмічної дискримінації. На законодавчому рівні ці результати мають бути перетворені на чіткі заборони, обов'язки, права, процедури та заходи відповідальності. На правозастосовному рівні необхідні інвентаризація систем, аудит, моніторинг, розгляд скарг, розслідування інцидентів і накопичення практики, яка дозволить періодично коригувати нормативну модель.

Секторальна конкретизація політики повинна здійснюватися на основі єдиного горизонтального каркасу. У сфері оборони центральними є змістовний людський контроль, відповідність міжнародному гуманітарному праву та спеціальний режим секретності; в охороні здоров'я - клінічна валідація, інформована згода, медичні дані та розподіл відповідальності; у правоохоронній і розвідувальній діяльності - судовий та парламентський контроль, обмеження біометричного спостереження і профілювання; у правосудді - незалежність судді, процесуальна рівність і заборона підміни судового розсуду; в освіті - права здобувачів, академічна доброчесність і людський перегляд оцінювання. Детальне обґрунтування цих режимів наведено у розділі 3, тому завдання підрозділу 4.1 полягає у визначенні спільних процедурних засад.

Особливості воєнного стану не повинні оформлюватися як загальне вилучення оборони, розвідки й національної безпеки з правового регулювання. У цих сферах може бути обмежено публічність реєстру, відкритість технічної документації та коло учасників консультацій, застосовано прискорені процедури або спеціальні органи оцінювання. Проте незмінними мають залишатися законна мета, необхідність і пропорційність, документування,

змістовний людський контроль, кібербезпека, фіксація інцидентів, персональна відповідальність і незалежний контроль у формі, сумісній із захистом таємниці.

Сучасні дослідження використання ІІІ у системі управління Збройних Сил України також підтверджують необхідність спеціального правового механізму, який поєднує оперативну ефективність із правовими, етичними та безпековими гарантіями [260]. Національна політика має розмежовувати допоміжні аналітичні системи, засоби розвідки та логістики, системи підтримки командних рішень і автономні засоби, здатні до вибору та ураження цілі. Що вищий рівень автономності й незворотності наслідку, то жорсткішим має бути режим допуску і контролю.

У межах процедурної моделі принципово важливо розмежувати три види оцінювання, які мають різний предмет і не повинні підміняти один одного. Оцінка впливу на захист персональних даних зосереджується на законності та ризиках обробки даних; HRIA/FRIA охоплює ширший спектр прав, демократію та верховенство права; оцінка відповідності перевіряє виконання технічних і організаційних вимог до самої системи. Для високоризикової системи орган публічної влади може бути зобов'язаний провести всі три процедури, але їх результати доцільно об'єднувати в єдиному досьє, щоб уникнути формального дублювання та суперечливих висновків.

Попередня оцінка повинна починатися ще до публічної закупівлі або укладення договору на розроблення. Інакше орган влади опиняється у ситуації технологічної та договірної залежності, коли після придбання закритої системи фактично неможливо забезпечити аудит, змінити постачальника або отримати належне пояснення. Тому до обґрунтування закупівлі необхідно включати оцінку потреби, ризику, сумісності з чинними реєстрами, вартості всього життєвого циклу, можливості міграції даних і припинення використання без втрати критичної функції.

Особливим елементом оцінки має бути аналіз автоматизаційного упередження - схильності посадової особи некритично приймати результат системи як більш точний або об'єктивний лише через його технологічне

походження. Запобігання цьому ризику потребує не тільки інструкції про людський контроль, а й організаційного розподілу відповідальності, регулярного навчання, перевірки рішень вибіркоким аудитом і заборони оцінювати ефективність працівника виключно за ступенем погодження з алгоритмом.

Алгоритмічний аудит доцільно поділяти на внутрішній, незалежний і регуляторний. Внутрішній аудит є постійною функцією постачальника та розгортувача; незалежний проводиться акредитованим або іншим компетентним суб'єктом у випадках, визначених законом; регуляторний здійснюється в межах державного нагляду, за скаргою чи після інциденту. Предметом аудиту мають бути не лише точність моделі, а й законність мети, походження даних, упередженість, документація, фактичні практики використання, людський контроль та виконання попередніх рекомендацій.

Технічні стандарти можуть деталізувати вимоги до систем управління ризиками, якості, кібербезпеки, точності та тестування, однак не повинні самостійно визначати межі втручання у права людини. Включення Планом заходів на 2025–2026 роки міжнародних стандартів ISO/IEC до переліку актів, які мають бути прийняті як національні, є важливим кроком для технологічної сумісності. Проте презумпція відповідності стандарту не може легалізувати заборонену практику або усунути обов'язок провести оцінку пропорційності конкретного використання [194].

Інтеграція систем ШІ до національної системи технічного регулювання має враховувати чинні закони про технічні регламенти та оцінку відповідності, стандартизацію й акредитацію органів з оцінки відповідності [217]. Вони створюють базові організаційні конструкції для призначення, акредитації, апеляції та контролю діяльності органів оцінки. Водночас специфіка ШІ потребує додаткових критеріїв компетентності: здатності оцінювати дані, моделі, кіберстійкість, алгоритмічну упередженість, людський контроль і фактичне функціонування після введення в експлуатацію.

Стандарти повинні виконувати допоміжну функцію доказування належної організації процесів, але не підміняти правову оцінку. Сертифікована система управління ризиками не доводить пропорційності конкретного біометричного спостереження, а відповідність технічним показникам точності не усуває дискримінаційного характеру мети. Тому презумпція відповідності стандарту має бути спростовною, а регулятор і суд повинні зберігати повноваження оцінювати реальне використання системи та її наслідки.

Прозорість доцільно будувати за багаторівневою моделлю. Перший рівень - інформація для кожної особи про факт і роль використання ШІ. Другий - розширена інформація для особи, щодо якої прийнято юридично значуще рішення. Третій - технічна й організаційна документація для аудитора та регулятора. Четвертий - публічні відомості про високоризикові системи, результати оцінки впливу і серйозні інциденти. Така модель дозволяє поєднати право на інформацію із захистом комерційної таємниці, безпеки та інтелектуальної власності.

Зміни до Закону України «Про адміністративну процедуру» мають прямо визначити, що використання системи ШІ не змінює суб'єкта владної компетенції та не звільняє адміністративний орган від відповідальності за рішення. Особі слід повідомляти про істотну роль системи; матеріали справи мають містити документовані результати, достатні для перевірки; посадова особа повинна оцінювати їх поряд з іншими доказами; у разі заперечення особи має забезпечуватися повторний перегляд без автоматичного відтворення попереднього результату.

Право на перегляд людиною буде формальним, якщо особа, яка здійснює перегляд, не має повноваження змінити рішення або не отримує інформації, достатньої для його критичної оцінки. Тому законодавство повинно вимагати функціональної незалежності перегляду, доступу до документації, можливості залучення експерта та заборони покладати на заявника обов'язок довести технічну помилку закритої системи. У справах, де алгоритмічна непрозорість

створена органом або постачальником, ризик недоведеності не повинен повністю переноситися на особу.

Окремі гарантії необхідні для вразливих груп. Система, яка формально демонструє однакову середню точність, може систематично помилятися щодо осіб певної статі, віку, інвалідності, етнічного походження або мовної групи. Тому оцінювання має проводитися за релевантними підгрупами, а відсутність достатніх даних про точність для конкретної групи повинна розглядатися як фактор підвищеного ризику, а не як доказ нейтральності системи.

Система заходів реагування має враховувати характер суб'єкта та наслідки порушення. Для приватного постачальника можуть застосовуватися фінансові санкції, обмеження введення в обіг і обов'язок відкликання. Для органу влади ключовими є припинення незаконної практики, скасування або перегляд рішень, відновлення прав, дисциплінарна відповідальність посадових осіб і відшкодування шкоди. У найбільш небезпечних випадках можливе застосування кримінально-правових норм, але криміналізація не повинна замінювати превентивний адміністративний контроль.

Ризикоорієнтована політика потребує узгодження із суміжними режимами - захистом персональних даних, кібербезпекою, технічним регулюванням, медичними виробами, захистом прав споживачів, адміністративною процедурою та публічними закупівлями. Рамковий закон має виконувати координаційну функцію: визначати загальні правила і прямо встановлювати, які спеціальні акти застосовуються кумулятивно. Це дозволить уникнути помилкової практики, за якої виконання одного набору вимог сприймається як звільнення від інших.

Координаційна функція рамкового закону повинна реалізовуватися через карту застосовного законодавства. Для кожної категорії систем доцільно визначити базові й додаткові режими: адміністративну процедуру, персональні дані, публічні реєстри, кібербезпеку, технічне регулювання, публічні закупівлі, захист споживачів та відповідний секторальний акт. Така карта може бути

додатком до закону або офіційною методикою, але не повинна змінювати встановлені законом права й обов'язки.

Зв'язок із підрозділом 4.2 полягає в тому, що кожен процедурний обов'язок повинен мати визначеного носія компетенції. Попередню класифікацію здійснює постачальник або розгортувач; секторальний орган перевіряє спеціальні вимоги; національний компетентний орган уніфікує практику та застосовує загальні заходи реагування; Уповноважений здійснює правозахисний контроль; суд перевіряє законність остаточного рішення. Без такого розподілу навіть детально сформульована процедура залишатиметься декларативною.

Запровадження нових обов'язків має бути поетапним. На першому етапі доцільно провести інвентаризацію систем у публічному секторі, затвердити методики та пілотні процедури; на другому - запустити обов'язкову класифікацію, HRIA/FRIA і реєстр для нових систем; на третьому - поширити вимоги на системи, які вже використовуються, із визначеним строком приведення у відповідність; на четвертому - забезпечити повну взаємодію з європейськими механізмами оцінки, стандартизації та нагляду. Перехідні строки не повинні стосуватися практик, які є неприйнятними за своєю природою.

Пропорційність перехідних обов'язків має враховувати не лише розмір суб'єкта, а й ризик системи. Для малого розробника низькоризикового рішення доцільні типові форми, консультаційна допомога і добровільні стандарти. Натомість використання високоризикової системи органом публічної влади не може звільнятися від оцінювання через брак власних фахівців; у такому разі держава повинна забезпечити спільні експертні центри, централізовані методики або залучення акредитованих суб'єктів. Обмеженість ресурсів є підставою для організаційної підтримки, а не для зниження правових гарантій.

Правова політика повинна бути доказовою та динамічною. Переліки високоризикових систем, методики оцінювання, стандарти точності й кібербезпеки не можуть залишатися незмінними за умов стрімкого

технологічного розвитку. Водночас їх оновлення не повинно здійснюватися лише відомчими листами або неpubлічними технічними рішеннями. Закон має встановити критерії та межі делегування, процедури консультацій, оприлюднення, оцінку регуляторного впливу і перехідні строки.

Періодичний перегляд доцільно проводити на підставі правового моніторингу, який охоплює дані державного реєстру, звіти про інциденти, результати аудитів, судову й адміністративну практику, інформацію Уповноваженого Верховної Ради України з прав людини, секторальних регуляторів, розробників, користувачів і громадянського суспільства. Такий моніторинг дозволяє встановлювати нові ризики, скасовувати неефективні вимоги та підтримувати інновації без зниження рівня захисту.

Ефективність політики доцільно оцінювати за системою юридично значущих індикаторів. До них належать кількість інвентаризованих і класифікованих систем, частка завершених HRIA/FRIA, строки реагування на інциденти, кількість переглянутих рішень, виконання приписів, частота повторних порушень, розподіл помилок між групами, доступність людського перегляду, результати судового контролю та витрати на виконання вимог. Саме по собі зростання кількості зареєстрованих систем або перевірок не свідчить про ефективність без оцінки фактичного відновлення прав і зменшення ризику.

Річний цикл правового моніторингу повинен завершуватися публічним узагальненим звітом і планом коригування політики. У звіті слід відображати типові порушення, нові категорії ризику, практику секторальних органів, результати оскарження, проблеми стандартів і потреби в законодавчих змінах. За наявності системного ризику перегляд не повинен відкладатися до планової дати. Водночас будь-яке посилення обмежень має проходити процедуру обґрунтування, консультацій і оцінки регуляторного впливу, щоб адаптивність не перетворилася на непередбачуваність.

Водночас аналіз положень AI Act свідчить, що європейська модель класифікує системи штучного інтелекту переважно за функціональним

критерієм, тобто залежно від сфери їх застосування, призначення або виду діяльності, у якій вони використовуються.

Такий підхід є ефективним для цілей гармонізації внутрішнього ринку Європейського Союзу, однак він не повною мірою враховує особливості побудови національної системи адміністративно-правового регулювання України, яка ґрунтується на конституційній ієрархії соціальних цінностей, принципі верховенства права, людиноцентризмі та пріоритетності забезпечення національної безпеки в умовах триваючої збройної агресії.

На нашу думку, адміністративно-правова оцінка допустимості використання систем штучного інтелекту повинна здійснюватися не лише з урахуванням технічних характеристик відповідної системи або сфери її застосування, а насамперед залежно від ступеня потенційного впливу на об'єкти адміністративно-правової охорони, які мають різний рівень правової цінності. Саме тому пропонується запровадити аксіологічний ризик-орієнтований тест адміністративно-правової оцінки використання систем штучного інтелекту, який ґрунтується на ієрархії конституційних та міжнародно визнаних правових благ.

Запропонований тест передбачає чотири послідовні рівні оцінювання ризику. На першому рівні визначається наявність потенційної загрози життю та здоров'ю людини як найвищій соціальній цінності; на другому – оцінюється можливий вплив системи штучного інтелекту на національну безпеку та функціонування держави; на третьому – встановлюється ступінь ризику для реалізації прав, свобод і законних інтересів людини; на четвертому – оцінюється потенційний вплив системи штучного інтелекту на функціонування демократичного врядування, забезпечення принципу верховенства права та інституційну спроможність держави. Кожен наступний рівень застосовується лише за відсутності підстав для віднесення системи до попереднього, більш небезпечного рівня ризику.

Саме така модель, на відміну від функціональної класифікації AI Act, дозволяє сформувати універсальний механізм адміністративно-правової оцінки

будь-якої системи штучного інтелекту незалежно від сфери її застосування та забезпечує пріоритетний захист тих суспільних цінностей, які Конституція України та міжнародне право визнають найвищими.

Перший рівень запропонованого аксіологічного тесту становить оцінка ризику заподіяння шкоди життю та здоров'ю людини. Саме цей критерій повинен мати найвищий пріоритет під час визначення допустимості використання систем штучного інтелекту, оскільки життя та здоров'я людини посідають найвищий щабель у системі правових цінностей як міжнародного, так і національного права.

Аксіологічною основою такого підходу виступає міжнародно-правова концепція невід'ємності права на життя. Так, ст. 3 Загальної декларації прав людини проголошує, що кожна людина має право на життя, свободу та особисту недоторканність [81]. Аналогічний підхід закріплено у статті 6 Міжнародного пакту про громадянські і політичні права, відповідно до якої право на життя є невід'ємним правом кожної людини і підлягає охороні законом [150]. Стаття 2 Конвенції про захист прав людини і основоположних свобод визначає право на життя як одну з фундаментальних гарантій демократичного суспільства, покладаючи на державу не лише обов'язок утримуватися від свавільного позбавлення життя, а й позитивний обов'язок створювати ефективні механізми його захисту [113]. Аналогічні положення містяться у статті 2 Хартії основоположних прав Європейського Союзу.

Конституційне закріплення відповідної ієрархії правових благ знайшло своє відображення у статті 3 Конституції України, відповідно до якої людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю [115]. Саме ця конституційна норма визначає людиноцентричну спрямованість усієї системи правового регулювання та встановлює пріоритет захисту життя і здоров'я людини перед будь-якими іншими публічними чи приватними інтересами.

У зв'язку з цим адміністративно-правове регулювання використання штучного інтелекту повинно виходити з презумпції абсолютного пріоритету

безпеки людини. Якщо функціонування систем ШІ потенційно здатне створити ризик заподіяння шкоди життю або здоров'ю людини, така система незалежно від сфери застосування повинна підлягати максимальному рівню державного контролю, спеціальним процедурам оцінки відповідності, обов'язковому людському контролю, постійному моніторингу функціонування та, у разі неможливості усунення відповідного ризику, забороні її використання.

Запропонований підхід принципово відрізняється від функціональної моделі AI Act. Якщо європейське законодавство визначає високий рівень ризику переважно через сферу застосування системи, то запропонована модель виходить із того, що визначальним критерієм має бути не місце використання технології, а ступінь потенційного впливу на життя і здоров'я людини як найвищу конституційну цінність. «Згідно дослідження міжнародного аналітичного агентства Global Market Insights, з 2017 по 2024 р. очікується щорічне зростання використання штучного інтелекту у сфері охорони здоров'я аж 40%» [146]. Наприклад, система штучного інтелекту, яка використовується у сфері охорони здоров'я виключно для адміністративного планування, може не створювати безпосередньої загрози життю людини, тоді як автономна система керування транспортними засобами, роботизована хірургічна платформа чи алгоритм управління критичною інфраструктурою здатні безпосередньо впливати на життя та фізичну безпеку людини незалежно від формальної категорії, до якої їх віднесено законодавством.

Саме тому перший рівень запропонованого тесту повинен виконувати функцію абсолютного фільтра допустимості використання систем штучного інтелекту. За наявності обґрунтованого ризику заподіяння шкоди життю чи здоров'ю людини подальше оцінювання за іншими рівнями тесту втрачає самостійне значення, оскільки правове регулювання має бути спрямоване насамперед на усунення або мінімізацію саме цього ризику.

Другим рівнем запропонованого аксіологічного ризик-орієнтованого тесту є встановлення потенційного впливу систем штучного інтелекту на національну безпеку та стійкість держави. Необхідність виокремлення цього

рівня обумовлена тим, що окремі системи штучного інтелекту, не створюючи безпосередньої загрози життю чи здоров'ю конкретної особи, здатні істотно впливати на функціонування державних інституцій, критичної інфраструктури, обороноздатності, інформаційного суверенітету та інших складових національної безпеки.

На відміну від першого рівня тесту, який спрямований на захист абсолютної конституційної цінності – життя і здоров'я людини, другий рівень орієнтований на забезпечення стабільності функціонування держави як необхідної передумови реалізації прав людини, підтримання конституційного ладу та гарантування публічного інтересу. У цьому контексті національна безпека розглядається не як самостійна політична категорія, а як об'єкт адміністративно-правової охорони, що потребує спеціальних механізмів правового забезпечення у процесі використання систем штучного інтелекту.

Підґрунтям для такого підходу є норми міжнародного та національного права. Відповідно до статті 2 Статуту Організації Об'єднаних Націй однією з основоположних засад міжнародного правопорядку є принцип суверенної рівності держав, поваги до їх територіальної цілісності та політичної незалежності [241]. Ці принципи визначають обов'язок держав створювати ефективні механізми захисту власного суверенітету від новітніх технологічних загроз, зокрема тих, що виникають унаслідок використання систем штучного інтелекту.

Особливого значення зазначений підхід набуває у європейському правовому просторі. Уже в преамбулі AI Act наголошується, що регулювання штучного інтелекту має сприяти не лише розвитку інновацій, а й забезпеченню громадської безпеки, демократичних цінностей, верховенства права та довіри до цифрових технологій [472]. Крім того, Регламент не поширюється на системи штучного інтелекту, що використовуються виключно для військових, оборонних або цілей національної безпеки, залишаючи їх регулювання у сфері компетенції держав-членів. Такий підхід фактично визнає, що питання

національної безпеки мають особливий правовий режим і не можуть повністю охоплюватися загальною моделлю ризик-орієнтованого регулювання.

В Україні необхідність виокремлення національної безпеки як самостійного критерію адміністративно-правової оцінки використання систем штучного інтелекту впливає безпосередньо з Конституції України. Так, стаття 17 визначає захист суверенітету, територіальної цілісності та забезпечення державної безпеки найважливішими функціями держави і справою всього Українського народу [115]. Відповідно, будь-яка діяльність органів публічної влади, пов'язана із впровадженням цифрових технологій, повинна здійснюватися з урахуванням необхідності забезпечення цих конституційних цінностей.

Розвиваючи конституційні положення, Закон України «Про національну безпеку України» визначає національну безпеку як захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних і потенційних загроз [202]. Таким чином, адміністративно-правова оцінка використання систем штучного інтелекту повинна охоплювати не лише ризики для окремої особи, а й потенційний вплив відповідних систем на спроможність держави виконувати свої конституційні функції.

Особливої актуальності запропонований підхід набуває в умовах повномасштабної збройної агресії проти України. Використання систем штучного інтелекту сьогодні охоплює управління критичною інфраструктурою, кіберзахист, автоматизований аналіз розвідувальної інформації, функціонування державних інформаційних ресурсів, безпілотні комплекси, системи підтримки прийняття управлінських рішень, цифрові платформи державного управління, інформаційно-психологічні операції та інші сфери, безпосередньо пов'язані із забезпеченням національної стійкості.

Науковці акцентують увагу: «Необхідно враховувати виклики та загрози, пов'язані з руйнівними можливостями ШІ, що являє собою глобальну небезпеку. Важливим безпековим напрямом мають стати розробки систем ШІ

для протидії високоінтелектуальній зброї противника, проведення досліджень з безпеки ШІ. Для цього буде створено відповідні науково-дослідні організації. Також необхідно розробити й впровадити нормативно-правові документи, які регулюють використання ШІ подвійного призначення» [242, с. 71].

Помилки функціонування таких систем або їх компрометація можуть спричинити наслідки, що виходять далеко за межі індивідуального порушення прав людини, створюючи загрозу для обороноздатності держави, функціонування критичної інфраструктури, інформаційного суверенітету та публічного порядку.

Саме тому другим етапом запропонованого тесту повинна бути оцінка здатності конкретної системи штучного інтелекту впливати на складові національної безпеки. До таких систем доцільно відносити насамперед ті, що використовуються у сфері оборони, секторі безпеки, кібербезпеки, державному управлінні, функціонуванні критичної інфраструктури, управлінні енергетичними, транспортними, фінансовими та комунікаційними системами, а також системи, здатні здійснювати масштабний вплив на інформаційний простір або процеси прийняття державних рішень.

На відміну від AI Act, який пов'язує рівень ризику переважно із функціональним призначенням системи, запропонований підхід виходить із її потенційного впливу на стійкість держави як конституційно значущого блага. Це дозволяє застосовувати однакові критерії адміністративно-правової оцінки незалежно від галузі використання штучного інтелекту та забезпечує адаптацію європейської моделі AI Governance до українських конституційних реалій.

З огляду на викладене, у разі встановлення, що система штучного інтелекту здатна створити загрозу національній безпеці або суттєво вплинути на функціонування критично важливих державних процесів, така система повинна підлягати спеціальному адміністративно-правовому режиму. Його елементами можуть бути обов'язкова державна оцінка ризиків, спеціальна процедура допуску до експлуатації, підвищені вимоги до кіберзахисту, безперервний державний моніторинг, спеціальні вимоги до людського

контролю та можливість негайного адміністративного обмеження або припинення використання у разі виникнення загроз.

Третім рівнем запропонованого аксіологічного ризик-орієнтованого тесту є оцінка потенційного впливу систем штучного інтелекту на права, свободи та законні інтереси людини. Саме цей рівень охоплює переважну більшість випадків використання штучного інтелекту у сфері публічного адміністрування, приватного сектору, цифрових послуг та суспільних відносин, у яких системи штучного інтелекту безпосередньо взаємодіють із людиною або приймають рішення, що можуть впливати на реалізацію її прав.

На відміну від перших двох рівнів тесту, де адміністративно-правова оцінка пов'язана із загрозою фундаментальним конституційним цінностям – життю людини та національній безпеці держави, третій рівень спрямований на забезпечення належного балансу між розвитком інноваційних технологій та гарантуванням основоположних прав людини. Саме ця складова найбільшою мірою відповідає людиноцентричній природі сучасного адміністративного права та європейській концепції *trustworthy AI*, відповідно до якої використання систем штучного інтелекту повинно здійснюватися із безумовною повагою до людської гідності, автономії особи та верховенства права.

Правову основу цього рівня становлять міжнародні акти, які закріплюють універсальний каталог фундаментальних прав людини. Так, Загальна декларація прав людини проголошує рівність усіх людей у правах і свободах, гарантує право на приватне життя, свободу думки, свободу вираження поглядів, право на справедливий суд та захист від дискримінації. Аналогічні гарантії деталізуються у Міжнародному пакті про громадянські і політичні права [150], Конвенції про захист прав людини і основоположних свобод [113] та Хартії основоположних прав Європейського Союзу [320].

Особливе значення для адміністративно-правового регулювання використання систем штучного інтелекту мають положення статей 7, 8, 21, 41 та 47 Хартії основоположних прав Європейського Союзу, які гарантують право на повагу до приватного життя, захист персональних даних, недискримінацію,

право на належне врядування та право на ефективний засіб юридичного захисту [320]. Саме ці права найчастіше зазнають потенційного впливу внаслідок застосування алгоритмічних систем прийняття рішень.

Важливим міжнародним орієнтиром виступає також Рекомендація Комітету Міністрів Ради Європи CM/Rec(2020)1 щодо впливу алгоритмічних систем на права людини, яка виходить із того, що держави повинні забезпечити правове регулювання алгоритмічних систем таким чином, щоб вони не призводили до дискримінації, порушення права на приватність, свободи вираження поглядів, свободи мирних зібрань, права на справедливий суд та інших фундаментальних прав людини [465]. У документі наголошується, що саме держава несе позитивний обов'язок щодо створення ефективних механізмів оцінювання ризиків використання алгоритмічних систем ще до початку їх експлуатації.

Конституційною основою третього рівня тесту є положення ст. 3 Конституції України, розвиваючи які Конституція гарантує рівність громадян перед законом (стаття 24), право на повагу до приватного і сімейного життя (стаття 32), свободу думки і слова (стаття 34), право на судовий захист (стаття 55), право на інформацію (стаття 34) [115] та інші права, які можуть зазнавати безпосереднього впливу внаслідок використання систем штучного інтелекту.

Особливістю цього рівня є те, що ризик виникає не лише у разі фізичного втручання у сферу прав людини, а й у процесі автоматизованого прийняття адміністративних рішень, алгоритмічного профілювання, використання біометричних технологій, систем розпізнавання облич, цифрового моніторингу поведінки, автоматизованої оцінки благонадійності особи, модерації інформаційного простору, рекомендаційних алгоритмів та інших сучасних цифрових технологій. У більшості випадків такі системи не становлять безпосередньої загрози життю людини чи національній безпеці, однак здатні істотно впливати на реалізацію конституційних прав, породжувати дискримінаційні наслідки, обмежувати автономію особи або створювати умови для алгоритмічної нерівності.

На відміну від перших двох рівнів, правові наслідки проходження третього рівня тесту не повинні автоматично призводити до заборони використання відповідної системи штучного інтелекту. Їх основною метою має бути запровадження комплексу адміністративно-правових гарантій, спрямованих на мінімізацію ризиків порушення прав людини. До таких гарантій належать забезпечення змістовного людського контролю (meaningful human oversight), алгоритмічна прозорість, пояснюваність рішень, проведення оцінки впливу на фундаментальні права (Fundamental Rights Impact Assessment), регулярний аудит алгоритмічних систем, створення ефективних процедур адміністративного й судового оскарження та здійснення державного нагляду за дотриманням вимог законодавства.

Таким чином, третій рівень аксіологічного ризик-орієнтованого тесту є завершальним етапом адміністративно-правової оцінки використання систем штучного інтелекту. Його особливість полягає в тому, що він забезпечує не обмеження технологічного розвитку, а його узгодження з конституційними принципами верховенства права, людиноцентризму та належного врядування. Саме на цьому рівні реалізується основна мета адміністративно-правового регулювання використання штучного інтелекту – забезпечення такого розвитку цифрових технологій, який не підриває систему фундаментальних прав людини, а сприяє їх ефективній реалізації.

Четвертим рівнем запропонованого аксіологічного ризик-орієнтованого тесту є оцінка впливу систем штучного інтелекту на функціонування демократичного врядування, забезпечення принципу верховенства права та інституційну спроможність держави. Необхідність виокремлення цього рівня обумовлена тим, що сучасні системи штучного інтелекту дедалі активніше інтегруються у процеси публічного адміністрування, прийняття адміністративних рішень, функціонування державних інформаційних систем, цифрових сервісів, виборчих процесів та інших сфер, які визначають якість державного управління і рівень довіри суспільства до публічної влади.

На відміну від попередніх рівнів тесту, які орієнтовані на захист конкретних об'єктів адміністративно-правової охорони, четвертий рівень спрямований на забезпечення стабільності функціонування самої системи публічної влади. Його предметом є оцінка того, чи не призводить використання штучного інтелекту до підриву засад демократичного врядування, ерозії принципу верховенства права, втрати прозорості діяльності адміністративних органів, надмірної алгоритмізації владних повноважень або зниження рівня підзвітності суб'єктів публічного адміністрування.

Доктринальною основою цього рівня є сучасна концепція AI Governance, відповідно до якої системи штучного інтелекту здатні впливати не лише на окремі права людини, а й на функціонування демократичних інститутів. Саме тому в преамбулі AI Act серед цілей правового регулювання визначено забезпечення захисту демократії, верховенства права та фундаментальних прав людини [472]. Аналогічний підхід відображено у Рекомендації Комітету Міністрів Ради Європи CM/Rec(2020)1, де наголошується, що алгоритмічні системи можуть створювати ризики для демократичних процесів, належного врядування та ефективного здійснення державою своїх позитивних зобов'язань щодо забезпечення прав людини [465].

Важливе значення має також Рамкова конвенція Ради Європи про штучний інтелект, права людини, демократію та верховенство права (Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, 2024), яка вперше на міжнародному рівні інтегрувала в єдину систему три взаємопов'язані цінності – права людини, демократію та верховенство права [333]. Це свідчить про поступове формування нової міжнародної доктрини, відповідно до якої оцінка допустимості використання ШІ не може обмежуватися лише аналізом ризиків для окремої особи, а повинна враховувати його вплив на функціонування демократичної держави загалом.

Конституційне підґрунтя цього рівня становлять положення Конституції України, насамперед ст. 1, відповідно до якої Україна є суверенною і

незалежною, демократичною, соціальною, правовою державою; ст. 5, яка визначає народ єдиним джерелом влади; ст. 6 щодо принципу поділу державної влади; ст. 8, яка закріплює принцип верховенства права; а також ст.19, відповідно до якої органи державної влади та їх посадові особи зобов'язані діяти виключно на підставі, в межах повноважень та у спосіб, визначені Конституцією та законами України [115]. Сукупність зазначених положень формує конституційну модель належного врядування, яка не може бути нівельована внаслідок автоматизації процесів публічного управління.

Застосування систем ІІІ у діяльності органів публічної влади породжує якісно нові ризики, які не охоплюються попередніми рівнями запропонованого тесту. До них належать автоматизоване прийняття адміністративних рішень без належного людського контролю, непрозорість алгоритмів, делегування дискреційних повноважень алгоритмічним системам, використання штучного інтелекту під час виборчих процесів, автоматизований розподіл публічних ресурсів, формування цифрових профілів громадян, застосування прогнозової аналітики у сфері державного управління, а також використання генеративного ІІІ для створення дезінформаційного контенту, здатного впливати на демократичні процеси.

Саме тому четвертий рівень аксіологічного тесту повинен передбачати оцінювання таких ризиків: порушення принципу верховенства права; зниження прозорості діяльності суб'єктів публічного адміністрування; надмірна алгоритмізація дискреційних повноважень; зниження рівня підзвітності органів публічної влади; неможливість ефективного адміністративного або судового контролю за алгоритмічними рішеннями; ризики впливу на демократичні процедури, включаючи виборчі процеси; підрив довіри суспільства до діяльності органів державної влади; виникнення системної залежності публічного управління від непрозорих алгоритмічних моделей.

Правовими наслідками проходження четвертого рівня тесту повинні стати запровадження обов'язкових вимог щодо алгоритмічної прозорості, забезпечення пояснюваності адміністративних рішень, заборона повної

автоматизації реалізації дискреційних повноважень, обов'язкове документування алгоритмічного процесу прийняття рішень, здійснення незалежного алгоритмічного аудиту, парламентського та громадського контролю, а також забезпечення права особи на перегляд будь-якого адміністративного рішення людиною.

Таким чином, четвертий рівень аксіологічного ризик-орієнтованого тесту завершує систему адміністративно-правової оцінки використання систем штучного інтелекту, забезпечуючи охорону не лише окремих правових благ, а й засад функціонування демократичної, правової держави. Саме інтеграція до моделі критерію демократичного врядування та верховенства права дозволяє розглядати запропонований тест як комплексний адміністративно-правовий механізм оцінювання використання штучного інтелекту, адаптований до сучасних європейських тенденцій розвитку AI Governance та конституційної моделі України.

Отже, інтенсивність правового регулювання використання систем штучного інтелекту повинна бути прямо пропорційною рівню загрози об'єктам правової охорони.

Таким чином, формується фактично новий принцип – принцип пропорційності адміністративно-правового впливу, який можна застосовувати незалежно від появи нових технологій. Він є похідним від принципу пропорційності. На нашу думку, його можна визначити наступним чином: принцип пропорційності адміністративно-правового впливу – це засаднича ідея ризик-орієнтованого регулювання використання систем штучного інтелекту, відповідно до якої інтенсивність адміністративно-правового впливу повинна перебувати у прямій залежності від ступеня потенційної загрози, яку відповідна система штучного інтелекту може створити для об'єктів адміністративно-правової охорони. При цьому зі зростанням рівня ризику повинні пропорційно посилюватися вимоги щодо державного контролю, оцінки відповідності, людського нагляду, прозорості, підзвітності, алгоритмічного аудиту та інших адміністративно-правових гарантій.

На підставі проведеного аналізу основними завданнями ризикоорієнтованої правової політики України слід визначити:

- 1) законодавче закріплення уніфікованих понять, принципів та категорій ризику;
- 2) встановлення чітко визначених заборонених практик і секторальних критеріїв високого ризику;
- 3) запровадження обов'язкових адміністративних процедур попередньої класифікації, HRIA/FRIA, оцінки відповідності, реєстрації, аудиту, моніторингу та повідомлення про інциденти;
- 4) гарантування права на інформацію, змістовне пояснення, людський перегляд та ефективне оскарження;
- 5) забезпечення управління даними, прозорості, журналювання, точності, надійності та кіберстійкості протягом усього життєвого циклу;
- 6) створення спеціального, але не позаправового режиму для воєнного стану, оборони, розвідки й національної безпеки;
- 7) підтримку інновацій через стандарти, добровільні кодекси, методичну допомогу та регуляторне експериментальне середовище;
- 8) формування системи постійного правового моніторингу й адаптивного перегляду нормативних вимог.

Отже, ризикоорієнтований підхід не може обмежуватися декларативним поділом систем III на категорії. Його зміст становить взаємопов'язана система матеріальних обмежень і адміністративних процедур, яка починається з визначення законної мети та попередньої класифікації, охоплює оцінювання впливу, якість даних, відповідність, реєстрацію, людський контроль і моніторинг та завершується коригувальними заходами, відповідальністю і правом особи на ефективний захист. Саме така модель перетворює принцип людиноцентризму на юридично дієвий механізм.

Запропонована конструкція становить нормативно-процедурну основу майбутньої інституційної моделі публічного адміністрування III. Визначення компетентного координатора, розподіл повноважень між органами, організація

секторального нагляду, адаптація законодавства до європейської моделі та послідовність упровадження підготовленого пакета нормативно-правових актів потребують окремого розгляду у підрозділі 4.2.

4.2. Напрями розвитку інституційної моделі публічного адміністрування та вдосконалення законодавства України у сфері використання штучного інтелекту в умовах євроінтеграції

Раніше одержані результати свідчать, що національне регулювання штучного інтелекту вже не може розвиватися виключно шляхом накопичення стратегічних документів, галузевих рекомендацій і поодиноких норм у законодавстві про інформацію, персональні дані та цифровізацію. Виявлені понятійна невизначеність, розпорошеність компетенції, відсутність спеціальних процедур оцінювання ризику, реєстрації, аудиту, постійного моніторингу й оскарження потребують не лише нормативного уточнення, а й формування інституційно спроможної системи публічного адміністрування. Сформована ризикоорієнтована модель визначає матеріальні обмеження та адміністративні процедури; натомість завданням цього підрозділу є встановлення суб'єктів, організаційних зв'язків і нормативних засобів, за допомогою яких такі процедури можуть реально функціонувати.

М. В. Карчевський обґрунтовано пов'язував майбутнє правового регулювання технологій із потребою постійного моніторингу, конвергенцією юридичних і технічних компетентностей та технологічною нейтральністю законодавства [94]. Зазначена позиція має безпосереднє значення для інституційної моделі у сфері ШІ. Орган, який здійснює нагляд за алгоритмічними системами, не може бути лише класичним адміністративним апаратом, орієнтованим на формальну перевірку документів. Йому необхідні юридичні, технічні, кібербезпекові, статистичні та правозахисні спроможності, доступ до незалежної експертизи, тестових середовищ і даних про фактичне функціонування систем протягом усього життєвого циклу.

Під інституційною моделлю публічного адміністрування використання ІІІ доцільно розуміти нормативно визначену систему органів публічної влади, інших уповноважених суб'єктів, їх компетенції, процедур взаємодії, інформаційних ресурсів і засобів юридичної відповідальності, спрямованих на формування політики, класифікацію ризиків, допуск систем до використання, нагляд за їх експлуатацією, захист прав осіб та реагування на інциденти. Її зміст не зводиться до створення одного спеціалізованого органу. Йдеться про узгодження нормативного, інституційного, процедурного, контрольно-наглядового та юрисдикційно-захисного елементів.

Функціональна структура цієї моделі має охоплювати п'ять взаємопов'язаних напрямів. Нормотворча функція полягає у встановленні загальних правил, критеріїв ризику та меж делегованого регулювання. Координаційна функція забезпечує узгодження діяльності центрального координатора, компетентного органу та секторальних регуляторів. Сервісно-інформаційна функція охоплює ведення реєстру, надання методичної допомоги, стандартизованих форм і роз'яснень. Контрольно-наглядова функція реалізується через перевірки, аудит, аналіз інцидентів і коригувальні заходи. Юрисдикційно-захисна функція передбачає розгляд скарг, перегляд рішень, відновлення порушених прав та судовий контроль. Відсутність хоча б одного з цих напрямів перетворює інституційну модель або на декларативну систему координації, або на суто каральний механізм без превентивної та сервісної складової.

Конституційною основою такої моделі є пріоритет людини, верховенство права, вимога діяльності органів державної влади виключно на підставі, у межах повноважень та у спосіб, передбачені Конституцією і законами України, гарантії приватності, інформаційних прав та судового захисту [115]. Звідси випливає принципова вимога: повноваження щодо перевірки алгоритмічної системи, доступу до технічної документації, зупинення її використання, застосування санкцій і розгляду скарг мають бути встановлені законом, а не виводитися із загальних завдань органу або з положень підзаконного акта.

Чинна Концепція розвитку штучного інтелекту визначає Мінцифри основним координатором формування державної політики, а серед проблем називає недосконалість правового регулювання, недостатність захисту персональних даних, складність перевірки відповідності систем законодавству й етичним принципам [215]. Проте Концепція має програмно-стратегічний характер і не встановлює компетенції наглядового органу, процедур перевірки чи обов'язкових засобів реагування. Аналогічно План заходів на 2025–2026 роки передбачає підготовку законопроекту, прийняття міжнародних стандартів як національних, використання ШІ у державному управлінні та обороні, але не створює завершеної системи адміністративного нагляду [195]. Це підтверджує, що інституційна проблема полягає не у повній відсутності суб'єктів, а у відсутності нормативно узгодженого розподілу функцій між ними.

Нині потенційні повноваження у сфері ШІ розподілені між Кабінетом Міністрів України, Мінцифри, Держспецзв'язку, Мінекономіки, органами стандартизації та акредитації, Уповноваженим Верховної Ради України з прав людини, а також секторальними суб'єктами у сферах охорони здоров'я, освіти, оборони, правоохоронної діяльності, фінансових послуг і правосуддя. Така багатосуб'єктність сама по собі не є недоліком: складність алгоритмічних систем об'єктивно потребує спеціалізації. Проблемою є те, що чинне законодавство не визначає єдиного координатора наглядової практики, порядку обміну інформацією, розмежування перевірок, вирішення компетенційних спорів і відповідальності за бездіяльність у разі виявлення системного ризику.

Для подолання зазначеної розпорошеності рамковим законом доцільно запровадити функціональну матрицю компетенції. У ній для кожної процедури має визначатися провідний орган, органи обов'язкового погодження, суб'єкти консультативної участі та орган оскарження. Наприклад, класифікацію загального ризику й ведення реєстру забезпечує національний компетентний орган; змістовну оцінку медичної, освітньої чи правоохоронної системи проводить відповідний секторальний регулятор; питання персональних даних оцінює Уповноважений або спеціалізований наглядовий суб'єкт;

кібербезпековий інцидент розглядається за участю Держспецзв'язку. Такий розподіл має закріплюватися не внутрішніми листами, а законом і урядовим порядком міжвідомчої взаємодії.

Європейська модель підтверджує доцільність поєднання централізованої координації з децентралізованим секторальним наглядом. AI Act передбачає функціонування Європейського офісу з питань ШІ, Європейської ради зі штучного інтелекту, консультативного форуму й наукової групи незалежних експертів, а на держави-члени покладає обов'язок визначити щонайменше один орган ринкового нагляду та один орган повідомлення, забезпечити їх незалежність, ресурси і єдиний контактний пункт [472]. Для України ця конструкція не повинна копіюватися механічно, проте вона демонструє ключову закономірність: політична координація, технічне оцінювання, правозахисний контроль і застосування примусових заходів не можуть бути зосереджені в одному структурному підрозділі без належних гарантій функціональної незалежності.

Рамкова конвенція Ради Європи про штучний інтелект, права людини, демократію та верховенство права також вимагає від держав запровадити законодавчі, адміністративні та інші заходи щодо прозорості, підзвітності, засобів правового захисту, управління ризиками й оцінювання впливу [333]. Підписання Конвенції Україною посилює потребу в такій інституційній моделі, яка здатна перевіряти не тільки технічну безпечність або відповідність ринковим вимогам, а й вплив систем на демократичні процеси, рівність, доступ до правосуддя та належне здійснення публічної влади.

Під час вибору національної моделі можливі три базові варіанти. Перший полягає у створенні окремого центрального органу виконавчої влади зі спеціальним статусом, компетенція якого охоплюватиме реєстрацію, перевірки, розгляд інцидентів, коригувальні заходи та санкції. Перевагами є спеціалізація, видимість відповідальності й уніфікація практики. Водночас така модель потребує значних бюджетних і кадрових ресурсів, може дублювати функції

секторальних регуляторів і створює ризик формального відокремлення нагляду за ІІІ від реального контексту його використання.

Другий варіант передбачає покладення всіх основних функцій на Мінцифри. Його перевагами є наявність політичної й експертної компетентності, зв'язок із цифровою трансформацією та можливість швидкої координації. Однак поєднання функцій стимулювання інновацій, розроблення державної політики, адміністрування експериментальних режимів і застосування санкцій створює інституційний конфлікт цілей. Орган, відповідальний за прискорене впровадження технологій, не повинен одноосібно визначати законність власних ініціатив або незалежно оцінювати наслідки систем, впроваджених у підпорядкованих проєктах.

Третім і найбільш збалансованим варіантом є мережева, або гібридна, модель. Вона має поєднувати: 1) Кабінет Міністрів України як суб'єкта загального спрямування політики; 2) Мінцифри як центрального координатора, розробника політики та методичної інфраструктури; 3) національний компетентний орган нагляду, функціонально незалежний під час перевірок і застосування заходів реагування; 4) секторальних регуляторів; 5) Уповноваженого Верховної Ради України з прав людини як суб'єкта правозахисного й інформаційно-правового контролю; 6) органи стандартизації, акредитації та оцінки відповідності; 7) незалежних аудиторів і науково-консультативну раду; 8) адміністративні суди та інші органи оскарження. Саме така конструкція відповідає міжгалузевій природі ІІІ та спеціальності 12.00.07, оскільки поєднує публічне управління, адміністративну процедуру, інформаційні режими і контроль.

Мережева модель повинна бути оформлена як юридично визначена система спільного адміністрування, а не як неформальна сукупність консультацій між відомствами. Кожна високоризикова система має отримувати унікальний ідентифікатор, а матеріали її класифікації, HRIA/FRIA, оцінки відповідності, реєстрації, аудитів, скарг та інцидентів мають об'єднуватися в єдине електронне досьє. Доступ до нього надається диференційовано:

постачальнику і розгортувачу - до власних матеріалів; секторальним і наглядовим органам - у межах компетенції; Уповноваженому та суду - в обсязі, необхідному для захисту прав; громадськості - до відкритої частини. Така конструкція безпосередньо продовжує процедурну модель, обґрунтовану вище.

У межах запропонованої моделі Кабінет Міністрів України повинен затверджувати державну політику, визначати компетентний орган, порядок взаємодії, процедури оцінювання впливу, ведення реєстру, повідомлення про інциденти та функціонування регуляторного експериментального середовища. Мінцифри доцільно зберегти функції стратегічної координації, підготовки законодавства, розроблення типових методик, організації міжнародного співробітництва й адміністрування відкритої інформаційної інфраструктури. Водночас рішення про невідповідність конкретної системи, її зупинення та застосування санкції повинні прийматися функціонально незалежно від політичного підрозділу, який сприяв її впровадженню.

Національний компетентний орган нагляду доцільно визначити законом як центральний орган виконавчої влади зі спеціальним статусом або як інший суб'єкт, правове становище якого сумісне з конституційною системою виконавчої влади. Закон має встановити прозорий конкурсний порядок призначення керівництва, строк повноважень, підстави дострокового припинення, вимоги щодо несумісності, окреме бюджетне фінансування, обов'язок щорічного публічного звіту та заборону втручання у конкретні перевірки. Загальні засади організації центральних органів виконавчої влади вимагають чіткого законодавчого визначення їх завдань, повноважень і підзвітності [219]. Тому формула «орган, визначений Кабінетом Міністрів України» може застосовуватися лише як перехідна, а основні повноваження і гарантії незалежності мають бути закріплені безпосередньо рамковим законом.

Компетенція такого органу повинна охоплювати: ведення єдиної наглядової практики; прийняття методичних актів у межах закону; планові й позапланові перевірки; доступ до документації, журналів і тестових середовищ; вимогу повторного оцінювання; розгляд повідомлень про серйозні інциденти;

обмеження функцій, тимчасове зупинення або заборону системи; застосування фінансових санкцій; розгляд скарг; координацію із секторальними органами та участь у міжнародній співпраці. При цьому він не повинен підміняти органи досудового розслідування, суди, органи захисту конкуренції чи кібербезпеки, а має передавати матеріали за належністю та координувати спільні дії.

Контрольно-наглядова діяльність у сфері ІІІ має здійснюватися за ризик-орієнтованою моделлю. Загальні засади державного нагляду у сфері господарської діяльності вимагають законності, передбачуваності, недопущення дублювання та пропорційності втручання; водночас специфіка ІІІ потребує спеціальних правил щодо дистанційного доступу до журналів, перевірки моделей, контрольного тестування та негайних заходів у разі серйозного ризику. Планові перевірки доцільно визначати на підставі категорії ризику, історії інцидентів, масштабу використання, суттєвих модифікацій і результатів попереднього аудиту. Позапланова перевірка має проводитися за скаргою, повідомленням про інцидент, виявленням невідповідності або обґрунтованою інформацією про використання системи поза заявленою метою [204].

Процедура перевірки повинна забезпечувати баланс ефективності нагляду та прав контролюваного суб'єкта. Рішення про її проведення має містити правову підставу, предмет, строк і склад перевіряльної групи; суб'єкт повинен мати право на представника, надання пояснень, отримання копій матеріалів та оскарження. Разом із тим відмова надати документацію, журнали, доступ до інтерфейсу тестування або відтворюваний набір даних не може блокувати нагляд. У такому разі закон має дозволяти застосування тимчасового обмеження експлуатації, якщо перевірити безпечність і законність іншим способом неможливо.

Доказами в наглядовому провадженні можуть бути технічна документація, журнали подій, результати контрольного тестування, звіти аудиторів, скарги, статистичні дані про точність і дискримінаційний вплив, а також висновки експертів. Комерційна таємниця не усуває обов'язку надати

інформацію компетентному органу; її захист забезпечується закритим режимом доступу й відповідальністю посадових осіб. Якщо модель є настільки непрозорою, що постачальник не здатний документально підтвердити її відповідність, ризик такої невизначеності не повинен переноситися на громадянина або державний орган-замовник.

Секторальний нагляд необхідний тому, що одна й та сама технічна модель набуває різного правового значення залежно від контексту. Медична система потребує перевірки клінічної валідності й безпеки пацієнта; правоохоронна - законності втручання у приватність, презумпції невинуватості й судового контролю; освітня - недискримінаційності оцінювання та академічної доброчесності; оборонна - дотримання міжнародного гуманітарного права, правил застосування сили й режиму державної таємниці. Тому рамковий закон має встановити мережеве регулювання: національний орган уніфікує критерії та координує практику, а секторальний орган проводить змістовну оцінку у межах своєї компетенції.

Спільна перевірка має завершуватися єдиним адміністративним рішенням або узгодженими рішеннями, які не суперечать одне одному. Провідний орган відповідає за строки, зведення висновків і повідомлення суб'єкта, тоді як секторальний орган несе відповідальність за оцінку спеціальних вимог. Якщо висновок правозахисного чи кібербезпекового органу свідчить про неприйнятний ризик, провідний орган не може його ігнорувати без окремого мотивованого обґрунтування, яке підлягає судовому контролю.

Окреме місце має належати Уповноваженому Верховної Ради України з прав людини. Масштабне профілювання, використання біометричних даних, автоматизовані адміністративні рішення й алгоритмічна дискримінація одночасно стосуються захисту персональних даних і ширшого комплексу основоположних прав. Тому Уповноваженому слід надати гарантований доступ до оцінок впливу, право ініціювати перевірку, брати участь у розгляді системних інцидентів і подавати обов'язкові для розгляду рекомендації. Методичні матеріали, підготовлені за участю Офісу Омбудсмана та Мінцифри,

вже орієнтують розробників і користувачів на системне оцінювання ризиків, якість даних і забезпечення прав суб'єктів персональних даних [182, с. 23 – 39]. Проте рекомендаційні інструменти мають бути доповнені законодавчими повноваженнями та процесуальними гарантіями.

Участь Уповноваженого повинна реалізовуватися не лише через загальні рекомендації, а й через процесуально визначені форми реагування. Законодавство про Уповноваженого передбачає парламентський контроль за додержанням конституційних прав і свобод та можливість внесення актів реагування. У сфері ШІ це дає підстави закріпити право витребувати матеріали оцінки впливу, ініціювати спільну перевірку, вимагати припинення обробки персональних даних у разі очевидної незаконності, звертатися до суду в інтересах осіб, які не можуть самотійно захистити свої права, та оприлюднювати тематичні доповіді про алгоритмічну дискримінацію [218].

Система оскарження має включати внутрішній перегляд розгортувачем, адміністративну скаргу до компетентного органу та судовий контроль. Кодекс адміністративного судочинства України покладає на суб'єкта владних повноважень обов'язок довести правомірність оскаржуваного рішення, дії чи бездіяльності. У справах, пов'язаних із ШІ, це правило означає, що орган влади повинен надати суду документацію про мету, версію системи, вхідні дані, роль алгоритмічного результату, людський перегляд і мотиви остаточного рішення. Особа не повинна доводити внутрішню технічну помилку системи, доступ до якої контролює відповідач [108].

Органи стандартизації, акредитації та оцінки відповідності забезпечують технічну складову моделі. План заходів на 2025–2026 роки передбачає прийняття низки міжнародних стандартів ISO/IEC як національних, зокрема щодо термінології, систем управління ШІ, управління ризиками, оцінювання стійкості й упередженості [195; 212; 188]. Водночас стандарт не може самотійно визначати допустимість втручання у права людини. Його роль полягає у конкретизації способу виконання законодавчої вимоги, тоді як закон установлює обов'язковий результат, межі дискреції, права особи й наслідки

невідповідності. Органи оцінки відповідності повинні бути акредитованими, компетентними та відокремленими від постачальника системи, а їх висновок не повинен позбавляти наглядовий орган права провести власну перевірку.

Кібербезпекова складова інституційної моделі потребує окремої координації. Законодавство про кібербезпеку та захист інформації в інформаційно-комунікаційних системах визначає загальні суб'єкти й вимоги щодо захисту державних інформаційних ресурсів, авторизації з безпеки, реагування на події та відповідальності. Для високоризикових систем ІІІ ці правила необхідно доповнити вимогами до захисту моделей і навчальних даних, протидії отруєнню даних, маніпуляції входами, викраденню параметрів, несанкціонованій модифікації та компрометації ланцюга постачання [204; 196].

Повідомлення про серйозний інцидент ІІІ та повідомлення про кіберінцидент мають подаватися через сумісні інформаційні канали. Якщо подія одночасно належить до обох категорій, суб'єкт повинен подавати одне первинне повідомлення з автоматичним спрямуванням його компетентним органам. Це запобігатиме розбіжностям у строках і змісті звітів. Водночас кібербезпекове усунення вразливості не завершує правову оцінку: після відновлення технічного функціонування необхідно встановити, чи були порушені права осіб, чи залишаються достовірними сформовані рішення і чи потрібне їх повторне прийняття.

Для запобігання формалізації контролю доцільно створити при національному компетентному органі науково-консультативну раду та реєстр незалежних експертів. До складу ради мають входити фахівці з адміністративного й інформаційного права, прав людини, кібербезпеки, машинного навчання, статистики, соціології та відповідних секторів. Її висновки не повинні підміняти владне рішення, але мають забезпечувати наукову обґрунтованість методик, оцінку нових класів систем і публічне обговорення регуляторних змін. Залучення громадянського суспільства й представників вразливих груп має бути обов'язковим при розробленні

критеріїв, які можуть системно впливати на доступ до публічних послуг або реалізацію прав.

Інституційна спроможність залежить від кадрової моделі. У структурі національного компетентного органу доцільно створити міждисциплінарні групи, які поєднують юристів у галузі адміністративного та інформаційного права, фахівців із машинного навчання, статистики, захисту даних і кібербезпеки. Для посад, пов'язаних із перевіркою високоризикових систем, слід установити вимоги до регулярного підвищення кваліфікації, професійної етики та декларування конфлікту інтересів. Залучений експерт не може оцінювати систему, у розробленні, постачанні чи аудиті якої він брав участь.

Нормативним ядром запропонованої моделі має стати підготовлений у межах дослідження проєкт Закону України «Про безпечне та відповідальне використання систем штучного інтелекту» (Додаток Е). Необхідність саме рамкового закону зумовлена тим, що чинні акти регулюють окремі інформаційні, адміністративні або секторальні аспекти, але не охоплюють життєвий цикл системи як єдиний об'єкт публічного нагляду. Водночас рамковий закон не повинен стати дослівною копією AI Act, оскільки Україна не має тотожної системи ринкового нагляду, структури регуляторів та обсягу адміністративної спроможності.

Підготовка пакета має здійснюватися з урахуванням вимог законодавства про правотворчу діяльність, яке закріплює принципи системності, наукового забезпечення, ресурсної забезпеченості, пропорційності, оцінки впливу, публічних консультацій та правового моніторингу. Для проєкту рамкового закону необхідна окрема концепція, яка визначить проблему, цілі, альтернативи, коло суб'єктів, фінансові наслідки та співвідношення із суміжними актами. Такий документ має відмежувати норми прямої дії від положень, реалізація яких потребує урядових процедур або секторальних технічних регламентів [207].

Закон повинен установлювати істотні елементи правового режиму: поняття, заборони, права осіб, обов'язки учасників, компетенцію органів,

підстави перевірок і санкцій. Підзаконним актам можна делегувати форми документів, технічні методики, порядок інформаційної взаємодії, строки окремих операцій та критерії, що деталізують закон. Неприпустимим є делегування уряду повноваження без чітких критеріїв розширювати перелік заборонених практик, запроваджувати нові підстави обробки чутливих даних або встановлювати додаткові обмеження конституційних прав.

Оцінка впливу законопроекту має охоплювати не лише витрати бізнесу. Необхідно окремо оцінити вплив на права людини, державний бюджет, адміністративну спроможність, конкуренцію, кібербезпеку, інновації та виконання євроінтеграційних зобов'язань. Публічні консультації доцільно проводити за групами адресатів: органи влади, розробники, малі підприємства, медичні та освітні установи, правоохоронні органи, професійні спільноти, правозахисні організації та представники вразливих груп. Зауваження мають супроводжуватися публічною таблицею їх врахування або мотивованого відхилення.

Важливо відразу передбачити механізм правового моніторингу закону. Через два роки після початку застосування основних вимог Кабінет Міністрів України повинен подати Верховній Раді звіт про функціонування реєстру, кількість перевірок та інцидентів, результативність скарг, витрати суб'єктів, вплив на інновації й виявлені колізії. Подальший перегляд здійснюється періодично або раніше у разі істотної зміни європейського регулювання, появи нових класів систем чи системного інциденту.

Проект рамкового закону доцільно оцінювати за шістьма функціональними блоками. Перший - понятійний і принциповий. Він закріплює терміни «система III», «постачальник», «розгортувач», «імпортер», «розповсюджувач», «суттєва модифікація», «серйозний інцидент», «високоризикова система», а також принципи законності, пропорційності, прозорості, недискримінації, захисту даних, безпеки та людського контролю. Уніфікація термінів має не лише теоретичне значення: вона визначає, хто є

адресатом обов'язку, в який момент він виникає та який суб'єкт відповідає за зміну функціонального призначення системи.

Другий блок - класифікація ризиків і заборонені практики. Його положення повинні кореспондувати з моделлю, обґрунтованою у підрозділі 4.1, але не дублювати її описово. Закон має встановлювати правові наслідки класифікації: заборону неприйнятних практик; обов'язкову оцінку відповідності, реєстрацію, HRIA/FRIA та постійний моніторинг для високоризикових систем; обов'язки прозорості для систем обмеженого ризику; добровільні кодекси для мінімального ризику. Перелік високоризикових сфер має бути достатньо визначеним, але допускати оновлення за процедурою, що гарантує парламентський і судовий контроль, аби делеговане регулювання не перетворилося на необмежену нормотворчу дискрецію виконавчої влади.

Третій блок - обов'язки учасників ланцюга створення і використання. Проєкт обґрунтовано розподіляє відповідальність між постачальником, імпортером, розповсюджувачем і розгортувачем. Це усуває поширену практичну проблему, коли орган публічної влади посиляється на закритість комерційної моделі, а постачальник - на спосіб її застосування замовником. Відповідальність має слідувати за фактичним контролем: суб'єкт, який суттєво змінює призначення, модель або дані, повинен набувати обов'язків постачальника; розгортувач відповідає за законну мету, якість вхідних даних, людський контроль і фактичний контекст експлуатації.

Особливе значення має окрема стаття про органи публічної влади. До закупівлі або розгортання високоризикової системи орган повинен визначити законну мету, підтвердити компетенцію, провести оцінку впливу, передбачити кадрові й бюджетні ресурси для людського контролю та оприлюднити мінімальну інформацію про систему. Такий підхід перетворює принцип законності зі статичної вимоги на послідовність адміністративних дій. Економія часу чи коштів не може сама по собі виправдовувати інтенсивне втручання у права, якщо мету можна досягти менш обтяжливим способом.

Четвертий блок - права осіб. Законопроект має закріпити право бути поінформованим про істотне використання ШІ, отримати змістовну інформацію про основні фактори рішення, вимагати перегляду компетентною посадовою особою, оскаржити рішення або використання системи, а також захиститися від алгоритмічної дискримінації. Право на пояснення не слід ототожнювати з вимогою розкрити весь програмний код. Достатнім має бути пояснення фактичних і правових факторів, категорій даних, ролі системи, причин прийняття або відхилення її результату та меж невизначеності, яке дозволяє особі ефективно реалізувати право на захист.

П'ятий блок - публічне адміністрування, нагляд і реєстр. У проекті доцільно закріпити національний компетентний орган, функціональну незалежність його наглядових рішень, мережеву взаємодію із секторальними регуляторами, повноваження Уповноваженого, публічну й закриту частини реєстру, регуляторне експериментальне середовище та підтримку малих і середніх підприємств. Відкритість реєстру повинна бути правилом, а закритість - винятком, обґрунтованим державною таємницею, безпекою або захистом уразливостей. Навіть у закритому режимі інформація має бути доступною уповноваженим контролюючим органам і суду.

Шостий блок - контроль, коригувальні заходи, відповідальність і спеціальні режими. Законопроект передбачає ризикорієнтовані перевірки, вимогу усунення порушення, обмеження функцій, зупинення, відкликання або заборону системи, а також фінансові санкції. Розмір санкції повинен відповідати принципам законності, пропорційності й індивідуалізації, ураховувати масштаб шкоди, повторність, співпрацю та фінансовий стан суб'єкта. Для оборони, розвідки, правоохоронної діяльності й критичної інфраструктури необхідні закриті процедури, однак вони не можуть скасовувати журналювання, внутрішній аудит, визначення відповідальних посадових осіб і незалежний контроль.

Принциповою перевагою рамкового законопроекту є поєднання ринкового та правозахисного підходів. Система може бути технічно справною,

але юридично неприпустимою через незаконну мету, непропорційне втручання або дискримінаційний результат. І навпаки, правомірна мета не компенсує низьку точність, відсутність кібербезпеки чи неможливість простежити дані. Тому нагляд має охоплювати одночасно технічну відповідність, адміністративну законність та інформаційні права.

Для малих і середніх підприємств законопроект має передбачити пропорційні механізми підтримки: типові форми документації, безоплатні консультації, доступ до пісочниці, спільні тестові середовища та можливість поетапного виконання окремих організаційних вимог. Пропорційність не означає зниження рівня захисту в чутливих сферах: заборонені практики та базові права осіб застосовуються однаково до всіх, тоді як спрощення може стосуватися форми звітності, способу підтвердження відповідності або доступу до інфраструктури.

Сам рамковий закон не забезпечить зміни практики без синхронного внесення змін до базових законодавчих актів. Саме тому другим елементом пакета є проєкт Закону України «Про внесення змін до деяких законодавчих актів України щодо використання систем штучного інтелекту» (Додаток Е). Його функція полягає у вбудовуванні загальних принципів у конкретні адміністративні та інформаційні процедури. Такий підхід відповідає висновку Білої книги про необхідність переходу від підготовчих позазаконодавчих інструментів до всеохопного юридично обов'язкового регулювання [152]. Водночас запропонований пакет іде далі, оскільки визначає не лише майбутній напрям, а й конкретні зміни до чинних процедур.

Найважливішими є зміни до Закону України «Про адміністративну процедуру». Чинна стаття 69 допускає автоматичне прийняття адміністративного акта у випадках, передбачених законом, але не формує повного режиму алгоритмічно підтриманого рішення [186]. Запропонована стаття 69-1 має встановити визначену законом мету, повідомлення особи, заборону покладати негативний акт виключно на результат ШІ за наявності дискреції, обов'язок посадової особи самостійно оцінити факти й

пропорційність, фіксацію версії системи, даних і результату, право на людський перегляд та доступ органу оскарження і суду до необхідної інформації.

Вказані зміни мають системоутворююче значення для адміністративного права. Вони не забороняють автоматизацію формалізованих рішень, але відмежовують її від випадків, де потрібні оцінка, балансування інтересів або застосування дискреції. Посадова особа не може замінити мотивування посиленням на «рекомендацію системи», а комерційна таємниця постачальника не повинна унеможливлювати судовий контроль. Алгоритмічний результат є доказовим або аналітичним елементом адміністративної справи, а не самостійним суб'єктом владного повноваження.

Поряд із Законом України «Про адміністративну процедуру» необхідно внести зміни до законодавства про адміністративні послуги. Воно визначає загальні засади доступності, відкритості та організації надання послуг, однак не регулює істотну роль алгоритмічної системи у встановленні права особи на результат. У паспорті адміністративної послуги доцільно зазначати факт використання високоризикової системи, категорії даних, відповідального адміністратора, можливість отримання послуги альтернативним способом і порядок людського перегляду [185].

Матеріали адміністративної справи повинні утворювати відтворений алгоритмічний слід. До нього належать версія системи, дата й час її використання, джерела вхідних даних, сформований результат, інформація про ручне коригування, мотиви прийняття або відхилення рекомендації та особа, відповідальна за остаточне рішення. Такий набір не дублює технічний журнал, а перетворює його релевантну частину на процесуальний матеріал, доступний органу оскарження та суду.

Зміни до Закону України «Про захист персональних даних» мають запровадити поняття профілювання, автоматизованого рішення, алгоритмічно виведених і біометричних даних, право на людське втручання, пояснення, заперечення й виправлення виведених даних, а також обов'язкову оцінку впливу на захист персональних даних для систематичного профілювання і

масштабної обробки біометрії [197]. Важливо узгодити цю оцінку з HRIA/FRIA: вони можуть проводитися в межах єдиного процесу, але мають зберігати різний предмет. DPIA оцінює ризики обробки персональних даних, тоді як FRIA охоплює ширший вплив на рівність, свободу вираження, справедливий суд, соціальні та інші права.

Запропоноване правило про право не бути об'єктом виключно автоматизованого рішення має містити чіткі винятки та гарантії. Воно не повинно перешкоджати технічній автоматизації масових формалізованих операцій, якщо закон вичерпно визначає умови рішення, дані є перевіреними, а особа може невідкладно вимагати людського перегляду. Натомість використання спеціальних категорій даних, біометричного профілювання або прогнозової оцінки поведінки має допускатися лише на підставі закону, за доведеної необхідності й пропорційності та під незалежним контролем.

Окремо необхідно врегулювати правовий статус алгоритмічно виведених даних. Профіль, рейтинг або прогноз, сформований системою на основі достовірних первинних відомостей, сам може бути помилковим або контекстуально непридатним. Особі слід надати право не лише виправити вихідний запис, а й оскаржити висновок, вимагати позначення його спірності, обмеження подальшого використання та повідомлення органів, яким він був переданий. Негативний алгоритмічний висновок не повинен безстроково відтворюватися в інших реєстрах після усунення його підстав.

Доповнення Закону України «Про доступ до публічної інформації» повинно забезпечити алгоритмічну прозорість органів влади. До обов'язково оприлюднюваних відомостей доцільно віднести найменування системи, мету, правову підставу, категорію ризику, постачальника, категорії даних, стислий виклад оцінки впливу, відповідальну посадову особу та порядок оскарження [190]. При цьому необхідно зберегти трискладовий тест обмеження доступу. Технічні деталі, уразливості або державна таємниця можуть бути закритими, однак особа, суд і компетентний орган мають отримувати мінімально необхідну інформацію для перевірки законності.

Зміни до Закону України «Про публічні електронні реєстри» повинні врегулювати вторинне використання реєстрових даних для навчання, валідації та застосування ІІІ. Наявність технічного доступу до даних не є юридичною підставою для їх необмеженого повторного використання. Необхідні визначена законом мета, документована перевірка сумісності з первинною метою, заборона соціального оцінювання й довільного профілювання, обов'язкове журналювання масових запитів та формування алгоритмічних висновків, простежуваність походження й виправлення помилок [208]. Саме якість реєстрових даних визначає законність багатьох майбутніх автоматизованих адміністративних рішень.

Зміни до Закону України «Про публічні закупівлі» мають запобігти ситуації, коли держава купує систему, яку фактично не може перевірити, змінити або припинити використовувати. Технічна специфікація повинна містити вимоги до точності, репрезентативності даних, кібербезпеки, журналювання, пояснюваності, людського контролю, переносимості, оновлень, аудиту й передачі документації [209]. Договір не може позбавляти замовника можливості мотивувати рішення, виконувати вимоги про захист даних або надати інформацію суду. Окремо слід передбачити повідомлення про суттєву модифікацію моделі та право розірвання договору у разі неприйняттого ризику.

Запропоновані закупівельні вимоги мають також антикорупційне значення. Попереднє визначення мети й категорії ризику, оцінка альтернатив, фіксація критеріїв ефективності та право незалежного аудиту знижують ризик закупівлі технології за формальними або політично мотивованими підставами. Водночас надмірно деталізовані технічні умови не повинні використовуватися для штучного звуження конкуренції під конкретного постачальника. Тому закон має встановлювати функціональні результати й мінімальні гарантії, а конкретні технічні параметри - визначатися пропорційно предмету закупівлі.

Управління закупленою системою має продовжуватися протягом усього строку договору. Замовник повинен вести реєстр модифікацій, перевіряти оновлення до їх розгортання, контролювати субпідрядників і походження

критичних компонентів, а також періодично оцінювати досягнення заявлених показників. Істотна зміна моделі, даних або способу використання повинна активувати повторну класифікацію та, за потреби, нову процедуру закупівлі. Це запобігатиме ситуації, коли після первинної оцінки постачальник фактично замінює систему через хмарне оновлення.

Третім рівнем пакета є підзаконне процедурне регулювання. Проект постанови Кабінету Міністрів України про затвердження Порядку проведення оцінки впливу високоризикових систем ІІІ на основоположні права (Додаток Е) конкретизує суб'єктів, строки, зміст, погодження, оприлюднення і перегляд FRIA. Такий акт необхідний, оскільки рамкова законодавча вимога без єдиної методики призведе до нерівномірної практики. Водночас підзаконний акт не може розширювати перелік обмежуваних прав або створювати нові підстави для втручання; він повинен регламентувати процедуру реалізації вимог, установлених законом.

Запропонований Порядок має охоплювати опис системи й мети, правову підставу, категорії осіб і даних, аналіз необхідності та альтернатив, оцінку якості даних, ризик дискримінації, людський контроль, консультації із заінтересованими сторонами, залишковий ризик і план моніторингу. Принципово важливим є правило, за яким економія коштів або часу не є самодостатньою підставою для інтенсивного втручання, а особи, пов'язані з постачальником, не можуть одноосібно затверджувати прийнятність ризику. Для систем у закритих секторах публічна консультація може замінюватися незалежною експертизою в захищеному режимі.

Проект постанови про Державний реєстр високоризикових систем ІІІ (Додаток Е) та повідомлення про серйозні інциденти забезпечує інформаційну інфраструктуру нагляду. Реєстр має складатися з публічної та закритої частин, містити відомості про призначення, суб'єктів, правову підставу, категорію ризику, оцінку відповідності й стислий зміст FRIA. Внесення до реєстру не повинно визнаватися дозволом або презумпцією законності: воно забезпечує облік і прозорість, але не замінює оцінку відповідності та наглядову перевірку.

Строки повідомлення про інцидент - попереднє повідомлення не пізніше 72 годин і повний звіт у визначений строк - мають узгоджуватися з кібербезпековими та інформаційними процедурами, щоб уникнути дублювання повідомлень.

Функціонування реєстру потребує особливої уваги до інформаційної безпеки. Закрита частина може містити архітектуру систем, відомості про вразливості, повні оцінки впливу та дані про оборонні або правоохоронні застосування. Тому необхідні розмежування доступу, журналювання дій користувачів, резервне копіювання, незалежний аудит безпеки та автоматизований обмін лише з уповноваженими органами. Водночас режим закритості не повинен перешкоджати оприлюдненню знеособленої інформації про типові інциденти і заходи запобігання, необхідної для суспільного навчання та розвитку стандартів.

Реєстр має бути не ізольованою базою, а ядром інформаційної взаємодії. Він повинен отримувати статусні відомості з систем оцінки відповідності, зберігати посилання на актуальну FRIA, приймати повідомлення про інциденти, фіксувати приписи та судові рішення, а також передавати узагальнені дані для правового моніторингу. Автоматизований обмін можливий лише за умови чіткої правової підстави, розмежування ролей володільців інформації, журналювання запитів та перевірки якості. Запис у реєстрі не створює права використовувати систему, але відсутність обов'язкового запису має бути самотійною підставою для зупинення її публічного розгортання.

Проект постанови про регуляторне експериментальне середовище (Додаток Е) має поєднати підтримку інновацій з контрольованістю ризику. Регуляторна пісочниця не є територією звільнення від права. Участь у ній не повинна скасовувати конституційні гарантії, правила захисту персональних даних, заборонені практики та обов'язок відшкодування шкоди. Її призначення полягає у випробуванні систем у визначених часових, функціональних і територіальних межах, перевірці майбутніх вимог, підготовці до оцінки відповідності та збиранні доказів для вдосконалення політики. Біла книга

обґрунтовано розглядає пісочницю як один із підготовчих інструментів, але вона не може замінити обов'язкові правила для неприйнятного й високого ризику [152].

Під час відбору учасників пісочниці необхідно оцінювати інноваційність, суспільну корисність, готовність прототипу, керованість ризику, наявність компетентної команди та неможливість безпечного тестування поза середовищем. Індивідуальний план повинен визначати строк, категорії даних, контрольні показники, відповідальних осіб, умови зупинення та порядок виходу. Результатом не може бути автоматичний дозвіл на ринок; суб'єкт отримує висновок про проведене тестування, виявлені ризики й готовність до формальних процедур.

Адміністрування пісочниці слід функціонально відокремити від остаточного наглядового рішення. Підрозділ, який консультував учасника та допомагав адаптувати систему, не повинен одноосібно підтверджувати її відповідність або вирішувати питання про санкцію. Водночас інформація, добровільно розкрита під час експерименту, не може автоматично використовуватися для покарання за добросовісно виявлений і своєчасно усунутий дефект, крім випадків приховування істотних обставин, заподіяння шкоди або продовження забороненої практики.

Усі проєкти мають прийматися як узгоджений пакет. Випереджальне введення реєстру без рамкового закону створить облік невизначеного кола систем. Запровадження FRIA без визначення високого ризику й правових наслідків залишкового ризику перетворить її на формальність. Прийняття рамкового закону без змін до адміністративної процедури, персональних даних, реєстрів і закупівель не дасть особі практичних процесуальних прав. Тому необхідна синхронізація набрання чинності, перехідних строків, методик, фінансування та підготовки персоналу.

Водночас пакет потребує подальшого юридико-технічного доопрацювання перед офіційним внесенням. По-перше, необхідно провести повну інвентаризацію колізій із секторальними законами, режимами державної

таємниці, ринкового нагляду, медичних виробів, фінансового регулювання та судоустрою. По-друге, фінансові санкції мають бути узгоджені з конституційними принципами юридичної відповідальності, бюджетним законодавством і процедурою їх оскарження. По-третє, слід визначити статус та процесуальні права органів оцінки відповідності й аудиторів. По-четверте, потрібно підготувати фінансово-економічні розрахунки створення реєстру, кадрового забезпечення і тестової інфраструктури.

Юридико-технічне доопрацювання має завершуватися підготовкою порівняльних таблиць, переліку підзаконних актів, які належить прийняти або скасувати, матриці компетенції та плану інформаційної взаємодії. Окремо необхідно визначити, які положення набирають чинності одночасно, а які - після створення реєстру, акредитації органів і затвердження методик. Невизначене відкладення дії норм до моменту «створення необхідних умов» є неприйнятним; закон повинен установлювати граничні строки та відповідальних суб'єктів.

Євроінтеграційна адаптація повинна здійснюватися за принципом функціональної еквівалентності, а не буквального відтворення. AI Act є регламентом внутрішнього ринку ЄС і спирається на систему нотифікованих органів, ринкового нагляду та взаємного визнання, якої Україна не може відтворити одномоментно. На першому етапі необхідно забезпечити сумісність термінів, класифікації, обов'язків операторів, технічної документації, стандартів, реєстрації та нагляду; надалі - формувати механізми визнання оцінки відповідності й участі у європейських інформаційних мережах.

Особливої обережності потребує адаптація правил до оборони та національної безпеки. AI Act містить винятки зі сфери дії для систем, призначених виключно для військових, оборонних або національно-безпекових цілей, однак це не означає відсутності правового регулювання в Україні. Національний закон має встановити окремий закритий режим, змістовний людський контроль, внутрішній і парламентський нагляд, аудит інцидентів та персональну відповідальність. Дослідження використання ШІ в управлінні

Збройних Сил України підтверджує потребу спеціального правового механізму, який поєднує ефективність військового управління з безпековими та етичними гарантіями [260].

Запровадження запропонованої моделі доцільно здійснювати поетапно. На підготовчому етапі мають бути проведені інвентаризація систем III в органах влади, визначення відповідальних підрозділів, підготовка кадрів, прийняття національних стандартів, запуск методичних пілотів FRIA та пісочниці. На законодавчому етапі приймаються рамковий закон і пакет змін, визначається компетентний орган, установлюються перехідні строки. На інституційному етапі створюються реєстр, система повідомлень, організовується секторальна взаємодія та акредитація. На повному операційному етапі застосовуються обов'язкові оцінки, аудит, перевірки, санкції та міжнародний обмін.

Для управління переходом доцільно створити тимчасовий міжвідомчий координаційний механізм із чітко визначеним строком діяльності. Його завданнями мають бути інвентаризація наявних систем, підготовка проєктів актів, узгодження технічної архітектури реєстру, формування кадрового плану, пілотування процедур і контроль виконання дорожньої карти. Після початку повноцінної роботи національного компетентного органу тимчасова структура припиняється, а її матеріали й повноваження передаються постійним інституціям.

Дорожня карта повинна містити не лише строки прийняття актів, а й вимірювані результати: частку проінвентаризованих систем, кількість підготовлених фахівців, час розгляду FRIA, частку реєстрових записів із повною документацією, строки реагування на інциденти, кількість успішно переглянутих рішень та витрати суб'єктів. Показники не повинні стимулювати формальне збільшення перевірок або санкцій; критерієм ефективності є зменшення серйозних інцидентів, підвищення якості рішень і реальна доступність засобів захисту.

Перехідні строки мають бути диференційованими. Заборонені практики повинні припинятися раніше, оскільки їх неприйнятність не залежить від створення повної адміністративної інфраструктури. Для високоризикових систем необхідний довший період, протягом якого суб'єкти проводять інвентаризацію, готують документацію, навчають персонал і здійснюють оцінювання. Системи, які вже використовуються органами влади, не можуть автоматично вважатися законними лише через попереднє придбання; їх продовження має залежати від оцінки ризику, а у випадку неприйнятного залишкового ризику - бути припинене.

До основних ризиків реалізації належать інституційне дублювання, дефіцит експертів, формалізація оцінок, надмірне закриття інформації, регуляторне захоплення органу великими постачальниками, непропорційні витрати для малого бізнесу та використання режиму національної безпеки для обходу гарантій. Їх мінімізація потребує чіткого розмежування компетенції, конкурсного добору, ротації експертів, публічної звітності, незалежного аудиту, пропорційних вимог, типових документів для малих підприємств і спеціальних процедур контролю за закритими системами.

Запобігання регуляторному захопленню потребує правил несумісності, прозорості зустрічей із заінтересованими суб'єктами, декларування конфліктів інтересів, ротації зовнішніх експертів і незалежного аудиту діяльності органу. Методики класифікації та перевірок мають проходити публічне обговорення, а відхилення від них у конкретній справі - окремо мотивуватися. Щорічний звіт повинен містити не лише статистику, а й аналіз типових порушень, використання закритих процедур, судового перегляду та виконання рекомендацій Уповноваженого.

Надмірна централізація створює ризик перевантаження та втрати секторальної компетентності, тоді як надмірна децентралізація - різної практики й можливості обирати найбільш сприятливого регулятора. Баланс забезпечується єдиними горизонтальними правилами, обов'язковими методиками, спільною інформаційною системою, механізмом вирішення спорів

і правом національного органу переглядати секторальну практику лише з питань загальних вимог, не підміняючи спеціальну оцінку.

Очікуваним результатом є не збільшення кількості заборон як самоціль, а формування передбачуваного режиму. Для органів влади він визначає процедуру законного впровадження; для розробників - зрозумілі критерії доступу до ринку й публічних закупівель; для громадян - інформацію, людський перегляд і можливість оскарження; для судів і контролюючих органів - доступ до документації та журналів; для держави - інструменти моніторингу системних ризиків. Це знижує правову невизначеність і одночасно підтримує інновації, оскільки відповідальний суб'єкт може прогнозувати вимоги до системи ще на стадії її проєктування.

Оцінювання результативності інституційної моделі має поєднувати кількісні й якісні індикатори. До перших належать строки процедур, кількість зареєстрованих систем, інцидентів, перевірок, скарг і виконаних приписів. До других - якість мотивування, доступність пояснення, рівень дискримінаційного впливу, здатність відтворити рішення, незалежність людського перегляду та довіра користувачів. Міжнародні принципи відповідального ШІ також орієнтують держави на людиноцентричність, підзвітність, надійність і систематичний перегляд політики на основі доказів [472].

Зв'язок із підрозділом 4.1 полягає в тому, що кожна матеріальна вимога й адміністративна процедура повинна мати визначеного інституційного носія. Класифікація ризику потребує органу, який ухвалює мотивоване рішення; HRIA/FRIA - незалежної перевірки та участі зачеплених груп; реєстрація - захищеної інформаційної системи; людський контроль - підготовленої посадової особи; інцидент - координованого реагування; оскарження - доступу до матеріалів і незалежного перегляду. Саме узгодження процедурного та інституційного рівнів надає запропонованій моделі ознак цілісного адміністративно-правового механізму.

Таким чином, оптимальною для України є гібридна мережева інституційна модель, у якій Мінцифри координує політику та методичну

інфраструктуру, функціонально незалежний національний компетентний орган здійснює нагляд і застосовує заходи реагування, секторальні органи забезпечують змістовну оцінку, Уповноважений контролює правозахисний і вимір захисту персональних даних, а суди гарантують остаточний контроль законності. Нормативною основою цієї моделі має стати узгоджений пакет рамкового закону, змін до базових законів і процедурних постанов Кабінету Міністрів України.

Запропонована система відповідає логіці спеціальності 12.00.07, оскільки її центральним предметом є не технічна конструкція алгоритму, а організація публічного адміністрування, адміністративні процедури, інформаційні правові режими, державний контроль, відповідальність і захист особи. Її впровадження має перетворити фрагментарні стратегічні орієнтири, встановлені Концепцією, Планом заходів і Білою книгою, на юридично обов'язковий, інституційно забезпечений та судово контрольований механізм безпечного й відповідального використання ШІ в Україні.

Висновки до розділу 4

1. Подальший розвиток національного регулювання штучного інтелекту не може здійснюватися шляхом накопичення стратегічних документів, галузевих рекомендацій і фрагментарних змін до окремих законів. Необхідним є перехід до цілісного адміністративно-правового та інформаційно-правового механізму, який поєднує матеріальні обмеження, адміністративні процедури, компетенцію органів публічної влади, інформаційні ресурси, державний нагляд, юридичну відповідальність і засоби захисту прав особи. Такий механізм має одночасно виконувати правозахисну, безпекову та інноваційно-стимулюючу функції.

2. Ризик-орієнтовану правову політику у сфері штучного інтелекту запропоновано розуміти як системну, науково обґрунтовану діяльність держави з формування і реалізації диференційованих правових режимів, за яких зміст та

інтенсивність заборон, обов'язків, процедур контролю і юридичних гарантій визначаються імовірністю, масштабом, тяжкістю та оборотністю негативного впливу конкретної системи ШІ на права людини, демократію, верховенство права, публічну й національну безпеку. Правове значення має не сам факт використання ШІ, а його функціональне призначення, середовище застосування, категорії даних, коло осіб, рівень автономності, характер можливих помилок і юридичних наслідків.

3. До засад національної ризикоорієнтованої політики віднесено людиноцентризм, верховенство права, законність, правову визначеність, необхідність і пропорційність втручання, превентивність, технологічну нейтральність, прозорість, пояснюваність, недискримінацію, якість даних, змістовний людський контроль, підзвітність, персоніфіковану відповідальність, кіберстійкість, участь заінтересованих сторін, адаптивність регулювання та підтримку безпечних інновацій. Обґрунтовано, що зазначені принципи повинні мати процедурне продовження у вигляді документованої перевірки законної мети, аналізу менш обмежувальних альтернатив, визначення відповідальних осіб, журналювання, аудиту, повідомлення особи, людського перегляду та ефективного оскарження.

4. Запропоновано законодавчо закріпити п'ять взаємопов'язаних категорій: заборонені практики неприйнятного ризику; високоризикові системи; системи обмеженого ризику, щодо яких застосовуються спеціальні вимоги прозорості; системи мінімального ризику, які переважно підпорядковуються загальному законодавству та добровільним стандартам; моделі ШІ загального призначення, включаючи моделі із системним ризиком. Класифікація повинна мати динамічний характер, а суттєва модифікація системи, зміна її мети, масштабування, підключення нових джерел даних або виявлення раніше невідомої закономірності шкоди мають зумовлювати повторне оцінювання.

5. Сформовано систему адміністративних процедур, необхідних для правомірного впровадження та експлуатації високоризикових систем ШІ

протягом усього життєвого циклу. До неї належать інвентаризація і попередня класифікація; перевірка законної мети, компетенції та менш обмежувальних альтернатив; оцінювання впливу на основоположні права; управління даними; оцінка відповідності; спеціальні вимоги до публічної закупівлі; державна реєстрація; змістовний людський контроль; післяреєстраційний моніторинг; повідомлення про серйозні інциденти; застосування коригувальних заходів; адміністративне та судове оскарження. Оцінка впливу на захист персональних даних, HRIA/FRIA та оцінка відповідності мають різний предмет і не повинні підміняти одна одну.

6. Для забезпечення простежуваності адміністративних рішень запропоновано запровадити паспорт ризику та єдине адміністративне дос'є системи ІІІ. Паспорт ризику має містити відомості про призначення системи, правову підставу, суб'єктів життєвого циклу, категорії даних, потенційно зачеплені права, вразливі групи, рівень автономності, сценарії шкоди, контрольні показники, засоби людського втручання і категорію ризику. В адміністративному дос'є доцільно поєднувати обґрунтування потреби, закупівельні матеріали, результати оцінок впливу й відповідності, опис людського контролю, реєстраційні відомості, аудити, скарги та матеріали про інциденти.

7. Змістовний людський контроль визначено як реальну організаційно-правову спроможність компетентної особи розуміти можливості й обмеження системи, перевіряти вхідні дані та результат, виявляти автоматизаційне упередження, відхиляти або коригувати алгоритмічну рекомендацію і безпечно зупиняти систему. Використання ІІІ не змінює суб'єкта владної компетенції та не звільняє адміністративний орган чи посадову особу від обов'язку дослідити обставини, мотивувати рішення і нести відповідальність за його зміст.

8. Обґрунтовано багаторівневу модель алгоритмічної прозорості. Перший рівень охоплює повідомлення про факт і роль використання ІІІ; другий - надання розширеної інформації особі, щодо якої приймається юридично значуще рішення; третій - доступ аудитора, компетентного органу та суду до

технічної й організаційної документації; четвертий - оприлюднення відомостей про високоризикові системи, їх призначення, правову підставу, результати оцінки впливу та серйозні інциденти. Захист державної, службової або комерційної таємниці повинен забезпечуватися диференційованим доступом, а не усуненням підзвітності.

9. Оптимальною для України визначено гібридну мережеву інституційну модель публічного адміністрування ІІІ, яка поєднує централізовану координацію із секторальним наглядом. У межах цієї моделі Кабінет Міністрів України забезпечує загальне спрямування політики; Міністерство цифрової трансформації України - стратегічну координацію, підготовку законодавства, методичне забезпечення, міжнародну взаємодію та відкриту інформаційну інфраструктуру; функціонально незалежний національний компетентний орган - перевірки, розгляд інцидентів і заходи реагування; секторальні регулятори - спеціальну оцінку; Уповноважений Верховної Ради України з прав людини - правозахисний та інформаційно-правовий контроль; суди - остаточний контроль законності.

10. Запропоновано запровадити аксіологічний ризик-орієнтований тест адміністративно-правової оцінки використання систем штучного інтелекту за такими рівнями: на першому рівні визначається наявність потенційної загрози життю та здоров'ю людини як найвищій соціальній цінності; на другому - оцінюється можливий вплив системи штучного інтелекту на національну безпеку та функціонування держави; на третьому - встановлюється ступінь ризику для реалізації прав, свобод і законних інтересів людини; на четвертому - оцінка впливу систем штучного інтелекту на функціонування демократичного врядування, забезпечення принципу верховенства права та інституційну спроможність держави.

11. Принцип пропорційності адміністративно-правового впливу - це засаднича ідея ризик-орієнтованого регулювання використання систем штучного інтелекту, відповідно до якої інтенсивність адміністративно-правового впливу повинна перебувати у прямій залежності від ступеня

потенційної загрози, яку відповідна система штучного інтелекту може створити для об'єктів адміністративно-правової охорони

12. Запропоновано закріпити функціональну матрицю компетенції, у якій для кожної процедури визначаються провідний орган, суб'єкти обов'язкового погодження, консультативні учасники та орган оскарження. Спільне адміністрування має забезпечувати єдині горизонтальні правила і наглядову практику, зберігаючи компетенцію секторальних органів щодо оцінки спеціальних медичних, освітніх, правоохоронних, оборонних та інших ризиків.

Нормативним ядром запропонованої моделі має стати Закон України «Про безпечне та відповідальне використання систем штучного інтелекту», у якому доцільно закріпити понятійний апарат, принципи, категорії ризику, заборонені практики, обов'язки постачальників, імпортерів, розповсюджувачів і розгортувачів, спеціальні вимоги до органів публічної влади, права осіб, інституційну систему, державний реєстр, регуляторне експериментальне середовище, контроль, коригувальні заходи, юридичну відповідальність та особливості застосування правил у закритих секторах.

13. Прийняття рамкового закону має супроводжуватися синхронним внесенням змін до законодавства про адміністративну процедуру, адміністративні послуги, захист персональних даних, доступ до публічної інформації, публічні електронні реєстри та публічні закупівлі. Зміни повинні врегулювати алгоритмічно підтримані адміністративні рішення, повідомлення і людський перегляд; профілювання та алгоритмічно виведені дані; право на пояснення і виправлення; правомірність повторного використання реєстрової інформації; журналювання та простежуваність; вимоги до документації, аудиту, кібербезпеки, переносимості даних, суттєвих модифікацій і припинення використання закуплених систем.

Третім рівнем нормативного забезпечення визначено процедурні акти Кабінету Міністрів України щодо проведення оцінки впливу високоризикових систем ШІ на основоположні права; ведення державного реєстру високоризикових систем і повідомлення про серйозні інциденти;

функціонування регуляторного експериментального середовища. Підзаконні акти повинні конкретизувати суб'єктів, строки, документи, порядок погодження, інформаційну взаємодію і методи контролю, але не можуть самостійно встановлювати нові підстави втручання у права, розширювати законодавчі заборони або визначати основні повноваження наглядових органів.

Євроінтеграційну адаптацію запропоновано здійснювати за принципом функціональної еквівалентності, а не буквального відтворення європейської моделі. Національне регулювання має бути сумісним із категоріями ризику, обов'язками учасників, технічною документацією, стандартами, процедурами оцінки відповідності та нагляду, водночас ураховуючи конституційну систему органів виконавчої влади України, стан публічних реєстрів, кадрові й фінансові ресурси, правовий режим воєнного стану та потреби відновлення держави. Оборона, розвідка і національна безпека не повинні утворювати позаправову сферу; для них допустимі спеціальні закриті та прискорені процедури зі збереженням законності, пропорційності, документування, людського контролю й незалежного нагляду.

Запровадження запропонованої моделі має здійснюватися поетапно: інвентаризація систем ІІІ у публічному секторі, підготовка кадрів і методик; прийняття рамкового закону та пакета змін; створення компетентного органу, державного реєстру, системи повідомлень і секторальної взаємодії; повноцінне застосування оцінок, аудитів, перевірок, коригувальних заходів і міжнародного обміну. Заборонені практики мають припинятися без очікування завершення всієї інституційної реформи, тоді як для приведення високоризикових систем у відповідність можуть установлюватися диференційовані перехідні строки.

14. До основних ризиків реалізації віднесено інституційне дублювання, дефіцит міждисциплінарних фахівців, формалізацію оцінок впливу, надмірне засекречування, регуляторне захоплення великими постачальниками, непропорційний адміністративний тягар для малого бізнесу та використання безпекових винятків для обходу гарантій. Їх мінімізація потребує законодавчого розмежування компетенції, конкурсного формування

керівництва й експертних органів, правил несумісності та конфлікту інтересів, публічної звітності, ротації експертів, незалежного аудиту регулятора, пропорційних вимог і спеціального контролю за закритими системами.

Результативність правової та інституційної моделі слід оцінювати не кількістю прийнятих актів, перевірок або санкцій, а якістю мотивування рішень, доступністю пояснення та оскарження, ефективністю людського контролю, зменшенням дискримінаційного впливу й серйозних інцидентів, строками реагування, виконанням приписів і передбачуваністю вимог для відповідальних розробників та користувачів. Постійний правовий моніторинг має охоплювати дані реєстру, звіти про інциденти, результати аудитів, адміністративну й судову практику та завершуватися періодичним переглядом нормативних вимог.

Обмеження використання штучного інтелекту слід розглядати не як сукупність ізольованих заборон, а як цілісний механізм публічного адміністрування, у якому кожна матеріальна вимога має відповідну адміністративну процедуру, визначеного інституційного носія, інформаційний ресурс, форму контролю і засіб юридичного захисту. Поєднання ризик-орієнтованої класифікації, превентивних процедур, гібридної мережевої моделі нагляду та узгодженого пакета законодавчих і підзаконних актів утворює концептуальну основу безпечного, відповідального та інноваційно сприятливого використання ШІ в Україні.

ВИСНОВКИ

За результатами дослідження вирішено наукову проблему щодо розробки теоретико-методологічних та правових засад використання штучного інтелекту в Україні:

1. Обґрунтовано закономірну трансформацію предмета інформаційного права від регулювання відносин щодо обігу інформації до регулювання суспільних відносин, пов'язаних із функціонуванням автономних інтелектуальних систем, здатних формувати юридично значущі рішення.

Необхідним є концептуальне розмежування у межах інформаційно-правового дискурсу загального доктринального поняття «штучний інтелект», що позначає науково-технологічний напрям та систему когнітивних методів обробки інформації, від нормативно-дефінітивної категорії «система штучного інтелекту». ШІ виступає лише концептуальним фундаментом, тоді як саме система ШІ як матеріалізований програмно-апаратний комплекс є безпосереднім об'єктом публічного адміністрування, державного контролю та правового обмеження, оскільки її функціонування здатне генерувати реальні ризики для прав особи.

ШІ як правова категорія являє собою високотехнологічну автономну інтелектуальну систему машинного походження, що характеризується внутрішньою здатністю до динамічної адаптації (самонавчання на основі великих масивів даних) і функціональною спроможністю безпосередньо або опосередковано формувати, оптимізувати чи реалізовувати алгоритмічні рішення (прогнози, рекомендації), які мають юридично значущий характер та можуть створювати потенційні ризики для фундаментальних прав і свобод людини, національної безпеки, демократичного врядування та публічного порядку.

Інтернет речей забезпечує виключно цифрову й апаратну інфраструктуру автоматизованого збирання, первинного передавання та транскордонного обміну даними між пристроями, тоді як штучний інтелект здійснює їх глибокий

інтелектуальний аналіз, когнітивне моделювання та кінцеву реалізацію владних, сервісних або управлінських рішень. Це зумовлює відмінність їхньої правової природи, предмета регулювання, ризиків і доводить вимогу спрямування ризик-орієнтованої правової політики держави не на регулювання технології ІІІ як абстрактного явища, а на встановлення суворих процедурних меж та обов'язків для суб'єктів життєвого циклу конкретних систем штучного інтелекту

2. Аксіолого-правовий вимір використання систем ІІІ формується під впливом гуманістичної та трансгуманістичної моделей технологічного розвитку, співіснування яких визначає сучасні тенденції правового регулювання автономних інтелектуальних систем. Це обумовлює необхідність побудови адміністративно-правового механізму використання штучного інтелекту на засадах людиноцентризму, що забезпечує пріоритет прав людини, збереження людської автономії та належний суспільний контроль за прийняттям юридично значущих рішень із використанням систем штучного інтелекту.

3. Результати проведеного аналізу соціальних очікувань, ризиків і суспільних пересторог щодо використання ІІІ відображають не лише рівень суспільної довіри до автономних алгоритмічних систем, а й виконують функцію емпіричних індикаторів юридично значущих ризиків, пов'язаних із можливим порушенням фундаментальних прав людини, втратою людського контролю над алгоритмічним прийняттям рішень, виникненням алгоритмічної упередженості, розмиванням юридичної відповідальності, загрозами академічній доброчесності, цифровій приватності та суспільній довірі до державних інституцій. Вони повинні враховуватися під час визначення меж адміністративно-правового регулювання.

Ризик-орієнтована модель правового регулювання систем ІІІ має формуватися на основі поєднання правового аналізу із результатами емпіричних соціологічних досліджень, що дає змогу визначати найбільш соціально чутливі сфери застосування ІІІ, забезпечувати диференціацію

правових режимів залежно від рівня потенційних ризиків та своєчасно адаптувати державну правову політику до суспільних очікувань щодо безпечного використання інтелектуальних систем.

4. Виявлено закономірність еволюції міжнародно-правового регулювання систем ШІ від інструментів «м'якого права» (soft law), заснованих на етичних принципах і саморегулюванні, до формування юридично обов'язкової (hard law) ризик-орієнтованої моделі. Кульмінацією цього процесу визначено AI Act, який закріпив екстериторіальний підхід, диференціацію обов'язків суб'єктів за рівнями ризику та систему державного контролю. Сформульовано методологічні засади імплементації цих стандартів у правову систему України з метою інтеграції до єдиного європейського цифрового ринку та забезпечення безпекових вимог в умовах воєнного стану.

5. Сучасна модель адміністративно-правового регулювання використання систем ШІ ґрунтується на функціональному розмежуванні компетенції суб'єктів відповідно до їх ролі у життєвому циклі системи ШІ та рівня впливу на ризики її функціонування. Адміністративно-правовий статус таких суб'єктів визначається не лише сукупністю їх прав і обов'язків, а й покладеними на них функціями щодо створення, постачання, розгортання, використання, оцінювання відповідності, здійснення державного нагляду та управління ризиками. В умовах сучасної людиноцентричної моделі правового регулювання ШІ не набуває самостійної правосуб'єктності, а юридична відповідальність за його функціонування покладається на людину-суб'єкта та інституційних суб'єктів, які здійснюють проєктування, впровадження, експлуатацію та контроль відповідних систем.

Нормативна модель, закріплена в AI Act, трансформувала підхід до визначення адміністративно-правового статусу учасників цих правовідносин, замінивши традиційне визначення суб'єктів за їх організаційно-правовою належністю функціональною моделлю розподілу компетенції, юридичних обов'язків і відповідальності залежно від місця суб'єкта у життєвому циклі системи штучного інтелекту. Функціональна роль у життєвому циклі системи

та обсяг ризиків, на управління якими вони здатні впливати зумовлює диференціацію їх компетенції, юридичних обов'язків і відповідальності

6. Чинне законодавство України: Конституція України, Закони України «Про інформацію», «Про захист персональних даних», «Про адміністративну процедуру», «Про доступ до публічної інформації», «Про публічні електронні реєстри», інші акти інформаційного та адміністративного законодавства, а також Концепція розвитку штучного інтелекту в Україні, програмно-стратегічні документи Міністерства цифрової трансформації України формують нормативні й організаційні передумови використання систем ШІ, однак не утворюють завершеного адміністративно-правового механізму їх регулювання, оскільки не забезпечують комплексного врегулювання всіх елементів життєвого циклу ШІ, процедур оцінювання відповідності, державного нагляду, управління ризиками та спеціального розподілу юридичної відповідальності.

Імплементація міжнародних стандартів має відбуватися не через механічне копіювання норм AI Act, а шляхом побудови цілісної нормативної архітектури: рамкового закону про систем ШІ, взаємоузгоджених змін до інформаційного й адміністративного законодавства, системи підзаконних актів та спеціальних адміністративних процедур, що забезпечить сумісність із правом ЄС та адаптованість до системи публічного адміністрування України на засадах безпечного, відповідального та людиноцентричного використання систем ШІ.

7. Соціально-правові передумови обмеження використання систем ШІ зумовлені об'єктивною необхідністю забезпечення збалансованого поєднання технологічного розвитку, публічних інтересів і належного захисту прав людини в умовах зростання автономності алгоритмічних систем. Людиноцентризм є системоутворюючим доктринальним критерієм правотворення, за яким визначаються допустимі межі алгоритмізації суспільних відносин та інтенсивність регуляторного впливу залежно від рівня ризику для прав людини і публічних інтересів.

Базовим критерієм адміністративно-правового обмеження систем III є характер та інтенсивність його впливу на фундаментальні права. На цій основі обґрунтовано правову диференціацію трьох моделей інтеграції людини в контур функціонування автономних систем: «людина в контурі управління» (*human-in-the-loop*), «людина над контуром управління» (*human-on-the-loop*) та «людина поза контуром управління» (*human-out-of-the-loop*), яка потребує найсуворіших обмежень або заборони застосування у сферах реалізації основоположних прав.

Такий підхід формує теоретичну основу ризик-орієнтованої моделі адміністративно-правового регулювання використання систем III, за якої форма інтеграції людини у процес функціонування алгоритмічної системи визначається ступенем її автономності, рівнем потенційного ризику та юридичною значущістю наслідків ухвалюваних рішень.

8. Сучасне міжнародно-правове регулювання використання систем III в автономних системах озброєння перебуває на етапі формування та ґрунтується переважно на нормах міжнародного гуманітарного права, практиці Міжнародного Комітету Червоного Хреста, документах ООН і концепції *meaningful human control*, що відображає загальну тенденцію до недопущення повної автономізації застосування летальної сили.

Обґрунтовано застосування функціонально-правового підходу до визначення меж використання систем III в автономних системах озброєння, де ключовим критерієм є реальна здатність людини здійснювати юридично значущий контроль над вибором цілі, прийняттям рішення про застосування летальної сили та особисто нести персональну відповідальність за наслідки. Концепцію *meaningful human control* визначено не як технічну характеристику архітектури, а як самостійний функціонально-правовий стандарт оцінки допустимості застосування систем III та відповідності його функціонування принципам міжнародного гуманітарного права, що виключає можливість повного делегування алгоритмам права на застосування сили.

Такий підхід забезпечує перехід від формальної оцінки моделей взаємодії людини й алгоритму до змістовної правової оцінки спроможності людини залишатися суб'єктом прийняття рішень і юридичної відповідальності, що виключає можливість делегування ІІІ автономного права на застосування летальної сили.

9. Адміністративно-правова допустимість автономії медичного ІІІ має оцінюватися не за ступенем автоматизації процесів, а за спроможністю забезпечення ефективного людського контролю над клінічно значущими рішеннями. Диференційовано правові режими використання систем ІІІ в медицині: автономні режими визначено допустимими виключно під час виконання допоміжних аналітичних, скринінгових та дослідницьких завдань. Натомість на етапах встановлення діагнозу, вибору протоколу лікування та прийняття клінічно значущих рішень обов'язковим є збереження безпосереднього людського контролю лікаря як гаранта прав пацієнта та суб'єкта юридичної відповідальності.

10. Сформульовано концепцію правової недопустимості алгоритмічної деформації дискреційних повноважень правоохоронних органів, яка виключає існування автономного алгоритмічного правозастосування, підміну індивідуального юридичного розсуду уповноваженої особи та ухвалення рішень, що породжують правові наслідки, без їх змістовної перевірки людиною.

Правомірні межі використання систем ІІІ у цій сфері визначають його як допоміжний інструмент інформаційно-аналітичної підтримки, прогнозування, біометричної ідентифікації та аналізу великих масивів даних. Допустимим застосування транскордонних баз даних розпізнавання обличчя в умовах відсічі збройній агресії (для ідентифікації військовополонених, загиблих, зниклих безвісти та воєнних злочинців) є виключно за наявності чіткої правової підстави, легітимної мети та жорстких часових і просторових обмежень. Необхідним є подолання інфраструктурної фрагментарності органів правопорядку через створення єдиного інтегрованого аналітичного простору на

принципах Data Science із обов'язковим логуванням дій та деідентифікацією осіб на ранніх етапах обробки.

11. У сфері правосуддя змістовний людський контроль є самостійною процесуальною гарантією реалізації права на справедливий суд, оскільки виключно суддя здатний здійснювати індивідуалізовану оцінку обставин справи на засадах справедливості й пропорційності. Використання систем ШІ є допустимим лише як допоміжного інформаційно-аналітичного інструменту для автоматизації технічних процесів, пошуку правової інформації та підготовки проєктів документів, і не може поширюватися на оцінку доказів, формування внутрішнього переконання судді та тлумачення норм права. Застосування систем із закритою логікою, автоматизоване прогнозування чи ухвалення судових рішень створюють пряму загрозу ст. 6 Конвенції про захист прав людини і основоположних свобод, через що обов'язковими умовами використання ШІ є його пояснюваність, прозорість та можливість незалежного аудиту й відхилення алгоритмічних висновків суддею.

Сучасні міжнародні стандарти, сформовані практикою ЄСПЛ, Європейською етичною хартією CEREJ, AI Act, рекомендаціями CNIL та іншими міжнародними документами, відображають єдину концепцію, відповідно до якої системи ШІ повинні посилювати ефективність здійснення правосуддя, але не можуть підміняти суддівський розсуд, незалежність суду та процесуальні гарантії реалізації права людини на справедливий суд.

12. Особливості правового регулювання використання систем ШІ в освіті та науковій діяльності визначаються необхідністю забезпечення балансу між цифровою модернізацією освітнього процесу та збереженням людської суб'єктності як основоположної цінності академічного середовища. Правові межі використання систем ШІ у цій сфері повинні визначатися не рівнем технологічних можливостей алгоритмічних систем, а характером їхнього впливу на самостійну когнітивну діяльність здобувачів освіти, педагогічний розсуд викладача, академічну свободу та академічну доброчесність.

Допустимими межами використання систем ШІ в освіті та науці є їх застосування для інформаційного пошуку, аналітичної обробки даних, мовного й технічного редагування, візуалізації інформації, автоматизації адміністративних процесів та інших допоміжних функцій, що не заміщують інтелектуальну діяльність людини, тоді як недопустимим є використання алгоритмічних систем для імітації авторства, підміни самостійної когнітивної діяльності, заміщення педагогічного розсуду, формування наукових результатів без належного творчого осмислення, а також прийняття остаточних рішень щодо оцінювання результатів навчання, якщо вони істотно впливають на освітню чи професійну траєкторію особи.

Академічна доброчесність в умовах поширення генеративних технологій повинна забезпечуватися не шляхом загальної заборони використання систем ШІ, а через нормативне розмежування допустимих і недопустимих способів його застосування, обов'язок декларування використання генеративних систем, прозорість алгоритмічної підтримки та збереження персональної відповідальності автора за результати освітньої й наукової діяльності.

Використання високоризикових систем ШІ для оцінювання знань, формування освітніх траєкторій, прокторингу та інших рішень, здатних впливати на реалізацію права на освіту, потребує обов'язкового людського контролю, можливості перевірки й оскарження алгоритмічних висновків, а також забезпечення недискримінаційності, захисту персональних даних, академічної свободи та інституційної автономії закладів освіти й науки.

13. Сучасна модель адміністративно-правового регулювання використання систем ШІ повинна базуватися на ризик-орієнтованій правовій політиці, за якої інтенсивність адміністративно-правового впливу, зміст адміністративних процедур, обсяг державного контролю та характер правових обмежень визначаються не видом технології чи сферою її застосування, а рівнем потенційної загрози для життя і здоров'я людини, національної безпеки, прав і свобод людини, демократичного врядування та верховенства права.

Розроблено авторський аксіологічний ризик-орієнтований тест адміністративно-правової оцінки допустимості використання систем ІІІ, який, на відміну від функціональної моделі класифікації ризиків, покладеної в основу AI Act, ґрунтується на ієрархії конституційних та міжнародно визнаних правових цінностей і передбачає послідовне оцінювання потенційного впливу ІІІ на життя і здоров'я людини, національну безпеку та стійкість держави, права, свободи й законні інтереси людини, а також демократичне врядування, верховенство права та інституційну спроможність держави, що забезпечує універсальний адміністративно-правовий механізм визначення допустимості використання систем штучного інтелекту незалежно від сфери їх застосування.

Визначено принцип пропорційності адміністративно-правового впливу, який повинен визначати не лише інтенсивність державного контролю, а й зміст адміністративних процедур, обсяг документації, характер людського контролю, рівень прозорості, періодичність адміністративного аудиту, післяринкового моніторингу та реагування на інциденти відповідно до ступеня ризику конкретної системи штучного інтелекту, що забезпечує адаптивність правового регулювання до розвитку цифрових технологій і виключає застосування уніфікованих регуляторних вимог до систем із різним рівнем потенційної небезпеки.

Запропоновано розглядати ризик-орієнтовану модель адміністративно-правового регулювання як безперервний цикл адміністративного управління, який охоплює попередню ідентифікацію та класифікацію ризиків, формування паспорта ризику системи штучного інтелекту, перевірку законної мети та менш обмежувальних альтернатив, оцінювання впливу на права людини (HRIA/FRIA), оцінку відповідності, управління даними, державну реєстрацію, забезпечення змістовного людського контролю, адміністративний аудит, післяринковий моніторинг, повідомлення про інциденти, застосування коригувальних заходів та забезпечення права особи на перегляд і оскарження алгоритмічно підтриманих рішень протягом усього життєвого циклу системи.

Доцільним є запровадження паспорта ризику систем ІІІ як базового адміністративного документа, що забезпечує узгодженість усіх процедур оцінювання ризиків, оцінки відповідності, НРІА/ФРІА, державного нагляду та взаємодії компетентних органів. Ризик-орієнтована модель повинна передбачати динамічну перекласифікацію систем ІІІ після зміни їх функціонального призначення, рівня автономності, масштабів використання, інтеграції з державними інформаційними ресурсами або виявлення нових ризиків, а також обов'язкове документування кожного адміністративного рішення щодо допуску системи до експлуатації.

Правове регулювання використання високоризикових систем ІІІ має здійснюватися у межах єдиного адміністративного дос'є, яке акумулює результати класифікації ризиків, НРІА/ФРІА, оцінки відповідності, державної реєстрації, адміністративних аудитів, моніторингу, повідомлень про інциденти та прийнятих адміністративних актів, забезпечуючи простежуваність усього життєвого циклу системи. Запропонована модель адміністративних процедур створює цілісний механізм AI governance, який поєднує превентивний захист прав людини, принцип людиноцентризму, належне врядування, адміністративно-процедурні гарантії, підтримку інновацій та виконання євроінтеграційних зобов'язань України шляхом імплементації найкращих міжнародних стандартів без їх механічного копіювання.

14. Сучасна вітчизняна модель публічного адміністрування використання систем ІІІ повинна ґрунтуватися на мережевій (гібридній) системі управління, яка забезпечує розмежування політичних, регуляторних, контрольно-наглядових, правозахисних, експертних і судових функцій та виключає концентрацію всіх повноважень у межах одного органу. Запропоновано інституційну модель публічного адміністрування використання систем ІІІ, яка визначає функціональну систему суб'єктів формування державної політики, регулювання, нагляду, контролю, сертифікації, оцінки відповідності, незалежного аудиту та захисту прав людини.

Оптимальна для України модель повинна поєднувати Кабінет Міністрів України як суб'єкта формування державної політики, Міністерство цифрової трансформації України як центрального координатора розвитку та методичного забезпечення, функціонально незалежний національний компетентний орган як суб'єкта державного нагляду і застосування заходів реагування, секторальних регуляторів, Уповноваженого Верховної Ради України з прав людини, органи стандартизації, акредитації й оцінки відповідності, незалежних аудиторів, науково-консультативну раду та адміністративні суди як взаємопов'язану систему AI governance.

Доцільним є законодавче запровадження функціональної матриці компетенції, яка визначає для кожної адміністративної процедури провідний орган, суб'єктів погодження, консультативної участі, адміністративного й судового оскарження, що забезпечує усунення дублювання повноважень, компетенційних конфліктів і фрагментарності державного регулювання.

Логічним є створення єдиного електронного адміністративного дос'є високоризикової системи III, яке акумулює матеріали класифікації ризиків, HRIA/FRIA, оцінки відповідності, державної реєстрації, адміністративних аудитів, повідомлень про інциденти, застосованих заходів реагування, результатів перевірок та судового контролю, забезпечуючи простежуваність адміністративних процедур протягом усього життєвого циклу системи.

Контрольно-наглядова діяльність у сфері використання систем III повинна здійснюватися за ризик-орієнтованою моделлю, яка передбачає проведення планових і позапланових перевірок залежно від категорії ризику, історії інцидентів, масштабів використання, суттєвих модифікацій системи та результатів попередніх аудитів, із наданням компетентному органу права доступу до технічної документації, журналів подій, тестових середовищ і можливості застосування тимчасового обмеження використання системи у разі неможливості підтвердження її безпечності та законності.

Обґрунтовано посилення ролі Уповноваженого Верховної Ради України з прав людини шляхом надання права ініціювати перевірки, отримувати

матеріали HRIA/FRIA, брати участь у розгляді системних інцидентів, звертатися до суду в інтересах осіб та подавати обов'язкові до розгляду рекомендації щодо усунення алгоритмічної дискримінації і порушень інформаційних прав.

Запропоновано комплексну модель нормативного забезпечення функціонування інституційної системи, основу якої становить розроблений проєкт рамкового Закону України «Про безпечне та відповідальне використання систем штучного інтелекту», а також взаємоузгоджений пакет законодавчих змін до Законів України «Про адміністративну процедуру», «Про захист персональних даних», «Про доступ до публічної інформації», «Про публічні електронні реєстри», «Про публічні закупівлі» та інших законодавчих актів. Передбачено законодавче врегулювання алгоритмічно підтриманих адміністративних актів шляхом доповнення Закону України «Про адміністративну процедуру» статтею 69¹, яка встановлює заборону ухвалення негативного адміністративного акта виключно на підставі результату функціонування системи штучного інтелекту за наявності дискреційних повноважень, обов'язок посадової особи здійснювати самостійну оцінку фактичних обставин і пропорційності втручання, забезпечувати фіксацію алгоритмічного сліду, людський перегляд та можливість повноцінного адміністративного й судового контролю.

Необхідним є нормативне закріплення права особи на отримання інформації про використання систем ШІ, змістовного пояснення алгоритмічно підтриманого рішення, людського перегляду, заперечення автоматизованої обробки, захисту від алгоритмічної дискримінації та оскарження результатів використання систем штучного інтелекту.

Запропоновано створення державного реєстру високоризикових систем ШІ, впровадження регуляторного експериментального середовища (AI Sandbox), спеціального порядку проведення HRIA/FRIA, інтегрованої системи повідомлення про серйозні інциденти та поетапної дорожньої карти імплементації законодавства, що забезпечує функціональну еквівалентність

української моделі європейським стандартам AI Act без їх механічного відтворення.

15. Сформовано цілісну концепцію вдосконалення законодавства України та механізмів публічного адміністрування у сфері використання систем ШІ, спрямовану на формування комплексної адміністративно-правової моделі його безпечного, людиноцентричного та ризик-орієнтованого використання, а також надані пропозиції до окремих галузевих законів зі сфер правовідносин, які були проаналізовані у дослідженні (Додатки Д, Е).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адміністративне право України : підручник / Т. О. Коломоєць, П. С. Лютіков, О. Ю. Меліхова та ін. ; за заг. ред. Т. О. Коломоєць. Вид. 2-ге, змін. і допов. Київ : Істина, 2012. 528 с.
2. Андрощук Г. О. Штучний інтелект: економіка, інтелектуальна власність, загрози (ч. 1). *Теорія і практика інтелектуальної власності*. 2021. № 2. С. 56–74. URL: <https://uran.inprojournal.org/article/view/236555>
3. Андрощук Г. О. Штучний інтелект: економіка, інтелектуальна власність, загрози (ч. 2). *Теорія і практика інтелектуальної власності*. 2021. № 3. С. 45–56. URL: http://nbuv.gov.ua/UJRN/Triv_2021_3_6
4. Андрощук А. Г., Малюга О. С. Використання штучного інтелекту у вищій освіті: стан і тенденції. *International Science Journal of Education & Linguistics*. 2024. Vol. 3, No. 2. P. 27–35. URL: <https://isg-journal.com/isjel/article/view/661>
5. Андрощук Г., Работягова Л. Технології розпізнавання обличчя: проблеми регулювання в Україні. *Теорія і практика інтелектуальної власності*. 2022. № 1. С. 66–77. URL: <https://inprojournal.org/2022-1-7/>
6. Апаров А. М. Концептуальні проблеми співвідношення понять «правосуб'єктність», «юридична особа» та «суб'єкт права» у сучасній теорії права. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична*. 2024. Вип. 41. С. 574–580. URL: <https://nzlubp.org.ua/index.php/journal/article/view/1495>
7. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти : монографія / за заг. ред. О. М. Бандурки. Харків : Вид-во Ун-ту внутр. справ, 2000. 368 с.
8. Арістова І. В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади : дис. ... д-ра юрид. наук : 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Харків, 2002. 496 с.

9. Арістова І. В. Роль інформаційної сфери та науки «Інформаційне право» у досягненні цілей сталого розвитку в умовах цифрової трансформації в Україні. *Аналітично-порівняльне правознавство*. 2025. № 4. Ч. 2. С. 92–96. URL: <https://app-journal.in.ua/wp-content/uploads/2025/08/16-1.pdf>
10. Арістова І. В. Система права України в умовах інформаційного суспільства та цифрової економіки. *Приватне та публічне право*. 2020. № 3. С. 44–51. URL: http://pp-law.in.ua/archive/3_2020/11.pdf
11. Арістова І. В. Становлення науки інформаційне право: питання методології (частина 2). *Публічне право*. 2016. № 3. С. 102-110. URL: http://nbuv.gov.ua/UJRN/pp_2016_3_16
12. Арістова І. В., Карпик Ю. А. Вплив цифрової економіки та європейської інтеграції на правотворчість у сфері інтелектуальної власності в умовах розбудови інформаційного суспільства та інформаційного законодавства в Україні. *Modern researches: progress of the legislation of Ukraine and experience of the European Union : collective monograph*. Riga : Izdevniecība «Baltija Publishing», 2020. Р. 255–288. URL: <https://drive.google.com/file/d/13W4E-mK4WKOnZC6WTkMSQ-cmE1pwfU16/view>
13. Баранов О. А. Визначення терміну «штучний інтелект». *Інформація і право*. 2023. № 1 (44). С. 32–49. URL: https://ippi.org.ua/sites/default/files/5_28.pdf
14. Баранов О. А. Ідентифікація робота з штучним інтелектом як суб'єкта права. *Інтернет речей: проблеми правового регулювання та впровадження* : матеріали II наук.-практ. конф. (м. Київ, 29 лист. 2018 р.) / упоряд. В. М. Фурашев, С. О. Дорогих. Київ : КПП ім. Ігоря Сікорського, Вид-во «Політехніка», 2018. С. 8–12. URL: <https://ippi.org.ua/internet-rechei-problemi-pravovogo-regulyuvannya-ta-vprovadzhennya-0>
15. Баранов О. А. Інтернет речей і штучний інтелект: витоки проблеми правового регулювання. *ІТ-право: проблеми та перспективи розвитку в Україні* : матеріали II Міжнар. наук.-практ. конф. (м. Львів, 17 листоп. 2017 р.). Львів :

НУ «Львівська політехніка», 2017. С. 18-42. URL: https://d1wqtxts1xzle7.cloudfront.net/55034651/itlawkonfer_2017_-libre.pdf

16. Баранов О. А. Інтернет речей (IoT): огляд правових проблем. *Інтернет речей: проблеми правового регулювання та впровадження : матеріали наук.-практ. конф.* (м. Київ, 24 жовт. 2017 р.). Київ : КПП ім. Ігоря Сікорського, 2017. С. 7–15. URL: https://ippi.org.ua/sites/default/files/zbirnik_2017__14.11.2017_-_vidredagovaniy.pdf

17. Баранов О. А. Інтернет речей (IoT): робот зі штучним інтелектом у правовідносинах. *Юридична Україна*. 2018. № 5–6. С. 75–95.

18. Баранов О. А. Інтернет речей: теоретико-методологічні основи правового регулювання. Т. 1. Сфери застосування, ризики і бар'єри, проблеми правового регулювання : монографія. Київ : Видавничий дім «АртЕк», 2018. 342 с.

19. Баранов О. А. «Інтернет речей» як правовий термін. *Юридична Україна*. 2016. № 5–6. С. 96–103. URL: http://nbuv.gov.ua/UJRN/urykr_2016_5-6_16

20. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика : монографія. Київ : Едельвейс, 2014. 497 с. URL: https://ippi.org.ua/sites/default/files/baranov_monografiya.pdf

21. Баранов О. А. Цивілізаційна місія цифрових трансформацій. *Інформація і право*. 2023. № 3 (46). С. 25–41. URL: <https://il.ippi.org.ua/article/view/287067>

22. Бачило І. Л., Соснін О. В. Інформаційне право як запорука інноваційного розвитку нації. *Віче*. 2012. № 1. С. 12–14. URL: <https://veche.kiev.ua/journal/2930/>

23. Бердник О. Інтернет речей як основна сучасна уразливість для інформаційної безпеки користувачів. *Світ телекомунікації та інформатизації : зб. матеріалів міжнар. наук.-техн. конф.* (м. Київ, 7 груд. 2017 р.). Київ, 2017. С. 300–302. URL: https://duikt.edu.ua/uploads/n_5218_58757739.pdf

24. Берназюк І. М. Рамкова конвенція Ради Європи про штучний інтелект у контексті захисту прав людини: виклики та значення для України. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2026. Т. 3, № 93. С. 18–30. URL: <https://visnyk-pravo.uzhnu.edu.ua/article/view/354445>

25. Берназюк І. М. Штучний інтелект і права людини: виклики для Європейської конвенції з прав людини. *Аналітично-порівняльне правознавство*. 2025. Вип. 3. ч. 1. С. 89–99. URL: <https://app-journal.in.ua/wp-content/uploads/2025/06/14.pdf>

26. Бегун А. В., Старіна Е. І. Особливості інформаційного права в контексті штучного інтелекту. *Моделювання та інформаційні системи в економіці : зб. наук. пр.* Київ : Київський національний економічний університет імені Вадима Гетьмана, 2023. Вип. 103. С. 37–46. URL: <https://ir.kneu.edu.ua/handle/2010/48354>

27. Бесчастний В. М., Костицький М. В., Кушакова-Костицька Н. В. Цифровий конституціоналізм: нова парадигма та перспективи розвитку в Україні. *Філософські та методологічні проблеми права*. 2022. № 2 (24). С. 9–26. DOI: <https://doi.org/10.33270/02222402.9>

28. Бочкова І. І., Врублевська-Місюна К. М. Правове регулювання використання штучного інтелекту в сфері освіти: захист прав студентів та викладачів. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Вип. 90, ч. 2. С. 23–29. DOI: <https://doi.org/10.24144/2307-3322.2025.90.2.3>

29. Брижко В. М. До гносеології категорії «інформація». *Інформація і право*. 2011. № 2 (2). С. 13–20. URL: <https://nasplib.isoftware.kiev.ua/bitstreams/da58ffcd-4d24-48eb-96a8-687d0b850e59/download>

30. Брижко В. М. Про узгодженість понять у сфері інформаційного права. *Правова інформатика*. 2009. № 1 (21). С. 39–45. URL: https://ippi.org.ua/sites/default/files/09bvmsip_1.pdf

31. Брижко В. М., Фурашев В. М. Інформаційне право та інформаційне законодавство : наукове видання. 2-ге вид., допов. Харків : Право, 2021. 288 с.
32. Бусол О. Ю. Потенційна небезпека штучного інтелекту. *Інформація і право*. 2015. № 2 (14). С. 121–128. URL: <http://il.ippi.org.ua/article/view/272708>
33. Варинський В. О. AI Act як ризик-орієнтована модель правового обмеження застосування штучного інтелекту у правоохоронній діяльності та діяльності спецслужб. *Південноукраїнський правничий часопис*. 2026. № 1. С.134-141. URL: <https://sulj.oduvs.od.ua/archive/2026/1/25.pdf>
34. Варинський В. Алгоритмічне забезпечення охорони громадського порядку: правові межі застосування штучного інтелекту у діяльності правоохоронних органів. *Академічні візії*. № 48. 2025. URL: <https://www.academy-vision.org/index.php/av/article/view/3189>
35. Варинський В. Етичні та правові ризики застосування штучного інтелекту у правоохоронній діяльності та діяльності спецслужб. *Вісник Петенціарної асоціації України*. 2026. №1. С. 245-256. URL: <https://doi.org/10.34015/2523-4552.2026.1.22>
36. Варинський В. О. Нормативне регулювання використання штучного інтелекту у правосудді. *Eastern Law*. 2024. URL: https://easternlaw.com.ua/wp-content/uploads/2014/02/varynskyi_146.pdf
37. Варинський В. Основні підходи правового регулювання використання штучного інтелекту в освіті. *Актуальні проблеми вдосконалення чинного законодавства України. Збірник наукових праць*. 2025. № 69. С. 140-151. URL: <https://journals.pnu.edu.ua/index.php/apiclu/article/view/10297/10007>
38. Варинський В. О. Оцінка впливу високоризикових систем штучного інтелекту на права людини як інструмент правової політики України. *Академічні візії*. № 55. 2026. URL: <https://www.academy-vision.org/index.php/av/article/view/3275/3115>
39. Варинський В.О. Правова парадигма довіри до штучного інтелекту (Частина II). *Право і суспільство*. 2026. № 1. С. 258-264. URL: https://pravoisuspilstvo.org.ua/archive/2026/1_2026/part_1/35.pdf

40. Варинський В. Правове регулювання обмеження використання штучного інтелекту в медицині: основні міжнародні підходи. *Український часопис міжнародного права*. 2026. № 1. С. 21-33. URL: <https://jusintergentes.com.ua/images/2026/1/21-33.pdf>
41. Варинський В. Правосуб'єктність штучного інтелекту: міф чи реальність. *Юридична Україна*. 2024. № 11. 60-68. URL: <https://yur-ukraine.com/pravosubyektnist-shtuchnogo-intelektu-mif-chy-realnist-2/>
42. Варинський В. Правосуб'єктність штучного інтелекту: критичний погляд на автономність. *Інформація і право*. 2024. № 4 (51). 83-94. URL: [https://doi.org/10.37750/2616-6798.2024.4\(51\).317919](https://doi.org/10.37750/2616-6798.2024.4(51).317919)
43. Варинський В.О. Соціально-правові чинники формування довіри до штучного інтелекту (Частина 1). *Право і суспільство*. 2025. № 6. С. 524-532. URL: http://pravoisuspilstvo.org.ua/archive/2025/6_2025/75.pdf
44. Варинський В. Стан правового регулювання використання штучного інтелекту у законодавстві України. *Юридична Україна*. 2025. № 1. URL: <https://yur-ukraine.com/stan-pravovogo-regulyuvannya-vykorystannya-shtuchnogo-intelektu-u-zakonodavstvi-ukrayiny>
45. Варинський В. Сучасні напрямки соціально-правових досліджень штучного інтелекту. *Наукові перспективи (Naukovі perspektivi)*. 2022. №. 12 (30). С.299-310. URL: [https://doi.org/10.52058/2708-7530-2022-12\(30\)-299-310](https://doi.org/10.52058/2708-7530-2022-12(30)-299-310)
46. Варинський В. Штучний інтелект в освіті: проблеми впровадження та регулювання. Створювальна сила знання : монографія. Книга друга / авт. кол. ; відп. ред.: І. А. Доннікова, Н. В. Кривцова. Одеса : Фенікс, 2025. С. 145-164. URL: https://repository.onma.edu.ua/id/eprint/717/1/Stvor_Syla_mono_.pdf
47. Василенко В. М. Інтеграція систем штучного інтелекту в державне управління: ризики, правові виклики та безпекові гарантії. *Вісник Кримінологічної асоціації України*. 2025. Т. 35, № 2, ч. 2. С. 574–585. URL: <https://vca.univd.edu.ua/index.php/vca/article/view/676>
48. Василенко В. М. Принципи громадського контролю за діяльністю Національної поліції. *Європейські перспективи*. 2018. № 4. С. 93–99. URL:

<https://dspace.univd.edu.ua/items/684f45e5-b3e8-44af-a9ea-d2f69eb0eda1>

49. Василенко В. М. Цифрова трансформація правоохоронних органів: ризики в умовах гібридних загроз та шляхи їх подолання. *Вісник Кримінологічної асоціації України*. 2024. Т. 32, № 2. С. 945–958. URL: <https://vca.univd.edu.ua/index.php/vca/article/view/433>

50. Віннікова Н. А. Штучний інтелект в контексті глобального управління. *Політікус*. 2022. Вип. 3. С. 65–70. URL: https://www.politicus.od.ua/3_2022/10.pdf

51. Войнов М. Штучний інтелект в медицині: чи загрожують інновації правам людини? *Українська Гельсінська спілка з прав людини*. URL: <https://www.helsinki.org.ua/articles/shtuchnyy-intelekt-v-medytsyni-chy-zahrozhuut-innovatsii-pravam-liudyny/>

52. Використання штучного інтелекту населенням України. *Київський міжнародний інститут соціології*. 26 берез. 2026. URL: <https://www.kiis.com.ua/?cat=reports&id=1599&lang=ukr&page=1>

53. Галуцько В. В. Адміністративно-правові відносини: алгоритм дослідження суспільних відносин. *Наукові записки. Серія: Право*. 2017. Вип. 1. С. 4–10. URL: https://cusu.edu.ua/images/nauk_zapiski/pravo/1_2017/4-10.pdf

54. Гиляка О. С. Новітні технології та права людини: аналіз деяких критичних проблем цифрової ери. *Вісник Національної академії правових наук України*. 2023. Т. 30, № 2. С. 15–30. URL: <https://visnyk.kh.ua/uk/journals/visnik-naprn-2-2023-r/novitni-tekhnologiyi-ta-prava-lyudini-analiz-deyakikh-kritichnikh-problem-tsifrovoyi-eri>

55. Гиляка О. С., Петришин О. В. Права людини в цифрову епоху: виклики, загрози та перспективи. *Вісник Національної академії правових наук України*. 2021. Т. 28. № 1. С. 17–35. URL: https://visnyk.kh.ua/web/uploads/pdf/Вісник%20НАПрНУ_Том%2028_1_2021_15-23.pdf

56. Гловюк І. В. Апеляційна скарга з галюцинаціями штучного інтелекту: висновки на майбутнє з одного кейсу у кримінальному провадженні.

Науковий вісник Ужгородського національного університету. Серія: Право. 2026. Вип. 93, ч. 5. С. 46–52. URL: <https://visnyk-pravo.uzhnu.edu.ua/article/view/355844>

57. Голосніченко І. П., Стахарський М. Ф., Золотарьова Н. І. *Адміністративне право України: основні поняття : навч. посіб. / за заг. ред. І. П. Голосніченка.* Київ : ГАН, 2005. 232 с.

58. Гончарук В. Л. Сучасні загрози економічній безпеці України в умовах збройної агресії: ризик-орієнтована модель державного управління. *Публічне управління та митне адміністрування.* 2025. № 4(47). С. 167–172.

59. Горбовський А. І., Войтович О. П. Дослідження безпеки у системах Інтернету речей. *Репозитарій Вінницького національного технічного університету.* URL: <http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/17277/2805.pdf>

60. Городиський І. М. Тенденції розвитку правового регулювання штучного інтелекту в Європейському Союзі. *ІТ-право: проблеми та перспективи розвитку в Україні : матеріали II Міжнародної наук.-практ. конф. (м. Львів, 17 листоп. 2017 р.).* Львів : НУ «Львівська політехніка», 2017. С. 51–57.

61. Гребенюк А. М., Прокопов С. О., Рибальченко Л. В. Використання технологій розпізнавання обличчя на відео- та фотозображеннях : методичні рекомендації. Дніпро : Дніпропетровський державний університет внутрішніх справ, 2023. 48 с.

62. Грохольський В. Л. Концептуальні підходи до адміністративно-правового забезпечення захисту прав, свобод і законних інтересів людини і громадянина окремими державними інституціями в європейських країнах. *Південноукраїнський правничий часопис.* 2022. № 4, ч. 1. С. 208–213. URL: https://www.sulj.oduvs.od.ua/archive/2022/4/part_1/31.pdf

63. Губанова Т. О. Використання штучного інтелекту в діяльності органів публічної влади: адміністративно-правове регулювання. *Київський юридичний журнал.* 2025. № 8. С. 11–18. URL:

<https://journals.fpk.kyiv.ua/index.php/kyivlawjournal/article/view/80>

64. Гумін О. М., Пряхін Є. В. Адміністративно-правовий статус особи: поняття та структура. *Наше право*. 2014. № 5. С. 32–37. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/5312/1/Пряхін%20Nashp_2014_5_7.pdf

65. Даніліян В. О. Інформаційне суспільство та перспективи його розвитку в Україні (соціально-філософський аналіз) : автореф. дис. на здобуття наук. ступеня канд. філософ. наук : спец. 09.00.03 «Соціальна філософія та філософія історії». Харків, 2006. 19 с. URL: https://library.nlu.edu.ua/POLN_TEXT/KNIGI/Monography_Danilian_O_V.pdf

66. Демчук Т. І. Інформаційно-аналітичні та організаційні методи правоохоронної діяльності. *Аналітично-порівняльне правознавство*. 2025. № 5, ч. 2. С. 144–148. URL: <https://app-journal.in.ua/wp-content/uploads/2025/10/23-1.pdf>

67. Денисова А. В. Адміністративна правосуб'єктність органів виконавчої влади як суб'єктів адміністративного нагляду: науковий підхід до характеристики. *Право і суспільство*. 2017. № 4. С. 143–147. URL: <https://elar.navs.edu.ua/server/api/core/bitstreams/41229bad-97bc-4005-91ed-12a57172fa69/content>

68. Денисова А. В. Діалектика й системний підхід як основа методології дослідження проблеми адміністративного нагляду органів виконавчої влади України. *Право і суспільство*. 2016. № 6. С. 108–113. URL: <https://elar.navs.edu.ua/server/api/core/bitstreams/e437c775-e8c9-4aa3-9e43-65a92ec3aff6/content>

69. Денисова А. В. Напрями адміністративного нагляду у сфері забезпечення безпеки життєдіяльності населення: питання систематизації. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2017. Вип. 43, т. 4. С. 127–130. URL: <https://dspace.onua.edu.ua/bitstreams/789f7a10-6bff-47dc-a25a-c1d4a11f5f18/download>

70. Діагностика. *Енциклопедія сучасної України* / Інститут енциклопедичних досліджень НАН України, URL: <https://esu.com.ua/article-24448>
71. Добровольська О. В., Штанько В. І. Філософський аналіз еволюції штучного інтелекту. *Дослідження з історії і філософії науки і техніки*. 2019. Т. 28, № 2. С. 43–64. URL: http://nbuv.gov.ua/UJRN/studhphst_2019_28_1_4.
72. Довгань О. Д. Глобалізаційні процеси в інформаційній сфері та їх вплив на інформаційну безпеку. *Часопис Київського університету права*. 2015. № 1. С. 114–118. URL: https://kup.edu.ua/doc/chasopis/chasopis_2015_1.pdf
73. Довгань О. Д., Ткачук Т. Ю. Artificial General Intelligence: новий етап глобальної правової дискусії. *Інформація і право*. 2026. № 1 (56). С. 67–81. DOI: [https://doi.org/10.37750/2616-6798.2026.1\(56\).357246](https://doi.org/10.37750/2616-6798.2026.1(56).357246)
74. Дослідницька служба Верховної Ради України. Аналітична записка з питань порівняльного законодавства щодо нормативно-правового регулювання технологій штучного інтелекту в Україні, Європі та США. Київ, 2025. URL: <https://research.rada.gov.ua/uploads/documents/33722.pdf>
75. Електронна система охорони здоров'я України (ЕСОЗ). Офіційний вебсайт. URL: <https://ehealth.gov.ua/>
76. Етичний кодекс ІІІ: Bosch встановлює корпоративні правила використання штучного інтелекту. Офіційний вебсайт Bosch в Україні. URL: <https://www.bosch.ua/news-and-stories/ai-code-of-ethics/>
77. Женевські конвенції про захист жертв війни від 12 серп. 1949 р. та Додаткові протоколи до них від 08 черв. 1977 р. URL: https://zakon.rada.gov.ua/laws/main/995_151
78. Жигалкін І. П. Система принципів трудового права України: проблеми сучасної теорії і практики : монографія. Харків: Право, 2015. 360 с.
79. Жураковський Б. Ю., Зенів І. О. Технології Інтернету речей : навч. посіб. Київ : КПІ ім. Ігоря Сікорського. 2021. 271 с. URL: <https://ela.kpi.ua/server/api/core/bitstreams/dcd9e1aa-8bcc-4e76-b1e0-ed133bf616b2/content>

80. Завадський А. А. Адміністративно-правове регулювання штучного інтелекту у сфері оборони: міжнародний вимір та національні пріоритети. *Збірник наукових праць Харківського національного педагогічного університету імені Г. С. Сковороди «Право»*. 2024. Вип. 40. С. 87–98.

81. Загальна декларація прав людини : Міжнародний документ від 10 груд. 1948 р. № 995_015. URL: https://zakon.rada.gov.ua/go/995_015

82. Задохайло О. А. Адміністративно-правове регулювання штучного інтелекту в Україні: сучасний стан та тенденції розвитку. *Збірник наукових праць Харківського національного педагогічного університету імені Г. С. Сковороди «Право»*. 2023. № 37. С. 9–14. URL: <https://journals.hnpu.edu.ua/index.php/law/article/view/12451%C2%A0>

83. Залєвський С. В. Правосуб'єктність штучного інтелекту в сфері права інтелектуальної власності: цивільно-правові проблеми. ЛОГОС. ОНЛАЙН URL: <https://www.ukrlogos.in.ua/10.11232-2663-4139.16.51.html>

84. Захарчук І. В. Адаптація міжнародного права до викликів нових технологій: штучний інтелект, автономні системи озброєнь та їх регулювання. *Аналітично-порівняльне правознавство*. 2025. Вип. 4, ч. 3. С. 398–404. DOI: <https://doi.org/10.24144/2788-6018.2025.04.3.58>

85. Заярний О. Інформаційно-правові особливості реалізації світових концепцій «розумного» міста на сучасному етапі цифрової трансформації України. *Право України* 2022. № 8. С. 13–27. DOI: <https://doi.org/10.33498/louu-2022-08-013>

86. Зачек О. І., Дмитрик Ю. І., Сенік В. В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ*. 2023. № 3. С. 148–156. URL: <http://journals.lvduvs.lviv.ua/index.php/law/article/view/637/628>

87. Іващенко С. Правові засади регулювання штучного інтелекту в Україні: сучасний стан та перспективи розвитку. *Адміністративне право і процес*. 2025. № 2. С. 24–32. URL: <https://applaw.net/index.php/journal/article/download/856/717/> С. 29.

88. Інформаційне суспільство в Україні: глобальні виклики та національні можливості : аналіт. доп. / Дубов Д. В., Ожеван О. А., Гнатюк С. Л. Київ : Національний інститут стратегічних досліджень. 2010. 64 с. URL: https://niss.gov.ua/sites/default/files/2011-02/dubov_infsus-31058.pdf

89. Іншин М. І., Щербина В. І. Ідеологічні основи сучасного трудового права України : монографія. Харків : Діса плюс, 2016. 328 с.

90. Каленіченко Л.І. Юридичні аспекти категорії «соціальна відповідальність» у системі суспільних наук. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2014. Вип. 11, т. 1. С. 14–17. URL: <https://dspace.univd.edu.ua/handle/123456789/18306>

91. Калюжний Р. А., Марценюк А. Г. Предмет та методи інформаційного права. *Правова інформатика*. 2008. № 3. С. 5-9. URL: <https://ippi.org.ua/sites/default/files/08kramip.pdf>

92. Калюжний Р. А. Інформаційне забезпечення державного управління (на прикладі системи органів внутрішніх справ). *Державне управління: теорія і практика* / за заг. ред. В. Б. Авер'янова. Київ : Юрінком Інтер, 1998. С. 395–405.

93. Кармаза О. О., Кушерець Д. В. Нормативно-правові джерела регулювання штучного інтелекту: Україна, Європейський Союз, США та Китай. *Юридичний науковий електронний журнал*. 2025. № 8. С. 23–28. DOI: <https://doi.org/10.32782/2524-0374/2025-8/2> .

94. Карчевський М. В. Перспективи правового регулювання в контексті гіпотези розвитку технологій трансгуманізму. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2019. № 1 (85). С. 115–127. URL: <https://rep.dnuvs.ukr.education/server/api/core/bitstreams/c144f0d3-4e84-4622-ae62-2f96e9afabff/content>

95. Карчевський М. В. Правове регулювання соціалізації штучного інтелекту. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2017. № 2 (78). С. 99–108. URL: <https://rep.dnuvs.ukr.education/server/api/core/bitstreams/5ea0f7b5-f3a8-4f21-8b20-e0955718199e/content>

96. Карчевський М. В. Про штучний інтелект та юридичний дискурс. Сайт професора Карчевського. 26 листоп. 2023 р. URL: <https://karchevskiy.com/2023/11/26/про-штучний-інтелект-та-юридичний-дис/>

97. Карчевський М. В. Трирівнева модель правового регулювання ІІІ. *Україна в умовах соціальної та цифрової трансформації: теоретичні моделі правового регулювання штучного інтелекту : матеріали наук.-практ. конф.* (Київ, 5 листоп. 2025 р.) / упоряд.: М. В. Дубняк, С. О. Дорогих, І. Ф. Корж, В. М. Фурашев. Київ; Одеса : Фенікс, 2025. С. 19–26. URL: https://ippi.org.ua/sites/default/files/zbirnik_tez_05.11.2025_1.pdf

98. Карчевський М. В. Штучний інтелект та протидія злочинності. *Використання технологій штучного інтелекту у протидії злочинності : матеріали наук.-практ. онлайн-семінару* (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. С. 32–43. URL: <https://karchevskiy.com/2020/11/06/ai-vs-crime/>

99. Карчевський М. В. Як і чому змінюється юридичний дискурс щодо штучного інтелекту. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання : матеріали Всеукр. наук.-практ. конф.* (м. Київ, 23 листоп. 2023 р.). Київ. 2023. С. 14–20. URL: [https://ippi.org.ua/sites/default/files/konferenciya_2023_socialna_i_cifrova_transfor
maciya_maket.pdf](https://ippi.org.ua/sites/default/files/konferenciya_2023_socialna_i_cifrova_transformaciya_maket.pdf)

100. Карчевський М. В., Куковинець Д. О. Використання технологій штучного інтелекту правоохоронними та судовими органами: світовий досвід та напрями розвитку національного законодавства. *Питання боротьби зі злочинністю*. 2023. Вип. 46. С. 21–31. URL: <https://pbz.nlu.edu.ua/article/view/301290>

101. Катеринчук І. П. Інформаційна підтримка та інформаційна протидія як складові системи інформаційного забезпечення правоохоронних органів. *Південноукраїнський правничий часопис*. 2016. № 2. С. 21–25. URL: <https://sulj.oduvs.od.ua/archive/2016/2/8.pdf>

102. Катеринчук І. П. Проблеми забезпечення інформаційної підтримки

прийняття управлінських рішень. *Право і безпека*. 2013. № 4 (51). С. 138–142.

103. Кешкентій Д. Верховний Суд (України) проти штучного інтелекту: наступ на прогрес чи обґрунтований захист процесуальної добросовісності? URL: <https://www.okremadumka.com/2026/01/26/верховний-суд-україни-проти-штучно/>

104. Коваленко Л. Етапи становлення інформаційного права в Україні. *Вісник академії правових наук України*. 2012. № 2. С. 175-182. URL: http://nbuv.gov.ua/UJRN/vapny_2012_2_20.

105. Коваленко Л. П. Інформаційне право в епоху цифрової трансформації суспільства. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2021. № 52. С. 22–26. URL: https://vestnik-pravo.mgu.od.ua/archive/juspradenc54/part_1/5.pdf

106. Коваленко Л. П. Теоретичні проблеми розвитку інформаційного права України : монографія. Харків : Право, 2012. 248 с.

107. Ковальчук О. Я. Організаційно-правове забезпечення цифровізації судочинства в Україні : дис. ... д-ра юрид. наук : 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Національний університет біоресурсів і природокористування України. Київ, 2025. 573 с. URL: https://www.nubip.edu.ua/sites/default/files/u145/dis_kovalchuk_0.pdf

108. Кодекс адміністративного судочинства України : Кодекс України від 06 лип. 2005 р. № 2747-IV. URL: <https://zakon.rada.gov.ua/go/2747-15>

109. Кодекс України про адміністративні правопорушення : Кодекс України від 07 груд. 1984 р. № 8073-X. URL: <https://zakon.rada.gov.ua/go/8073-10>

110. Кодекс суддівської етики : затв. рішенням XX чергового з'їзду суддів України від 18 верес. 2024 р. URL: <https://zakon.rada.gov.ua/rada/show/n0001415-24>

111. Конвенція про заборону або обмеження застосування конкретних видів звичайної зброї, які можуть вважатися такими, що завдають надмірних ушкоджень або мають невибіркову дію : Конвенція ООН від 10 жовт. 1980 р.

URL: https://zakon.rada.gov.ua/go/995_266

112. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Конвенція Ради Європи від 28 січ. 1981 р. № 108. URL: https://zakon.rada.gov.ua/go/994_326

113. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини) : Конвенція Ради Європи від 04 листоп. 1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004

114. Кононов Д. А. Ризик-орієнтований підхід до бюджетного планування в системі національної безпеки України. *Дослідження та інновації*. 2025. № 3(6). С. 32–35.

115. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-ВР>

116. Корейба Ю. В. Джерела інформаційного права України : автореф. дис. ... канд. юрид. наук : 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Київ, 2015. 22 с.

117. Корж І. Ф. Необхідність встановлення правового статусу штучного інтелекту. *Інформація і право*. 2025. № 4 (55). С. 94–105. URL: <https://il.ippi.org.ua/article/view/346348>

118. Корж І. Ф. Цифровізація та правова безпека в Україні. *Інформація і право*. 2026. № 1 (56). С. 27–39. DOI: [https://doi.org/10.37750/2616-6798.2026.1\(56\).357173](https://doi.org/10.37750/2616-6798.2026.1(56).357173)

119. Корж І. Ф. Штучний інтелект і право. *Право в умовах соціальної та цифрової трансформації* : колективна монографія / за заг. ред. О. А. Баранова, В. М. Фурашева. Київ ; Одеса : Фенікс, 2021. С. 44–61. URL: https://ippi.org.ua/sites/default/files/socialna_i_cifrova_transformaciya_2021.pdf

120. Користін О. О. Щодо дослідження систем та методологій управління ризиками у сфері кібербезпеки. *Актуальність та особливості наукових досліджень в умовах воєнного стану* : зб. матеріалів IV Міжнар. наук.-практ. інтернет-конф. з нагоди відзначення Дня науки–2024 в Україні (м. Київ,

22 трав. 2024 р.). Київ : ДНДІ МВС України, 2024. URL: <https://dspace.nadpsu.edu.ua/bitstream/123456789/4556/1/>

121. Користін О. Є., Свиридюк Н. П. Ризик-орієнтований підхід щодо оцінювання загроз у сфері лісового господарства. *Наука і правоохорона*. 2023. № 2(60). С. 194–202.

122. Кормич Б.А. Інформаційне право : підручник. Харків: БУРУН і К, 2011. 334 с. URL: <https://dspace.onua.edu.ua/server/api/core/bitstreams/9123a0ca-d67b-436c-9abc-148a2d3b8745/content>

123. Кормич Б. А Конституційно-правове регулювання інформаційних відносин. *Юридичний вісник*. 2013. № 3. С. 46–51. URL: https://yurvisnyk.in.ua/v3_2013/10.pdf

124. Корнієнко М. В., Шкута О. О.. Штучний інтелект у кримінальному провадженні, зарубіжний досвід і міжнародно-правові стандарти. Львів–Торунь: Liha-Pres, 2024.

125. Костенко І. В. Штучний інтелект у системі публічного управління: інституційні виклики, управлінські трансформації та нормативно-правові орієнтири. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Вип. 92, ч. 3. С. 206–212. URL: <https://visnyk-pravo.uzhnu.edu.ua/article/view/350546>

126. Костенко О. В. Аналіз національних стратегій розвитку штучного інтелекту. *Інформація і право*. 2022. № 2 (41). С. 58–69. URL: <https://il.ippi.org.ua/article/view/270365>

127. Костенко О. В. Електронна юрисдикція, метавсесвіт, штучний інтелект, цифрова особистість, цифровий аватар, нейронні мережі: теорія, практика, перспективи. *Наукові інновації та передові технології*. 2022. № 2(4). С. 54–78. DOI: [https://doi.org/10.52058/2786-5274-2022-2\(4\)-54-78](https://doi.org/10.52058/2786-5274-2022-2(4)-54-78)

128. Костенко О. В. Напрями розвитку права у сфері Інтернету речей (IoT) та штучного інтелекту. *Актуальні проблеми вітчизняної юриспруденції*. 2021. № 3. С. 130–136. URL: <https://www.researchgate.net/publication/356893915>

129. Костенко С.О. Правовий режим великих мовних моделей та

об'єктів, створених за їх допомогою. Штучний інтелект, сучасні технології та право в Україні : монографія / за заг. ред.: О. А. Костенка ; Держ. наук. установа «Інститут інформації, безпеки і права НАПрН України». Київ; Одеса : Фенікс, 2026. С. 16-38. https://ippi.org.ua/sites/default/files/2100_monografiya_finish.pdf

130. Костенко С. О. Феномен права цифровізації та його вплив на юридичну освіту. *Аналітично-порівняльне правознавство*. 2025. № 2. С. 54–60. URL: <https://journal-app.uzhnu.edu.ua/article/view/326787>

131. Костенко О. Цифрова юрисдикція: модель. *Інформація і право*. 2025. № 4 (55). С. 24–45. URL: <https://il.ippi.org.ua/article/view/346297>

132. Костенко О. В., Маньгора В. В., Шапенко Л. О., Маньгора Т. В. Нові напрями інформаційного права та дефініції в епоху цифрових трансформацій і електронної юрисдикції. *Юридичний науковий електронний журнал*. 2024. № 10. С. 268–274. DOI: <https://doi.org/10.32782/2524-0374/2024-10/61>.

133. Костенко О. А., Шапенко Л. О. Сприйняття штучного інтелекту в Україні: соціально-правовий аналіз у вимірі інформаційного права та цифрової юрисдикції. *Інформація і право*. 2026. № 2 (57). URL: <https://il.ippi.org.ua/article/view/364302>

134. Крамаренко К. С., Тітко І. А. Напрями використання штучного інтелекту в кримінальних провадженнях (за матеріалами судової практики). *Аналітично-порівняльне правознавство*. 2026. № 1, ч. 3. С. 75–81. URL: <https://journal-app.uzhnu.edu.ua/article/view/353208>

135. Кримінальний кодекс України : Кодекс України від 05 квіт. 2001 р. № 2341-III. URL: <https://zakon.rada.gov.ua/go/2341-14>

136. Круц А. О. «Інтернет речей»: допомога чи загроза?! *Інтернет речей: проблеми правового регулювання та впровадження : матеріали II наук.-практ. конф.* (м. Київ, 29 листоп. 2018 р.). Київ : КПП ім. Ігоря Сікорського, 2018. С. 60–61.

137. Кудінов С. С. Правова політика з формування антитерористичної компетентності в Україні : монографія Одеса : Видавець Букаєв Вадим

Вікторович, 2019. 267 с.

138. Кулинич В. Правове регулювання використання штучного інтелекту в Україні та ЄС. *Asters*. 16 груд. 2025 р. URL: https://www.asterslaw.com/ua/press_center/publications/pravove_regulyuvannya_vikoristannya_shtuchnogo_intelektu_v_ukraini_ta_es/

139. Куракін О. М. Механізм правового регулювання: теоретико-правова модель : автореф. дис. ... д-ра юрид. наук : 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень». Харківський національний університет внутрішніх справ. Харків, 2016. 40 с. URL: <https://dspace.univd.edu.ua/items/1b753290-a0c2-46c4-bb03-8175bb67d4e0>

140. Куракін О. М. Особливості предмета правового регулювання. *Часопис Київського університету права*. 2015. № 3. С. 28–33. URL: <https://files.core.ac.uk/download/300240068.pdf>

141. Кутовий О. В., Бурма С. К. Автономні системи озброєнь і штучний інтелект як виклик міжнародному гуманітарному праву та правам людини. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Вип. 90, ч. 5. С. 185–194.

142. Ліманте А., Москвитин Ю. Технологія розпізнавання обличчя: ризики застосування у воєнний час. *Юридична газета*. 13 верес. 2024 р. URL: <https://yur-gazeta.com/dumka-eksperta/tehnologiya-rozpiznavannya-oblichchya-riziki-zastosuvannya-u-voenniy-chas.html>

143. Мазур М. Принцип правової визначеності та зміни судової практики. *Supreme Observer*. 02 лип. 2025 р. URL: <https://so.supreme.court.gov.ua/authors/607/pryntsyyp-pravovoi-vyznachenosti-ta-zminy-sudovoi-praktyky>

144. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : дис. ... канд. юрид. наук : 12.00.01 Київський національний університет внутрішніх справ. Київ, 2007. 188 с.

145. Марущак А. І. Вплив міжнародних процесів регулювання штучного інтелекту на інформаційне право України. *Інформація і право*. 2023. № 4 (47).

С. 55–63. URL: <https://il.ippi.org.ua/article/view/291582>

146. Махненко Д. І знову про штучний інтелект. Допомога, загроза чи пусті балачки? *Юридична газета*. 2021. № 11(741). URL: <https://yur-gazeta.com/publications/practice/inshe/i-znovu-pro-shtuchniy-intelekt-dopomoga-zagroza-chi-pusti-balachki.html>

147. Мей К. *Інформаційне суспільство: скептичний погляд* / пер. з англ. М. Войцицької. Київ : К.І.С., 2004. 220 с.

148. Меликов Р. Г. Автономні системи озброєння та принцип розрізнення в міжнародному гуманітарному праві. *Право і суспільство*. 2021. № 6. С. 315–320. DOI: <https://doi.org/10.32842/2078-3736/2021.6.46>

149. Меликов Р. Г. Застосування автономних систем озброєння під час російсько-української війни: нові виклики міжнародному гуманітарному праву. *Юридичний науковий електронний журнал*. 2023. № 1. С. 619–622. DOI: <https://doi.org/10.32782/2524-0374/2023-1/145>.

150. Міжнародний пакт про громадянські і політичні права : Міжнародний пакт ООН від 16 груд. 1966 р. URL: https://zakon.rada.gov.ua/go/995_043

151. Міжнародний пакт про економічні, соціальні і культурні права : Міжнародний пакт ООН від 16 груд. 1966 р. URL: https://zakon.rada.gov.ua/laws/show/995_042

152. Міністерство цифрової трансформації України. Біла книга з регулювання ШІ в Україні. 2024. 30 с. URL: <https://ai.thedigital.gov.ua/vision>

153. Міністерство цифрової трансформації України. Регулювання штучного інтелекту в Україні: Дорожня карта та bottom-up підхід. URL: <https://ai.thedigital.gov.ua/vision>

154. Міністерство цифрової трансформації України. Рік після прийняття постанови про Sandbox: перші результати. 14 листоп. 2025 р. URL: <https://ai.thedigital.gov.ua/news/One%20year%20after%20the%20adoption%20of%20the%20Sandbox%20resolution%3A%20first%20results>

155. Міністерство цифрової трансформації України. Україна посіла 5-те

місце за індексом онлайн-сервісів у глобальному рейтингу ООН: 20 вер. 2024.
URL: <https://digitalstate.gov.ua/news/govtech/ukraines-govtech-topping-global-rankings>

156. Міністерство цифрової трансформації України. Український GovTech у топі світових рейтингів. Digital State UA. 09 лют. 2025.
URL: <https://digitalstate.gov.ua/uk/news/govtech/ukrayinskyu-govtech-u-topi-svitovykh-reytnykh>

157. Моргунов О. А. Поняття та механізм адміністративно-правового регулювання публічного адміністрування сфер фізичної культури і спорту. *Юридичний науковий електронний журнал*. 2019. № 3. С. 274–277. URL: https://www.lsej.org.ua/3_2019/72.pdf

158. Москвич Л. М. Правовий статус носіїв судової влади в Україні (професійні судді, народні засідателі, суд присяжних) : монографія / Л. М. Москвич, С. О. Іваницький, І. О. Русанова ; за заг. ред. І. Є. Марочкина. Х. : ФІНН, 2009.

159. Мрак В. Методи розпізнавання обличчя у системах відеоспостереження з використанням машинного навчання. *Інфокомунікаційні технології та електронна інженерія*. 2023. Т. 3. № 2. С. 33–42. URL: <https://science.lpnu.ua/uk/itee/all-volumes-and-issues/volume-3-number-2-2023/metody-rozpiznavannya-oblychchya-u-systemah>

160. Муравська Ю., Сліпченко Т. Правове регулювання штучного інтелекту в Україні та світі . *Актуальні проблеми правознавства*. 2024. № 1(37). С. 188–195. DOI: <https://doi.org/10.35774/app2024.01.188>

161. Наскільки далеко може зайти AI та чому його бояться технологіери: 8 ризиків штучного інтелекту, які вже змінюють наше майбутнє. Laba.ua. 3 лип. 2023 р. URL: <https://laba.ua/blog/3625-naskilky-daleko-mozhe-zayty-shtuchnyy-intelekt>

162. Нашинець-Наумова А. Ю. Адміністративно-правові основи застосування штучного інтелекту в публічному управлінні в умовах післявоєнного відновлення України. *Вчені записки Таврійського національного*

університету імені В. І. Вернадського. Серія: Юридичні науки. 2026. Т. 37 (76), № 1. С. 138–144. URL: <https://elibrary.kubg.edu.ua/id/eprint/57463/>

163. Некіт К. Г. Деякі правові проблеми Інтернету речей і напрями їх вирішення. *Часопис цивілістики*. 2018. Вип. 31. С. 54–58.

164. Некіт К. Г. Інтернет речей та інформаційна безпека: деякі правові проблеми. *Інтернет речей: проблеми правового регулювання та впровадження : матеріали наук.-практ. конф.* (м. Київ, 24 жовт. 2017 р.). Київ : КПП ім. Ігоря Сікорського, 2017. С. 61–65.

165. Некрасов В., Катамадзе Г. Ризик-орієнтований підхід (РОП) в діяльності органів правопорядку. *Реалізація філософії «Intelligence-Led Policing» в системі кримінального аналізу Національної поліції України*. 2024. С. 311–341.

166. Нечаєва І. А., Панкова А. Ю. Ризик-орієнтований підхід до управління змінами. *Управління змінами та інновації*. 2023. № 8. С. 23–27. DOI: <https://doi.org/10.32782/CMI/2023-8-4>

167. Оніщенко Н. М., Сунегін С. О. Проблеми протидії правопорушенням в інформаційній сфері: реалії та перспективи. *Віче*. 2012. № 11. С. 33–36. URL: http://nbuv.gov.ua/UJRN/viche_2012_11_13

168. Осадчий В. І. Механізм правового регулювання. *Митна справа*. 2013. № 5, ч. 2, кн. 2. С. 336–340.

169. Основи законодавства України про охорону здоров'я : Закон України від 19 листоп. 1992 р. № 2801-XII. URL: <https://zakon.rada.gov.ua/go/2801-12>

170. Павлюк О. В. Цивільно-правова охорона об'єктів права інтелектуальної власності, створених із використанням технологій штучного інтелекту : дис. ... д-ра філософії : 081 Право. Львівський державний університет внутрішніх справ. Львів, 2024. 223 с. URL: <https://dspace.lvduvs.edu.ua/handle/1234567890/7488>

171. Патерило І. В. Право як ціннісна категорія : автореф. дис. ... канд. юрид. наук : 12.00.01. Київ, 2006. 20 с.

172. Перспективи та межі використання штучного інтелекту в кримінальному процесі. Центр Дністрянського ; Міжнародний фонд «Відродження». 2024. URL: <https://www.irf.ua/wp-content/uploads/2024/02/ai.pdf>

173. Петришин О. В., Гиляка О. С. Права людини в цифрову епоху: виклики, загрози та перспективи. *Вісник Національної академії правових наук України*. 2021. Т. 28, № 1. С. 17–35. URL: <https://visnyk.kh.ua/uk/journals/visnik-napnru-1-2021r/prava-lyudini-v-tsifrovu-epokhu-viklyki-zagrozi-ta-perspektivi>

174. Петрів О. Захист персональних даних у добу штучного інтелекту: міжнародні підходи та виклики. *CEDEM (Центр демократії та верховенства права)*. URL: <https://cedem.org.ua/consultations/zahyst-personalnyh-danyh-u-dobu-shtuchnogo-intelektu-mizhnarodni-pidhody-ta-vyklyky/>

175. Пилипчук В. Г., Баранов О. А., Гиляка О. С. Правове забезпечення сфери штучного інтелекту: сучасний стан та перспективи розвитку. *Інформація і право*. 2021. № 1 (36). С. 5–14. URL: <https://il.ippi.org.ua/article/view/238389>

176. Пилипчук В. Г., Баранов О. А., Гиляка О. С. Проблема правового регулювання у сфері штучного інтелекту в контексті розвитку законодавства Європейського Союзу. *Вісник Національної академії правових наук України*. 2022. Т. 29, № 2. С. 35–62. URL: <https://visnyk.kh.ua/uk/journals/visnik-napnru-2-2022-r/problema-pravovogo-regulyuvannya-u-sferi-shtuchnogo-intelektu-v-konteksti-rozvitku-zakonodavstva-yevropeyskogo-soyuzu>

177. Пилипчук В. Г., Дзьобань О. П. *Інформаційне суспільство: філософсько-правовий вимір : монографія*. Ужгород : ТОВ «ІВА», 2014. 282 с. URL: <https://ippi.org.ua/informatsiine-suspilstvo-filosofsko-pravovii-vimir>

178. Підгородинський В. М. Штучний інтелект та кримінальне право: сучасні грані досліджень. *Кримінально-виконавча система: Вчора. Сьогодні. Завтра*. № 2 (16), 2024. С. 84–94. URL: <https://sjcriminal.pau.edu.ua/wp-content/uploads/2024/12/7.-Підгородинський-В.-М.pdf>

179. Позова Д. Д. Система джерел правового регулювання інформаційно-технологічних відносин. *Часопис цивілістики*. 2017. Вип. 24. С. 93–96. URL: <https://dspace.onua.edu.ua/items/27baaa6b-d726-48fd-840d->

71985e07bc47

180. Попович Т. П. Правосуб'єктність штучного інтелекту: майбутнє чи ілюзія? *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Т. 1, № 89. С. 144–149. URL: <https://visnyk-pravo.uzhnu.edu.ua/article/view/335495> с. 149

181. Постанова Верховного Суду від 08 лип. 2025 р. у справі № 925/496/24. URL: <https://iplex.com.ua/doc.php?regnum=128775966>

182. Права людини в епоху штучного інтелекту: виклики та правове регулювання : методичний матеріал / У. Шадська та ін. Київ : EU4DigitalUA, Офіс Омбудсмана України, Міністерство цифрової трансформації України, 2024. 44 с.

183. Приступенко Т., Євдокименко І. Правове регулювання використання штучного інтелекту в медіа: український та світовий досвід. *Наукові записки Інституту журналістики*. 2025. Т. 86, № 1. С. 9–20. DOI: <https://doi.org/10.17721/2522-1272.2025.86.1>

184. Проєкт Закону про внесення змін до статті 190 Кримінального кодексу України щодо криміналізації протиправних (шахрайських) діянь, вчинених із використанням інформаційно-комунікаційних систем або систем штучного інтелекту : проєкт Закону України від 03 лип. 2026 р. № 15379. URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/70271>

185. Про адміністративні послуги : Закон України від 06 верес. 2012 р. № 5203-VI. URL: <https://zakon.rada.gov.ua/go/5203-17>

186. Про адміністративну процедуру : Закон України від 17 лют. 2022 р. № 2073-IX. URL: <https://zakon.rada.gov.ua/go/2073-20>

187. Про академічну доброчесність : Закон України від 18 груд. 2025 р. № 4742-IX. URL: <https://zakon.rada.gov.ua/go/4742-20>

188. Про акредитацію органів з оцінки відповідності : Закон України від 17 трав. 2001 р. № 2407-III. URL: <https://zakon.rada.gov.ua/go/2407-14>

189. Про визнання такими, що втратили чинність, деяких актів Кабінету Міністрів України : постанова Кабінету Міністрів України від 14 січ. 2026 р. №

24. URL: <https://zakon.rada.gov.ua/go/24-2026-%D0%BF>

190. Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI. URL: <https://zakon.rada.gov.ua/go/2939-17>

191. Про електронні комунікації : Закон України від 16 груд. 2020 р. № 1089-IX. URL: <https://zakon.rada.gov.ua/go/1089-20>

192. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05 жовт. 2017 р. № 2155-VIII. URL: <https://zakon.rada.gov.ua/go/2155-19>

193. Про запровадження Національної системи індикаторів розвитку інформаційного суспільства : Постанова Кабінету Міністрів України від 28.11.2012 № 1134. *Офіційний вісник України*. 2012. № 91. Ст. 3681.

194. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021–2024 роки : розпорядження Кабінету Міністрів України від 12 трав. 2021 р. № 438-р. URL: <https://zakon.rada.gov.ua/go/438-2021-%D1%80>

195. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки : розпорядження Кабінету Міністрів України від 9 трав. 2025 р. № 457-р. URL: https://zakon.rada.gov.ua/laws/main/457-2025-p?utm_source=chatgpt.com#Text

196. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05 лип. 1994 р. № 80/94-ВР. URL: <https://zakon.rada.gov.ua/go/80/94-%D0%B2%D1%80>

197. Про захист персональних даних : Закон України від 01 черв. 2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/go/2297-17>

198. Про захист персональних даних : проєкт Закону України від 25 жовт. 2022 р. № 8153. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/40707>

199. Про інформацію : Закон України від 02.10. 92. № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12/ed19921002#Text>

200. Про інформацію : Закон України. Закон України від 02.10. 92. № 2657-XII. Редакція від 20.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/2657->

12#Text

201. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки : Указ Президента України від 11 трав. 2023 р. № 273/2023. URL: <https://zakon.rada.gov.ua/go/273/2023>

202. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII. URL: <https://zakon.rada.gov.ua/go/2469-19>

203. Про освіту : Закон України від 05.09.2017 № 2145-VIII. URL: <https://zakon.rada.gov.ua/go/2145-19>

204. Про основні засади державного нагляду (контролю) у сфері господарської діяльності : Закон України від 05 квіт. 2007 р. № 877-V. URL: <https://zakon.rada.gov.ua/go/877-16>

205. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

206. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 № 537-V. *Відомості Верховної Ради України*. 2007. № 12. Ст. 102.

207. Про правотворчу діяльність : Закон України від 24 серп. 2023 р. № 3354-IX. URL: <https://zakon.rada.gov.ua/go/3354-20>

208. Про публічні електронні реєстри : Закон України від 18 листоп. 2021 р. № 1907-IX. URL: <https://zakon.rada.gov.ua/go/1907-20>

209. Про публічні закупівлі : Закон України від 25 груд. 2015 р. № 922-VIII. URL: <https://zakon.rada.gov.ua/go/922-19>

210. Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні : Постанова Верховної Ради України від 01.12.2005 № 3175-IV. URL: <https://zakon.rada.gov.ua/laws/show/3175-15#Text>

211. Про Рекомендації парламентських слухань на тему: «Стратегія інноваційного розвитку України на 2010–2020 роки в умовах глобалізаційних викликів» : Постанова Верховної Ради України від 21.10.2010 № 2632-VI. URL:

<https://zakon.rada.gov.ua/laws/show/2632-17#Text>

212. Про стандартизацію : Закон України від 05 черв. 2014 р. № 1315-VII. URL: <https://zakon.rada.gov.ua/go/1315-18>

213. Про схвалення Концепції Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року : розпорядження Кабінету Міністрів України від 13 квіт. 2024 р. № 320-р. URL: <https://zakon.rada.gov.ua/go/320-2024-%D1%80>

214. Про схвалення Концепції розвитку електронної охорони здоров'я : розпорядження Кабінету Міністрів України від 28 груд. 2020 р. № 1671-р. URL: <https://zakon.rada.gov.ua/go/1671-2020-%D1%80>

215. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 2 груд. 2020 р. № 1556-р. URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-p>

216. Про схвалення Стратегії розвитку штучного інтелекту в Україні на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2026-2028 роках : проєкт розпорядження Кабінету Міністрів України. URL: <https://storage.thedigital.gov.ua/files/7/77/de9bc60806aa166e5394d0a64128b77a.pdf>

217. Про технічні регламенти та оцінку відповідності : Закон України від 15 січ. 2015 р. № 124-VIII. URL: <https://zakon.rada.gov.ua/go/124-19>

218. Про Уповноваженого Верховної Ради України з прав людини : Закон України від 23 груд. 1997 р. № 776/97-ВР. URL: <https://zakon.rada.gov.ua/go/776/97-%D0%B2%D1%80>

219. Про центральні органи виконавчої влади : Закон України від 17 берез. 2011 р. № 3166-VI. URL: <https://zakon.rada.gov.ua/go/3166-17>

220. Пядишев В. Г. Перспективи розвитку проактивної діяльності поліції: зарубіжний погляд. *Право і суспільство*. 2024. № 1, т. 2. С. 403–412. URL: https://pravoisuspilstvo.org.ua/archive/2024/1_2024/part_2/63.pdf

221. Пядишев В. Г., Балтовський О. А. Сучасні проблеми цифрової криміналістики – зарубіжний погляд. *Держава та регіони. Серія: Право*. 2025.

№ 3 (88). С. 166–172. DOI: <https://doi.org/10.32782/1813-338X-2025.3.22>

222. Пядишев В. Г., Лісніченко Д. В. Організаційно-правові умови відповідального використання штучного інтелекту у правоохоронній діяльності для забезпечення громадської безпеки. *Південноукраїнський правничий часопис*. 2026. № 1. С. 83–88.

223. Рабінович П. М. Основи загальної теорії права та держави. Вид.- 6-е. Харків : Консум, 2002. 160 с.

224. Рабінович П. М. Сутність праворозуміння. *Право України*. 2007. № 9. С. 3–7.

225. Радзієвська О. Г. Окремі питання правового забезпечення інформаційної безпеки в умовах інноваційного розвитку суспільства. *Дослідження інновацій та перспективи розвитку науки і техніки у XXI столітті* : матеріали Міжнар. наук.-практ. конф. (м. Рівне, 25–26 листоп. 2021 р.). Ч. 1. Рівне : Видавничий дім «Гельветика», 2021. С. 167–170.

226. Радзивілл О. Правове регулювання штучного інтелекту в Європейському Союзі: етичні та нормативні виклики. *Інформація і право*. 2022. № 3(42). С. 15–24. URL: <https://il.ippi.org.ua/article/view/300706>

227. Радутний О. Е. Штучний інтелект, інформаційна безпека та законотворчий процес (кримінально-правовий аспект). *Інформація і право*. 2018. № 1 (24). С. 149–158. URL: <https://il.ippi.org.ua/article/view/273218>

228. Рекомендація CM/Rec(2020)1 Комітету Міністрів Ради Європи державам-членам щодо впливу алгоритмічних систем на права людини. Ухвалена Комітетом Міністрів 8 квітня 2020 року на 1373-му засіданні Заступників Міністрів. URL: https://court.gov.ua/storage/portal/supreme/rizne/CM_Rec_2020_1_08_04_2020.pdf

229. Розенфельд Н. А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : автореф. дис. ... канд. юрид. наук : 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче

право». Київ : Інститут держави і права ім. В. М. Корецького НАН України, 2003. 17 с.

230. Савінова Н. А. Кримінально-правова політика забезпечення інформаційного суспільства в Україні : монографія. Київ : ТОВ «ДКС Центр», 2013. 492 с.

231. Сафаров А. Скандал з витоком даних у Facebook: як це сталося. *Deutsche Welle*. 14 квіт. 2018 р. URL: <https://www.dw.com/uk/скандал-з-витоком-даних-у-facebook-як-це-сталося/a-43385507>

232. Система розпізнавання обличчя: правові аспекти використання в Україні та в ЄС. Українська Гельсінська спілка з прав людини. URL: <https://www.helsinki.org.ua/articles/systema-rozpiznavannia-oblychchia-pravovi-aspekty-vykorystannia-v-ukraini-ta-v-yes/>

233. Скакун О. Ф. Теорія держави і права : підручник Харків : Консум, 2008. 656 с.

234. Скільки українців користуються ІІІ та чи готові платити за нього. *Факти ICTV*. 08 квіт. 2026. URL: <https://fakty.com.ua/ua/styl-zhyttia/nauka-tekhnologii/20260408-skilky-ukrayincziv-korystuyutsya-shi-ta-chy-gotovi-platyty-za-nogo/>

235. Слободянюк А. В., Андрущенко Н. О. Процес ухвалення рішення. *Психологія управління та конфліктологія : навч. посіб.* Вінниця : ВНТУ, 2010. С. 45–48.

236. Словник української мови : в 11 т. Т. 4. Київ : Наукова думка, 1973. 840 с.

237. Слюсаренко К. Р. Інформаційне право в епоху штучного інтелекту: виклики та перспективи розвитку сучасної юриспруденції. *Держава та регіони. Серія: Право*. 2023. № 4. С. 211–216. URL: https://law.stateandregions.zp.ua/archive/4_2023/35.pdf

238. Соколік В. Д., Пащенко Д. В., Швець С. А., Башанова Н. Є. Правове регулювання використання штучного інтелекту в публічному управлінні: виклики цифрової епохи. *Науковий вісник Одеського національного*

економічного університету. 2025. № 4(329). С. 30–36.
DOI: <https://doi.org/10.32680/2409-9260-2025-4-329-30-36>.

239. Соснова Д. Розумний Інтернет речей – технологія майбутнього. *Світ телекомунікації та інформатизації* : зб. матеріалів міжнар. наук.-техн. конф. (м. Київ, 7 груд. 2017 р.). Київ, 2017. С. 17–20.

240. Співак О. М. Правові засади регулювання штучного інтелекту в Україні та Польщі. *Юридичний науковий електронний журнал*. 2024. № 4. С. 815–817. DOI: <https://doi.org/10.32782/2524-0374/2024-4/198>

241. Статут Організації Об'єднаних Націй : міжнародний документ від 26 черв. 1945 р. URL: https://zakon.rada.gov.ua/go/995_010

242. Стратегія розвитку штучного інтелекту в Україні : монографія / А. І. Шевченко, С. В. Барановський, О. В. Білокобильський та ін. ; за заг. ред. А. І. Шевченка. Київ : Інститут проблем штучного інтелекту МОН України і НАН України, 2023. 305 с. URL: https://jai.in.ua/archive/2023/ai_mono.pdf

243. Стратегія розвитку штучного інтелекту в Україні на період до 2030 року : проєкт. Міністерство цифрової трансформації України, 2026. URL: <https://ai-files.thedigital.gov.ua/documents/Проект%20Стратегії%20розвитку%20ШІ%202030.docx.pdf>

244. Стукаленко О. В. Нотатки до розуміння категорії «механізм правового регулювання». *Правова держава*. 2017. № 26. С. 23–27. URL: <https://dspace.onu.edu.ua/server/api/core/bitstreams/07b29149-6e17-4ac3-809a-35984930b395/content>

245. Теличко О. А., Рекун В. А., Чабаненко Ю. С. Проблеми визначення та нормативного закріплення поняття «штучний інтелект» у законодавстві зарубіжних країн та України. *Юридичний науковий електронний журнал* 2021. № 2. С. 310–314.

246. Теорія держави і права. Академічний курс : підручник / [О. В. Зайчук, А. П. Заєць, В. С. Журавський та ін.] ; за ред. О. В. Зайчука, Н. М. Оніщенко. 2-ге вид., перероб. і допов. Київ : Юрінком Інтер, 2008. 688 с.

247. Тетерятник Г. К. Кримінальне провадження в умовах надзвичайних правових режимів: теоретико-методологічні та праксеологічні основи : монографія. Одеса : Гельветика, 2021. 499 с.

248. Тимошенко Є. А. Правове забезпечення застосування штучного інтелекту в Україні : дис. ... д-ра філософії : 081 Право. Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України». Київ, 2024. 204 с. URL: https://ippi.org.ua/sites/default/files/disertaciya_timoshenko_ie_a.pdf

249. Ткаченко Н. О. Аналіз визначення поняття «соціальна відповідальність» та його інтегроване розуміння у фармації. *Запорожский медицинский журнал*. 2013. № 3 (78). С. 125–128. URL: <https://zmj.zsmu.edu.ua/article/download/14090/11916/19042>

250. Товкун Л. В., Леонович М. Ю. Правове регулювання штучного інтелекту: міжнародний досвід та перспективи впровадження для України. *Юридичний науковий електронний журнал*. 2024. № 12. С. 278–282. DOI: <https://doi.org/10.32782/2524-0374/2024-12/62>.

251. Турецька О. В., Яворська Т. М. Стан нормативно-правового регулювання штучного інтелекту в Україні та світі. *Вісник студентського наукового товариства Донецького національного університету імені Василя Стуса*. 2025. Т. 2, № 17. С. 215–219. URL: <https://jvestnik-sss.donnu.edu.ua/article/view/17334>

252. Тюрю Ю. І. Адміністративно-правовий механізм реалізації правової доктрини у сфері штучного інтелекту в Україні : дис. ... д-ра юрид. наук : 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Дніпропетровський державний університет внутрішніх справ. Дніпро, 2023. 381 с

253. Тюрю Ю. Визначення поняття адміністративно-правового регулювання діяльності зі створення, впровадження та використання штучного інтелекту в Україні. *Juris Europensis Scientia*. 2022. № 3. С. 73–77. URL: https://jes.nuoua.od.ua/archive/3_2022/14.pdf

254. Угода між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» (2021–2027) : міжнародний договір від 05 верес. 2022 р.
URL: https://zakon.rada.gov.ua/go/984_005-22

255. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : міжнародний договір від 27 черв. 2014 р. URL: https://zakon.rada.gov.ua/go/984_011

256. Україна піднялася на 14 позицій у світовому рейтингу зі штучного інтелекту: допомогла цифровізація держпослуг. *Forbes Ukraine*. 23 груд. 2025.
URL: <https://forbes.ua/news/ukraine-pidnyalasya-na-14-pozitsiy-u-svitovomu-reytingu-zi-shtuchnogo-intelektu-posivshi-40-te-mistse-23122025-35066>

257. Ухвала Київського апеляційного суду від 30 лип. 2025 р. у справі № 11-кп/824/1818/2025. Єдиний державний реєстр судових рішень.
URL: <https://reyestr.court.gov.ua/Review/129699665>

258. Ухвала Касаційного господарського суду у складі Верховного Суду від 08 лют. 2024 р. у справі № 925/200/22. Єдиний державний реєстр судових рішень. URL: <https://reyestr.court.gov.ua/Review/116984639>

259. Федчак І. А. Системи штучного інтелекту в кримінології: загрози і можливості. *Український політико-правовий дискурс*. 2025. Вип. 10. С. 120–127.
URL: <https://polit-discourse.com/index.php/main/article/view/210>

260. Фівкін П. М., Іващенко С. М. Правове регулювання використання штучного інтелекту у системі управління Збройних Сил України. *Актуальні проблеми політики*. 2026. Вип. 77. С. 48–54.
DOI: <https://doi.org/10.32782/app.v77.2026>

261. Фріс П. Л. Кримінально-правова політика Української держави: теоретичні, історичні та правові проблеми: монографія. Київ : Атіка, 2005. 332 с.

262. Фурашев В. М. Інформація, інформаційне право, цифрові технології: зв'язок та вплив на соціальну трансформацію. *Соціальна і цифрова*

трансформація: теоретичні та практичні проблеми правового регулювання : матеріали Всеукр. наук.-практ. конф. (м. Київ, 2 груд. 2021 р.) / наук. кер. О. А. Баранов ; упоряд. В. М. Фурашев, С. О. Дорогих. Київ : Фенікс, 2021. С. 11–24. URL:

https://ippi.org.ua/sites/default/files/socialna_i_cifrova_transformaciya_2021.pdf

263. Фурашев В. М., Ланде Д. В., Григор'єв О. М., Фурашев О. В. *Електронне інформаційне суспільство України: погляд у сьогодення і майбутнє* : монографія. Київ : ТОВ «Інжиніринг», 2005. 164 с.

264. Ханкевич А. М., Соломко Д. К. Трирівнева модель аналітичної діяльності Служби безпеки України: ризик-орієнтований підхід до організації. *Юридичний науковий електронний журнал*. 2025. № 8. С. 181–192.

265. Харитонова О. І. Багатоаспектність розуміння «штучного інтелекту». *ІТ-право та кібербезпека в умовах гібридної війни* : матеріали Всеукр. круглого столу (м. Одеса, 12 квіт. 2025 р.) / за заг. ред. Є. О. Харитонової, Ю. Кривенка. Одеса : Фенікс, 2025. С. 35–40. URL: <https://dspace.onua.edu.ua/server/api/core/bitstreams/40ee87eb-0065-409b-ba79-d8079c94ef33/content#page=35>

266. Харитонова О. І., Харитонов Є. О. Цифрова людина, цифрова особа та цифрова особистість: до проблеми співвідношення. *Часопис цивілістики*. 2023. Вип. 49. С. 5–13. URL: <https://clj.nuoua.od.ua/archive/49/1.pdf>

267. Харитонова О. І. Харитонов Є.О., Галупова Л.І. Поняття і зміст права на цифровий образ. *Штучний інтелект, сучасні технології та право в Україні* : монографія / за заг. ред.: О. А. Костенка; Держ. наук. установа «Інститут інформації, безпеки і права НАПрН України». Київ; Одеса : Фенікс, 2026. С. 6-16. URL:

https://ippi.org.ua/sites/default/files/2100_monografiya_finish.pdf

268. Ходжалієва С. «Галюцинації» штучного інтелекту та їх вплив на розгляд судових справ. *Вища школа адвокатури НААУ*. 08 верес. 2025 р. URL: <https://www.hsa.org.ua/lectors/xodzalijeva-salatin/articles/galiucinaciyi-stucnogo-intelektu-ta-yix-vpliv-na-rozgliad-sudovix-sprav>

269. Цивільний кодекс України : Кодекс України від 16 січ. 2003 р. № 435-IV. URL: <https://zakon.rada.gov.ua/go/435-15>

270. Шепітько М. В. Перспективи використання штучного інтелекту органами кримінальної юстиції в ЄС та Україні. *Матеріали IX (XXII) Львівського форуму кримінальної юстиції, 26–27 жовт. 2023 р.* Львів : ЛьвДУВС, 2023. С. 264–269. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/6592/1/26-27_10_2023.pdf

271. Шинкар Т. І. Адміністративно-правові засади регулювання обмеження права на інформацію в інтересах національної безпеки : дис. ... д-ра юрид. наук : 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Львів : Львівський державний університет внутрішніх справ, 2023. 510 с. URL: <https://dspace.lvduvs.edu.ua/handle/1234567890/6933>

272. Штучний інтелект у правосудді – допомога чи загроза судовому розсуду: думки суддів Верховного Суду. Верховний Суд. 11 берез. 2026 р. URL: <https://supreme.court.gov.ua/supreme/pres-centr/news/1987559/>

273. Щербина Б. С., Ткаченко В. В. Штучний інтелект як суб'єкт цивільного права. *Юридичний вісник. Повітряне і космічне право.* 2021. № 1 (58). С. 142–148. URL: <https://jrnl.kai.edu.ua/index.php/UV/article/download/15321/22197>

274. Щодо проєкту стратегії розвитку штучного інтелекту в Україні на 2022–2030 рр. / авторський колектив Інституту проблем штучного інтелекту МОН України і НАН України. *Artificial Intelligence.* 2022. Т. 27, № 1. С. 75–157. URL: https://www.slyusar.kiev.ua/AI_2022-1-1_ua.pdf

275. Явір В. А., Маркішев Д. О. Академічна доброчесність: спроби законодавчого врегулювання в контексті євроінтеграції України. *Альманах права.* 2024. Вип. 15. С. 189–194. URL: <https://almanahprava.org/assets/images/issues/15/almanac-15-ua.pdf>

276. Янишівський М. М. Формування публічної політики у сфері штучного інтелекту: міжнародний досвід для України : дис. ... д-ра філософії : 281 «Публічне управління та адміністрування». Національний університет

«Львівська політехніка». Львів, 2025. 301 с. URL: <https://ena.lpnu.ua/handle/ntb/111682>

277. Ярмакі Х. П. Адміністративно-наглядова діяльність міліції в Україні : дис. ... д-ра юрид. наук : 12.00.07. Харківський національний університет внутрішніх справ. Харків, 2006. 438 с.

278. Ярмакі Х. П. Механізм адміністративно-правового регулювання. *Південноукраїнський правничий часопис*. 2013. № 2. С. 81–87. URL: http://nbuv.gov.ua/UJRN/Pupch_2013_2_17

279. Achtes Gesetz zur Änderung des Straßenverkehrsgesetzes vom 16. Juni 2017. *Bundesgesetzblatt*. Teil I. 2017. Nr. 38. S. 1648–1650. URL: https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s1648.pdf%27%5D

280. Adoption of a European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment at the 31st Plenary Meeting of the CEPEJ in Strasbourg on 3 and 4 December 2018. European Commission for the Efficiency of Justice (CEPEJ). 4 Dec. 2018. URL: <https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment>

281. Ahmed Z. This AI Claims to Predict Crimes before They Happen Based on Real-Time CCTV Analysis. *TechSpot*. 15 Sept. 2024. URL: <https://www.techspot.com/news/104723-ai-claims-predict-crimes-before-they-happen-based.htm>

282. AI and Privacy: Balancing Technology and Compliance in Law Enforcement. Veritone Blog. 12 Mar. 2025. URL: <https://www.veritone.com/blog/ai-and-privacy-balancing-technology-and-compliance-in-law-enforcement/>

283. AI Surveillance Privacy: Balancing Security and Privacy Rights. Volt AI Blog. 14 July 2025. URL: <https://volt.ai/blog/ai-surveillance-privacy-balancing-security-and-privacy-rights>

284. AI in Teaching and Learning. ETH Zurich. URL: <https://ethz.ch/en/the-eth-zurich/education/ai-in-education.html>.

285. Akata Z., Balliet D., de Rijke M., et al. A Research Agenda for Hybrid Intelligence: Augmenting Human Intellect with Collaborative, Adaptive, Responsible, and Explainable Artificial Intelligence. *Computer*. 2020. Vol. 53, No. 8. P. 18–28. URL: <https://doi.org/10.1109/MC.2020.2996587>

286. Amnesty International. Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance. *Research*. 11 June 2020. URL: <https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/>

287. Anagnostou M. The Potential Implementation of Predictive Algorithms as Tools Assisting Judges of the European Court of Human Rights in the Decision-Making Process and the Impact on the Right to a Fair Hearing. Master's thesis. Tilburg University. LL.M. Law & Technology. Tilburg, 2023. URL: <http://arno.uvt.nl/show.cgi?fid=161833>

288. Angwin J., Larson J., Mattu S., Kirchner L. Machine Bias: There's Software Used across the Country to Predict Future Criminals. And It's Biased against Blacks. *ProPublica*. 23 May 2016. URL: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

289. A Roadmap for U.S. Robotics: From Internet to Robotics. 2016 Edition. University of California San Diego; Carnegie Mellon University; Computing Community Consortium, 2016. URL: <https://cra.org/cra/wp-content/uploads/sites/2/2016/11/roadmap3-final-rs-1.pdf>

290. Artificial Intelligence Market Trends 2025: Generative AI, AI Chips, and Cloud AI Platforms Fuel Industry Expansion. MarketsandMarkets Blog. 2026. 19 May. URL: <https://www.marketsandmarketsblog.com/artificial-intelligence-market-trends-2025-generative-ai-ai-chips-and-cloud-ai-platforms-fuel-industry-expansion.html>

291. Artificial Intelligence Standardization White Paper. China Electronics Standardization Institute (CESI), 2018. 116 p. URL: <https://www.cesi.cn/images/editor/20180124/20180124135528742.pdf>.

292. Artificial intelligence: The promises and the threats. *The UNESCO Courier*. 2018. July–September. No. 3. P. 3. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000265211>
293. Artigot i Golobardes M., Grasso G., Iamiceli P., Maugeri M. R., eds. Artificial Intelligence, Judicial Decision-Making and Fundamental Rights: JuLIA Handbook. 2nd ed. Scuola Superiore della Magistratura, 2024. 219 p. URL: https://ssm-italia.eu/wp-content/uploads/2025/02/JuLIA_handbook-Justice_final.pdf
294. Asimov I. I, Robot. New York : Gnome Press, 1950.
295. Asimov I. Robots and Empire. New York : Doubleday, 1985. 363 p.
296. Asimov I. The Complete Robot. New York : Doubleday, 1982.
297. Assembly Bill No. 331. Automated Decision Tools. 2023–2024 Regular Session. *California Legislative Information*. URL: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB331
298. Barbaro C. The European Ethical Charter of the CEPEJ. EEEI – Experts Institute. 29 May 2019. URL: <https://experts-institute.eu/en/europe-of-justice/cepej-en/the-european-ethical-charter-of-the-cepej/>
299. Barrat J. Our Final Invention: Artificial Intelligence and the End of the Human Era. New York : Thomas Dunne Books, 2013. 336 p.
300. Bell D. The Coming of Post-Industrial Society: A Venture in Social Forecasting. New York : Basic Books, 1973. 507 p.
- ^{301.} Benasayag M. Humans, Not Machines, Create Meaning: Interview by Régis Meyran. *The UNESCO Courier*. 2018. July–September. P. 15–17. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000265211>.
302. Bengio Y., et al. International AI Safety Report 2025. UK Government, 2025. URL: <https://www.gov.uk/government/publications/international-ai-safety-report-2025>
303. Bengio Y. Call for Red Lines to Prevent Unacceptable AI Risks. AI Red Lines. URL: <https://www.airedlines.org/>

304. Bergengruen V. Ukraine's «Secret Weapon» Against Russia Is a Controversial U.S. Tech Company. *TIME*. 14 Nov. 2023. URL: <https://time.com/6334176/ukraine-clearview-ai-russia/>

305. Big Brother Watch and Others v. the United Kingdom. Nos. 58170/13, 62322/14 and 24960/15. Judgment of 25 May 2021. *European Court of Human Rights*. HUDOC. URL: <https://hudoc.echr.coe.int>

306. Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People. The White House, Office of Science and Technology Policy. Washington, DC, 2022. URL: <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>

307. Bosch. Code of Ethics for Artificial Intelligence. Robert Bosch. GmbH, 2020. URL: https://assets.bosch.com/media/en/global/stories/ai_codex/bosch-code-of-ethics-for-ai.pdf

308. Bostrom N. Superintelligence: Paths, Dangers, Strategies. Oxford : Oxford University Press, 2014. 352 p.

309. Brown E. 21 Open Source Projects for IoT. *Linux.com*. 2016. URL: <https://www.linux.com/news/21-open-source-projects-iot/>

310. Brynjolfsson E., McAfee A. The Business of Artificial Intelligence. *Harvard Business Review*. 18 July 2017. URL: <https://hbr.org/2017/07/the-business-of-artificial-intelligence>

311. Bühler K. The Mental Development of the Child. New York : Harcourt, Brace, 1930. 304 p.

312. Cambridge Dictionary. Cambridge University Press. URL: <https://dictionary.cambridge.org/>

313. Cameron L. Internet of Things Meets the Military and Battlefield: Connecting Gear and Biometric Wearables for an IoMT and IoBT. *IEEE Computer Society*. URL: <https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt>

314. Carrillo M. R. *Artificial Intelligence: From Ethics to Law. Telecommunications Policy*. 2020. Vol. 44, No. 6. Article 101937. DOI: <https://doi.org/10.1016/j.telpol.2020.101937>

315. Case of Big Brother Watch and Others v. the United Kingdom, Nos. 58170/13, 62322/14 and 24960/15, Judgment of 25 May 2021. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=001-210077>

316. Case of Glukhin v. Russia, No. 11519/20, Judgment of 4 July 2023. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=002-14142>

317. Case of Ruiz Torija v. Spain, No. 18390/91, Judgment of 9 Dec. 1994. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=001-57909>

318. Case of S. and Marper v. the United Kingdom, Nos. 30562/04 and 30566/04, Judgment of 4 Dec. 2008. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=001-90051>

319. Chapman J. AI Anxiety: Career concerns of the creative industries. *Empower Agency*. URL: <https://empower.agency/ai-anxiety/>

320. Charter of Fundamental Rights of the European Union. *Official Journal of the European Union*. 2012. C 326. P. 391–407. URL: https://eur-lex.europa.eu/eli/treaty/char_2012/oj/eng

321. Cheruvu R. Human-in/on-the-Loop Design for Human Controllability. *Handbook of Human-Centred Artificial Intelligence*. Singapore : Springer, 2026. DOI: https://doi.org/10.1007/978-981-97-8440-0_75-1

322. Christensen H. I., Okamura A., Mataric M., Kumar V., Hager G., Choset H. *Next Generation Robotics*. 2016. arXiv:1606.09205. URL: <https://arxiv.org/abs/1606.09205>

323. Cisco Internet Business Solutions Group. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. San Jose, CA, 2011. URL: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

324. Clayton J., Derico B. Clearview AI Used Nearly 1m Times by US Police, It Tells the BBC. *BBC News*. 27 Mar. 2023. URL: <https://www.bbc.com/news/technology-65057011>

325. Clifford C. Bill Gates: A.I. is like nuclear energy – «both promising and dangerous». *CNBC*. 26 Mar. 2019. URL: <https://www.cnn.com/2019/03/26/bill-gates-artificial-intelligence-both-promising-and-dangerous.html>

326. Coco A. Exploring the Impact of Automation Bias and Complacency on Individual Criminal Responsibility for War Crimes. *Journal of International Criminal Justice*. 2023. Vol. 21, No. 5. P. 1077–1096. URL: <https://academic.oup.com/jicj/article/21/5/1077/7281035>

327. Cohen-Lazry G., Oron-Gilad T. Is Staying out of Bomb-Shelters a Human-Automation Interaction Issue? *Technology in Society*. 2016. Vol. 47. P. 25–30. URL: <https://www.sciencedirect.com/science/article/pii/S0160791X16300814>

328. Colombo G. Algorithmic Bias and Social Justice: When AI Reflects Our Inequities. *N5 Blog*. 2 July 2025. URL: <https://blog.n5now.com/en/sesgos-algoritmos-y-justicia-social-cuando-la-ia-refleja-nuestras-inequidades/>

329. Commission nationale de l’informatique et des libertés (CNIL). Développement des systèmes d’IA : les recommandations de la CNIL pour respecter le RGPD. 8 Apr. 2024. URL: <https://www.cnil.fr/fr/developpement-des-systemes-dia-les-recommandations-de-la-cnil-pour-respecter-le-rgpd>

330. Council on Criminal Justice. Principles for the Use of AI in Criminal Justice. Washington, D.C. : Council on Criminal Justice, Oct. 2025. URL: <https://counciloncj.org/principles-for-the-use-of-ai-in-criminal-justice/>

331. Council of Europe. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108). Strasbourg, 28 Jan. 1981. URL: <https://rm.coe.int/1680078b37>

332. Council of Europe. European Commission for the Efficiency of Justice (CEPEJ). European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment. Strasbourg : Council of Europe, 2018. URL: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>

333. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. CETS No. 225. Vilnius, 5 Sept.

2024. URL: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225>

334. Council of Europe. Methodology for Assessing the Risks and Impacts of Artificial Intelligence Systems from the Perspective of Human Rights, Democracy and the Rule of Law: Resource Model for Context-Based Risk Analysis (COBRA). Strasbourg : Council of Europe, 2025. URL: <https://rm.coe.int/prems-002726-gbr-2006-huderia-texte-web-a4/48802ba7b1>

335. Council of the European Union. Artificial Intelligence: Conclusions on the Coordinated Plan on Artificial Intelligence. Council document 6177/19. Brussels, 11 February 2019. Adopted by the Council on 18 February 2019. URL: <https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/en/pdf>

336. Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108). Guidelines on Facial Recognition. Strasbourg : Council of Europe, 2021. 29 p. URL: <https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.htm>

337. Courtland R. Bias Detectives: The Researchers Striving to Make Algorithms Fair. *Nature*. 2018. Vol. 558, No. 7710. P. 357–360. URL: <https://www.nature.com/articles/d41586-018-05469-3>

338. Crotoft R., Kaminski M. E., Price W. N. II. Humans in the Loop. *Vanderbilt Law Review*. 2023. Vol. 76. Iss. 2. P. 429–504. URL: <https://www.vanderbiltlawreview.org/article/humans-in-the-loop/>

339. Declaration of Principles. Building the Information Society: A Global Challenge in the New Millennium. *World Summit on the Information Society*. Geneva, 10–12 Dec. 2003. Document WSIS-03/GENEVA/DOC/4-E. Geneva : International Telecommunication Union, 2003. URL: <https://www.itu.int/net/wsis/docs/geneva/official/dop.html>

340. Declaration on the Right to Development. United Nations General Assembly Resolution 41/128 of 4 Dec. 1986. Office of the United Nations High Commissioner for Human Rights. URL: <https://www.ohchr.org/en/instruments->

mechanisms/instruments/declaration-right-development

341. Deene J. Can a Judge Use AI to Reach a Verdict, and Will You Still Have a Fair Trial? ICTRecht, 2023. URL: <https://www.ictrechtswijzer.be/en/can-a-judge-use-ai-to-reach-a-verdict-and-will-you-still-have-a-fair-trial/>

342. Dejaview: A Crime Prevention Technology from South Korea. *iConext*. 27 Jan. 2025. URL: <https://iconext.co.th/2025/01/27/dejaview-a-technology-for-crime-prevention/>

343. Dellermann D., Calma A., Lipusch N., Weber T., Weigel S., Ebel P. The Future of Human-AI Collaboration: A Taxonomy of Design Knowledge for Hybrid Intelligence Systems. *arXiv*. 2021. arXiv:2105.03354. URL: <https://arxiv.org/abs/2105.03354>

344. Dellermann D., Ebel P., Söllner M., Leimeister J. M. Hybrid Intelligence. *Business & Information Systems Engineering*. 2019. Vol. 61, No. 5. P. 637–643. URL: <https://doi.org/10.1007/s12599-019-00595-2>

345. Department of Defense. Department of Defense Announces Successful Micro-Drone Demonstration. *CHIPS Magazine*. Jan. 2017. URL: <https://www.war.gov/News/Releases/Release/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration/>

346. Deutch S. AI Judges in Courts of the Future and the Right to a Fair Trial. *SSRN Electronic Journal*. 2025. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5189606

347. Dias S. A. de J., Sátiro R. M. Artificial Intelligence in the Judiciary: A Critical View. *Futures*. 2024. Vol. 164. Article 103493. URL: <https://doi.org/10.1016/j.futures.2024.103493>

348. Dignum V. Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way. Cham : Springer, 2019. 127 p. URL: <https://doi.org/10.1007/978-3-030-30371-6>

349. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 Dec. 2018 Establishing the European Electronic Communications Code

(Recast). *Official Journal of the European Union*. 2018. L 321. P. 36–214.
URL: <https://eur-lex.europa.eu/eli/dir/2018/1972/oj>

350. Dreyfus H. L., Dreyfus S. E. *Mind over Machine: The Power of Human Intuition and Expertise in the Era of the Computer*. New York : Free Press, 1986. 257 p.

URL: <https://www.semanticscholar.org/paper/86cff4d050beb90fed2e1ceac8940c8221b120aa>

351. Dreyfus H. L. *What Computers Can't Do: The Limits of Artificial Intelligence*. Rev. ed. New York : Harper & Row, 1979. 354 p.

352. Duffourc M. N., Cahill R. A. Legal Implications of AI Standard of Care Integration on Patients' Informed Consent: Lessons from Surgery. *npj Digital Medicine*. 2025. Vol. 8. Art. 157.

URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC12764478/>

353. Dvorsky G. Experts Sign Open Letter Slamming Europe's Proposal to Recognize Robots as Legal Persons. *Gizmodo*. 13 Apr. 2018.
URL: <https://gizmodo.com/experts-sign-open-letter-slamming-europe-s-proposal-to-1825240003>

354. Ebers M., Navas S., eds. *Algorithms and Law*. Cambridge : Cambridge University Press, 2020. Chapter: Regulating AI and Robotics. P. 37–99.
URL: <https://www.cambridge.org/core/books/algorithms-and-law/regulating-ai-and-robotics/7734781511EDE9F9A1E4345467AD40BA>

355. Eliot L. B. An Impact Model of AI on the Principles of Justice: Encompassing the Autonomous Levels of AI Legal Reasoning. *arXiv*. 2020.
URL: <https://arxiv.org/abs/2008.12615>

356. Ellis R. K. *Field Guide to Learning Management Systems*. Alexandria, VA : American Society for Training & Development, 2009.
URL: https://web.archive.org/web/20140824102458/http://www.astd.org/~media/Files/Publications/LMS_fieldguide_20091

357. *Ergi v. Turkey*, no. 23818/94, Judgment of 28 July 1998. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=001-58204>

358. Ethics Guidelines for Trustworthy AI. High-Level Expert Group on Artificial Intelligence. Brussels : European Commission, 2019. URL: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

359. ETH Zürich. ChatGPT. AI in Education. URL: <https://ethz.ch/en/the-eth-zurich/education/educational-development/ai-in-education/chatgpt.html>

360. Ethical Autonomy Project. Scharre P. Autonomous Weapons and Operational Risk. Center for a New American Security. Washington, DC, 2016. 54 p. URL: <https://www.cnas.org/publications/reports/autonomous-weapons-and-operational-risk>

361. European Data Protection Board. Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement. Version 2.0. Adopted on 17 May 2023. Brussels : European Data Protection Board, 2023. URL: https://www.edpb.europa.eu/documents/guideline/guidelines-052022-on-the-use-of-facial-recognition-technology-in-the-area-of_en

362. European Commission for the Efficiency of Justice (CEPEJ). European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment. Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3–4 December 2018). Strasbourg : Council of Europe, 2019. 79 p. URL: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>

363. European Commission. 2030 Digital Compass: the European Way for the Digital Decade. Communication from the Commission. COM(2021)118 final. Brussels, 9 March 2021. URL: https://commission.europa.eu/system/files/2023-01/cellar_12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02_DOC_1.pdf

364. European Commission. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM(2021)206 final. Brussels, 21 April 2021. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>

365. European Council. European Council Meeting (19 October 2017) –

Conclusions. EUCO 14/17. Brussels, 19 October 2017.
URL: <https://www.consilium.europa.eu/media/21620/19-euco-final-conclusions-en.pdf>

366. European Council. Special meeting of the European Council (1 and 2 October 2020) – Conclusions. EUCO 13/20. Brussels, 2 October 2020.
URL: <https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf>

367. European Economic and Social Committee (EESC). Artificial Intelligence: Europe Needs to Take a Human-in-Command Approach, Says EESC. Press release, 1 June 2017. Brussels : European Economic and Social Committee.
URL: <https://www.eesc.europa.eu/en/news-media/press-releases/artificial-intelligence-europe-needs-take-human-command-approach-says-eesc>

368. European Parliament. Draft Report on Artificial Intelligence in Education, Culture and the Audiovisual Sector (2020/2017(INI)). Committee on Culture and Education. Brussels, 2021.
URL: [https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2017\(INI\)&l=en](https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2017(INI)&l=en)

369. European Parliament. European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation on artificial intelligence (Artificial Intelligence Act) (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)). Official Journal of the European Union. 2025. C/2025/1027. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C_202501027

370. European Parliament. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) (2018/C 252/25). *Official Journal of the European Union*. 2018. C 252. P. 239–252. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017IP0051>

371. European Parliament. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for

artificial intelligence (2020/2014(INL)) (2021/C 404/76). *Official Journal of the European Union*. 2021. C 404. P. 107–124. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020IP0276>

372. European Parliament. European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies (2020/2015(INI)) (2021/C 404/85). *Official Journal of the European Union*. 2021. C 404. P. 129–143. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020IP0277>

373. European Parliament. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)) (2021/C 404/63). *Official Journal of the European Union*. 2021. C 404. P. 63–86. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020IP0275>

374. Evers V. Of Robots and Humans. *The UNESCO Courier*. 2018. July–September. No. 3. P. 11–13. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000265240>

375. Executive Order 14365 of December 11, 2025. Ensuring a National Policy Framework for Artificial Intelligence. *Federal Register*. 2025. Vol. 90. No. 239. P. 58499–58503. URL: <https://www.federalregister.gov/documents/2025/12/16/2025-23092/ensuring-a-national-policy-framework-for-artificial-intelligence>

376. Financial Action Task Force (FATF). Guidance on Risk-Based Supervision. Paris : FATF, 2021. URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-supervision.html>

377. Flores A. W., Bechtel K., Lowenkamp C. T. False Positives, False Negatives, and False Analyses: A Rejoinder to «Machine Bias». *Federal Probation*. 2016. Vol. 80. No. 2. P. 38–46. URL: https://www.uscourts.gov/sites/default/files/80_2_6_0.pdf

378. Flórez Rojas M. L. Algocracy in the Judiciary: Challenging Trust in the System. *Revista de Estudios Sociales*. 2025. No. 93. P. 107–128.

URL: <https://journals.openedition.org/revestudsoc/59583>

379. Floridi L. The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities. Oxford : Oxford University Press, 2023. 288 p.
URL: <https://doi.org/10.1093/oso/9780198883098.001.0001>

380. Fournier-Tombs E. Towards a United Nations Internal Regulation for Artificial Intelligence. *Big Data & Society*.2021. Vol. 8, Issue 2. DOI: 10.1177/205395172111039493.

381. Framework Act on the Development of Artificial Intelligence and the Creation of a Foundation for Trust. Republic of Korea. Korean Law Translation Center.

URL: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=71019&lang=ENG

382. Friedman B., Hendry D. G. Value Sensitive Design: Shaping Technology with Moral Imagination. Cambridge, MA : MIT Press, 2019. 256 p.

383. Friedman B., Hendry D. G., Borning A. A Survey of Value Sensitive Design Methods. *Foundations and Trends in Human-Computer Interaction*. 2017. Vol. 11, Issue 2. P. 63–125. DOI: 10.1561/11000000015.

384. Full Self-Driving (Supervised). Tesla Support.
URL: <https://www.tesla.com/support/fsd>

385. Future of Life Institute. An Open Letter to the United Nations Convention on Certain Conventional Weapons. 2017.
URL: <https://futureoflife.org/open-letter/autonomous-weapons-open-letter-2017/>

386. Gaebel M., Morrisroe A. The Future of Digitally Enhanced Learning and Teaching in European Higher Education Institutions: Final Report. Brussels : European University Association (EUA), 2023.
URL: https://www.eua.eu/images/pdf/digi-he_final_report.pdf

387. Ganascia J.-G. Artificial Intelligence: Between Myth and Reality. *UNESCO Courier*. 2018. No. 3. P. 7–10.
URL: <https://courier.unesco.org/en/articles/artificial-intelligence-between-myth-and-reality>

388. Gartner Says Worldwide AI Spending Will Total \$1.5 Trillion in 2025.

Gartner. 2025. 17 Sept. URL: <https://www.gartner.com/en/newsroom/press-releases/2025-09-17-gartner-says-worldwide-ai-spending-will-total-1-point-5-trillion-in-2025>

389. Gillis A. S. What Is Internet of Things (IoT)? *TechTarget*. 2021. URL: <https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT>

390. Gomez B. Elon Musk warned of a ‘Terminator’-like AI apocalypse – now he’s building a Tesla robot. *CNBC*. 2021. Aug. 24. URL: <https://www.cnbc.com/2021/08/24/elon-musk-warned-of-ai-apocalypse-now-hes-building-a-tesla-robot.html>

391. Great Britain. House of Lords. Select Committee on Artificial Intelligence. AI in the UK: Ready, Willing and Able? Report of Session 2017–19. HL Paper 100. London : House of Lords, 2018. URL: <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>

392. Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems. Report of the 2019 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems. Geneva : United Nations, 2019. CCW/GGE.1/2019/3. 11 p. URL: <https://documents.un.org/doc/undoc/gen/g19/198/94/pdf/g1919894.pdf>

393. Guersenzvaig A. Autonomous Weapon Systems: Failing the Principle of Discrimination. *IEEE Technology and Society Magazine*. 2018. Vol. 37, No. 1. P. 55–61. URL: https://www.researchgate.net/publication/323595574_Autonomous_Weapon_Systems_Failing_the_Principle_of_Discrimination

394. Güleç v. Turkey, no. 21593/93, Judgment of 27 July 1998. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=001-58215>

395. Harwood S. The Roles of the Provider and Deployer in AI Systems and Models. Stephenson Harwood. 12 September 2024. URL: <https://www.shlegal.com/insights/the-roles-of-the-provider-and-deployer-in-ai-systems-and-models>

396. High-Level Expert Group on Artificial Intelligence. Ethics Guidelines for Trustworthy AI. Luxembourg : Publications Office of the European Union, 2019. 41 p. DOI: <https://doi.org/10.2759/346720>. URL: <https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>

397. Hill K. What We Learned About Clearview AI and Its Secret “Co-Founder”. *The New York Times*. 18 Mar. 2021. URL: <https://www.nytimes.com/2021/03/18/technology/clearview-facial-recognition-ai.html>

398. Hintze A. Understanding the Four Types of AI, from Reactive Robots to Self-Aware Beings. *The Conversation*. 2016. URL: <https://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-67616>

399. Hirosawa T., et al. A Narrative Review of Artificial Intelligence in Medical Imaging and Its Clinical Applications. *Journal of Medical Imaging and Radiation Sciences*. 2025. URL: <https://www.sciencedirect.com/science/article/pii/S1546221825004874>

400. Hoffberger-Pippan E., Vohs V., Köhler P. Autonomous Weapons Systems: UN Expert Talks Facing Failure. *Stiftung Wissenschaft und Politik (SWP)*. URL: <https://www.swp-berlin.org/en/publication/autonomous-weapons-systems-un-expert-talks-facing-failure-time-to-consider-alternative-formats>

401. Horvitz E. Reflections on AI and the Future of Human Flourishing. *AI Anthology*. Microsoft. URL: <https://unlocked.microsoft.com/ai-anthology/eric-horvitz/>

402. How Police Force Uses Data to Assess Risk and Predict Crime. *Financial Times*. 2 July 2018. URL: <https://www.ft.com/content/81af2e14-7fb9-11e8-bc55-50daf11b720d>

403. Huq A. Z. Racial Equity in Algorithmic Criminal Justice. *Duke Law Journal*. 2019. Vol. 68. P. 1043–1134. URL: <https://scholarship.law.duke.edu/dlj/vol68/iss6/1>

404. IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems. Version 2. IEEE, 2017. URL: https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead_v2.pdf

405. IoT Analytics. Number of Connected IoT Devices Growing 13% to 18.8 Billion Globally. 2024. URL: <https://iot-analytics.com/number-connected-iot-devices/>

406. Intelligence Advanced Research Projects Activity (IARPA). About IARPA. URL: <https://www.iarpa.gov/who-we-are/about-us>

407. International Telecommunication Union. Recommendation ITU-T Y.2060. Overview of the Internet of Things. Geneva : ITU, 2012. URL: <https://www.itu.int/rec/T-REC-Y.2060-201206-I/en>

408. International Committee of the Red Cross. Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach. *International Review of the Red Cross*. 2021. Vol. 102, No. 913. P. 453–477. URL: <https://international-review.icrc.org/articles/artificial-intelligence-and-machine-learning-in-armed-conflict-a-human-centred>

409. International Committee of the Red Cross. Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects. Expert Meeting Report, 26–28 March 2014, Geneva. Geneva : ICRC, 2014. URL: <https://www.icrc.org/en/document/report-icrc-meeting-autonomous-weapon-systems-26-28-march-2014>

410. International Committee of the Red Cross. ICRC Position on Autonomous Weapon Systems: ICRC's Recommendations for a Norm-Setting Response to the Issues Raised by Autonomous Weapon Systems. Geneva : ICRC, 2021. 8 p. URL: <https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems>

411. International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use. ICH E6(R3) Guideline for Good Clinical Practice.

2025.

URL: https://database.ich.org/sites/default/files/ICH_E6%28R3%29_Step4_FinalGuideline_2025_0106.pdf

412. In Ukraine, Identifying the Dead Comes at a Human Rights Cost. *WIRED*. 22 Feb. 2023. URL: <https://www.wired.com/story/russia-ukraine-facial-recognition-technology-death-military>

413. Ipsos. Six in Ten (61%) Respondents Across 26 Countries Oppose the Use of Lethal Autonomous Weapons Systems. Research Findings. 2019. URL: https://www.ipsos.com/sites/default/files/ct/news/documents/2019-01/human-rights-watch-autonomous-weapons-pr-01-22-2019_0.pdf

414. Jonas H. The Imperative of Responsibility: In Search of an Ethics for the Technological Age. Chicago : The University of Chicago Press, 1984. 255 p.

415. Johnson K. Face Recognition Software Led to His Arrest. It Was Dead Wrong. *WIRED*. 28 Feb. 2023. URL: <https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/>

416. Johnson K. B., et al. Precision Medicine, AI, and the Future of Personalized Health Care. *Journal of the American Medical Informatics Association*. 2020. Vol. 27, No. 2. P. 201–207. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC7877825/>

417. Judson J. Iron Dome Batteries Activated to Fill Cruise Missile Defense Gap. *Defense News*. 13 Nov. 2020. URL: <https://www.defensenews.com/land/2020/11/13/iron-dome-batteries-activated-to-fill-cruise-missile-defense-gap/>

418. Kallenborn Z. Meet the Future Weapon of Mass Destruction, the Drone Swarm. *Bulletin of the Atomic Scientists*. 2021. URL: <https://thebulletin.org/2021/04/meet-the-future-weapon-of-mass-destruction-the-drone-swarm>

419. Kharpal A. Stephen Hawking Says AI Could Be “Worst Event in the History of Our Civilization.” *CNBC*. 2017. URL: <https://www.cnn.com/2017/11/06/stephen-hawking-ai-could-be-worst-event->

in-civilization.html

420. Kinoshita G.-I., Aida S., Mori M. A Pattern Classification by the Time-Varying Threshold Method: Application of the Method to Visual and Tactile Senses. *Proceedings of the First International Joint Conference on Artificial Intelligence (IJCAI-69)*. Washington, D.C., 1969. P. 417–427.

421. Köhler W. *The Mentality of Apes*. London : Routledge & Kegan Paul, 1925. 342 p.

422. Kondrup E. Informed Consent, Redefined: How AI and Big Data Are Changing the Rules. Petrie-Flom Center Blog. 11 Apr. 2025. URL: <https://petrieflom.law.harvard.edu/2025/04/11/informed-consent-redefined-how-ai-and-big-data-are-changing-the-rules/>

423. Kott A. Challenges and Characteristics of Intelligent Autonomy for Internet of Battle Things in Highly Adversarial Environments. *Proceedings of the AAAI Spring Symposium*. 2018. URL: <https://ui.adsabs.harvard.edu/abs/2018arXiv180311256K/abstract>

424. Krohs U. Informed Consent to AI-Based Decisions in Healthcare: Must Patients Understand the AI's Output? *Oslo Law Review*. 2024. Vol. 11. No. 1. P. 97–118. URL: <https://www.idunn.no/doi/10.18261/olr.11.1.7>

425. Lapenna S. What Is Internet of Things (IoT)? 139+1 Definitions Since 1999. *IoT Insights*. 2022. URL: <https://www.rtsrl.eu/blog/what-is-internet-of-things-iot/>

426. Law Enforcement Embraces AI for Efficiency amid Rising Privacy Concerns. GIP Digital Watch Observatory. 28 Aug. 2025. URL: <https://dig.watch/updates/law-enforcement-embraces-ai-for-efficiency-amid-rising-privacy-concerns>

427. Li T. W., Hsu S., Fowler M., Zhang Z., Zilles C., Karahalios K. Am I Wrong, or Is the Autograder Wrong? Effects of AI Grading Mistakes on Learning. *Proceedings of the 2023 ACM Conference on International Computing Education Research (ICER '23)*. New York : ACM, 2023. URL: <https://doi.org/10.1145/3568813.3600124>

428. Lopes G. P. Bias in Adjudication and the Promise of AI: Challenges to Procedural Fairness. *Law, Technology and Humans*. 2025. Vol. 7. No. 1. P. 47–69. URL: <https://repository.tilburguniversity.edu/server/api/core/bitstreams/189d57e1-574e-4d69-9890-392d27efa57e/content>
429. Mac R., Hill K. Clearview AI Settles Suit and Agrees to Limit Sales of Facial Recognition Database. *The New York Times*. 9 May 2022. URL: <https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html>
430. Machi V. Internet of Things to Provide Intelligence for Urban Warfare. *National Defense*. 22 Jan. 2018. URL: <https://www.nationaldefensemagazine.org/articles/2018/1/22/internet-of-things-to-provide-intelligence-for-urban-warfare>
431. Mantelero A. Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI. The Hague : T.M.C. Asser Press, 2022. 200 p. DOI: <https://doi.org/10.1007/978-94-6265-531-7>
432. Marchant G. E. “Soft Law” Governance of Artificial Intelligence. In: Werthner H., Prem E., Lee E. A., Ghezzi C. (eds.). *AI, Robotics, and Society*. Cambridge : Cambridge University Press, 2021. P. 56–68.
433. Marchant G. E., Meyer A., Scanlon M. Integrating Social and Ethical Concerns into Regulatory Decision-Making for Emerging Technologies. *Minnesota Journal of Law, Science & Technology*. 2010. Vol. 11, No. 1. P. 345–381.
434. Marchant G. E., Meyer A., Scanlon M. Regulatory Frontiers: Integrating Social and Ethical Concerns into Regulatory Decision-Making for Emerging Technologies. In: Brownsword R., Scotford E., Yeung K. (eds.). *The Oxford Handbook of the Law and Regulation of Technology*. Oxford : Oxford University Press, 2017.
435. Martin K. D., Zimmermann J. Artificial Intelligence and Its Implications for Data Privacy. *Journal of Responsible Technology*. 2024. Vol. 19. URL: <https://www.sciencedirect.com/science/article/pii/S2666659624000423>
436. McCarthy J., Minsky M. L., Rochester N., Shannon C. E. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence: August 31,

1955. *AI Magazine*. 2006. Vol. 27, No. 4. P. 12–14. URL: AI Magazine
437. McCann and Others v. the United Kingdom. No. 18984/91, Judgment of 27 Sept. 1995. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=001-57943>
438. McCorduck P. *Machines Who Think*. 2nd ed. Natick, MA : A. K. Peters, 2004. 576 p.
439. Met Police Use of Facial Recognition in London Surges. *Financial Times*. 2024. URL: <https://www.ft.com/content/c33322a7-eba7-4299-8172-4ce1d4e88908>
440. Minds Beyond the Brain. *The UNESCO Courier*. July–September 2018. P. 15–17. URL: <https://unesco.public.lu/dam-assets/courriers/265211eng.pdf>
441. Mirbabaie M., Stieglitz S., Frick N. R. J. Artificial Intelligence in Disease Diagnostics: A Critical Review and Classification on the Current State of Research Guiding Future Direction. *Health and Technology*. 2021. Vol. 11. P. 693–731. URL: <https://link.springer.com/article/10.1007/s12553-021-00555-5>
442. Mittelstadt B. The Impact of Artificial Intelligence on the Doctor-Patient Relationship. Strasbourg : Council of Europe, Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO), 2022. 67 p. URL: <https://edoc.coe.int/en/bioethics/11065-the-impact-of-artificial-intelligence-on-the-doctor-patient-relationship.html>
443. Medsker L. R. *Hybrid Intelligent Systems*. Boston : Kluwer Academic Publishers, 1995. 289 p.
444. Megalokonomou R., Goulas S., Sotirakopoulos P. Flawed Oversight: Teachers Don't Catch AI's Grading Mistakes When AI Is Harsh. *SSRN Electronic Journal*. 2025. URL: <https://ssrn.com/abstract=5294732>
445. Merleau-Ponty M. *Phenomenology of Perception*. Translated by Colin Smith. London : Routledge, 1962. 544 p.
446. Moor J. H. The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years. *AI Magazine*. 2006. Vol. 27, No. 4. P. 87–91.
447. Moroianu Zlătescu I., Zlătescu P. E. Implementation of the European

Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment. SSRN Electronic Journal, 2022.
URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4067356

448. Morrow J. D. Improving the Operator-Swarm Dynamic under Mental Fatigue Constraints : Master's Thesis. Missouri University of Science and Technology. 2025. 62 p.
URL: https://scholarsmine.mst.edu/cgi/viewcontent.cgi?article=9232&context=masters_theses

449. Musk E. Full Elon Musk Interview with Tucker Carlson Fox News (Unedited). YouTube. 2023.
URL: <https://www.youtube.com/watch?v=bQ45lsDxL6Q>

450. Musk E. Interview at Atreju 2023. Agenzia Italia News. 16 Dec. 2023. YouTube. URL: https://www.youtube.com/watch?v=WPf4_5DCP-E

451. Musk E. Remarks at the MIT AeroAstro Centennial Symposium. Massachusetts Institute of Technology. 24 Oct. 2014.
URL: <https://www.youtube.com/watch?v=YRvf00NooN8>

452. Musk E. Remarks at the Wall Street Journal CEO Council Summit. London, 23 May 2023. *The Independent*. 24 May 2023. URL: <https://www.the-independent.com/tv/news/elon-musk-ai-weapons-technology-b2344971.html>

453. Müller V. C. Autonomous Killer Robots Are Probably Good News. *Drones and Responsibility: Legal, Philosophical and Sociotechnical Perspectives on the Use of Remotely Controlled Weapons*. Cham : Springer, 2016. P. 67–81. URL: <https://philarchive.org/rec/MLLAKR>

454. Nahavandi S. Trusted Autonomy Between Humans and Robots: Toward Human-on-the-Loop in Robotics and Autonomous Systems. *IEEE Systems, Man, and Cybernetics Magazine*. 2017. Vol. 3, No. 1. P. 10–17.
URL: https://www.deakin.edu.au/__data/assets/pdf_file/0003/1344477/Trusted-autonomy-IEEE-article.pdf

455. Novelli C., Hacker P., Morley J., Trondal J., Floridi L. A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National

Authorities. *arXiv*. 2024. URL: <https://arxiv.org/pdf/2407.10369>

456. North Atlantic Treaty Organization. NATO Allies Take Further Steps Towards Responsible Use of AI, Data, Autonomy and Digital Transformation. URL: https://www.nato.int/cps/en/natohq/news_208342.htm

457. North Atlantic Treaty Organization. Summary of NATO's Autonomy Implementation Plan. URL: https://www.nato.int/cps/en/natohq/official_texts_208376.htm

458. Okinawa Charter on Global Information Society : G8 Kyushu–Okinawa Summit, Okinawa, 22 July 2000. URL: <https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html>

459. O. Reg. 306/15: Pilot Project – Automated Vehicles. Highway Traffic Act. Ontario e-Laws. URL: <https://www.ontario.ca/laws/regulation/150306>

460. Petit N. Law and Regulation of Artificial Intelligence and Robots: Conceptual Framework and Normative Implications. *SSRN Electronic Journal*. 2017. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2931339

461. Proceedings of the First International Joint Conference on Artificial Intelligence (IJCAI-69). Washington, D.C., 7–9 May 1969. URL: <https://dblp.org/db/conf/ijcai/ijcai69.html>

462. Pouillet Y. Do We Need Regulation of the Digital Platforms? – An EU Approach. Presentation delivered at the AI4IA (Artificial Intelligence for Information Accessibility). *Conference, UNESCO Information for All Programme (IFAP)*, 28 September 2021. URL: <https://ai4iaconference.com/2021-ai4ia-conference-resources/>

463. Rafael Advanced Defense Systems Ltd. Iron Dome Air Defense System. URL: <https://www.rafael.co.il/worlds/air-missile-defense/iron-dome/>

464. Ramanath. AI Incident Database Statistics 2026. *Presenc AI*. Updated May 2026. URL: <https://presenc.ai/research/ai-incident-database-statistics-2026>

465. Recommendation CM/Rec(2020)1 of the Committee of Ministers to Member States on the Human Rights Impacts of Algorithmic Systems. Adopted by the Committee of Ministers on 8 April 2020. *Council of Europe*. URL: Official PDF

466. Reed C. How Should We Regulate Artificial Intelligence? *Philosophical Transactions of the Royal Society A*. 2018. Vol. 376. Article 20170360. DOI: 10.1098/rsta.2017.0360.

467. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). *Official Journal of the European Union*. 2016. OJ L 119. P. 1–88. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

468. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC and repealing Council Directives 90/385/EEC and 93/42/EEC. *Official Journal of the European Union*. 2017. OJ L 117. P. 1–175. URL: <https://eur-lex.europa.eu/eli/reg/2017/745/oj>

469. Regulation (EU) 2018/1971 of the European Parliament and of the Council of 11 December 2018 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Agency for Support for BEREC (BEREC Office). *Official Journal of the European Union*. 2018. L 321. P. 1–35. URL: <https://eur-lex.europa.eu/eli/reg/2018/1971/oj>

470. Regulation (EU) 2024/1350 of the European Parliament and of the Council of 14 May 2024 Establishing a Union Resettlement and Humanitarian Admission Framework and Amending Regulation (EU) 2021/1147. *Official Journal of the European Union*. 2024. L. URL: <https://eur-lex.europa.eu/eli/reg/2024/1350/oj>

471. Regulation (EU) 2024/1351 of the European Parliament and of the Council of 14 May 2024 on Asylum and Migration Management, Amending Regulations (EU) 2021/1147 and (EU) 2021/1060 and Repealing Regulation (EU) No 604/2013. *Official Journal of the European Union*. 2024. L. URL: <https://eur-lex.europa.eu/eli/reg/2024/1351/oj>

472. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. 2024.

URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

473. Riaz C. H. Legal Technology and Bias: A Threat to Fair Trial Rights? *International Journal of Science and Research Archive*. 2025. Vol. 16. No. 2. P. 299–304. URL: https://journalijsra.com/sites/default/files/fulltext_pdf/IJSRA-2025-2310.pdf

474. Rigano C. Using Artificial Intelligence to Address Criminal Justice Needs. *National Institute of Justice*. 2019. URL: <https://www.ojp.gov/pdffiles1/nij/252038.pdf>

475. Robot Ethics Charter Establishment Committee. Robot Ethics Charter Establishment Committee Report. Ministry of Commerce, Industry and Energy, Republic of Korea, 2007.

476. Roman Zakharov v. Russia, no. 47143/06, Judgment of 4 Dec. 2015. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=001-159324>

477. Rudenko O., Zaika O., Varynskyi V., Kulchii I., Myroshnychenko A. Digitization of local self-government based on the use of artificial intelligence in the context of sustainable development. *Edelweiss Applied Science and Technology*, 2024. Vol. 8, No. 6. P. 1468–1480. URL: <https://doi.org/10.55214/25768484.v8i6.2263>

478. Rudenko O., Rafalskyi I., Yermak O., Varynskyi V., Konoplia Y. The Potential and Prospects of Artificial Intelligence Use in Strategic Planning: Issues of Security and Defense. *AD ALTA: Journal of Interdisciplinary Research*. 2024. Vol. 14/02-XLIV. 6-12. URL: https://www.magnanimitas.cz/ADALTA/140244/papers/A_01.pdf

479. Russell S. Human Compatible: Artificial Intelligence and the Problem of Control. New York : Viking, 2019. 352 p.

480. Russell S. J., Norvig P. Artificial Intelligence: A Modern Approach. 2nd ed. Upper Saddle River, NJ : Prentice Hall, 2003. 1132 p.

481. Shelever N., Varynskyi V., Burdonosova M., Rogach O., Pylyp V. Electronic Means of Ensuring Fair Justice: Contemporary and Development

Prospects. *Lex Humana*. 2024. Vol. 16(1). 557–572. URL: <https://seer.ucp.br/seer/index.php/LexHumana/article/view/2973>

482. Searle J. R. *Minds, Brains and Science*. Cambridge, MA : Harvard University Press, 1984. 104 p.

483. Selçuk S., Konca N. K., Kaya S. AI-Driven Civil Litigation: Navigating the Right to a Fair Trial. *Computer Law & Security Review*. 2025. Vol. 57. Article 106136.

URL: <https://www.sciencedirect.com/science/article/pii/S2212473X25000094>

484. Simmler M., Canova G. Facial Recognition Technology in Law Enforcement: Regulating Data Analysis of Another Kind. *Computer Law & Security Review*. 2024.

URL: <https://www.sciencedirect.com/science/article/pii/S0267364924001572>

485. Slyusar V. Artificial Intelligence as the Basis of Future Control Networks. Coordination Problems of Military Technical and Defense Industrial Policy in Ukraine. *Weapons and Military Equipment Development Perspectives : Proceedings of the VII International Scientific and Practical Conference*. Kyiv, 8–10 October 2019. P. 76–77.

486. Sreelatha A. Exploring the Use of AI in Legal Decision Making: Benefits and Ethical Implications. *Woxsen University White Papers*. 31 May 2021. URL: <https://woxsen.edu.in/research/white-papers/exploring-the-use-of-ai-in-legal-decision-making-benefits-and-ethical-implications/>

487. SRI International. SRI International Leading Security Research for U.S. Army Research Lab Initiative to Develop and Secure the Internet of Battlefield Things (IoBT). PR Newswire. 2018. URL: <https://www.prnewswire.com/news-releases/sri-international-leading-security-research-for-us-army-research-lab-initiative-to-develop-and-secure-the-internet-of-battlefield-things-iobt-300601689.html>

488. Standing Committee of the National People's Congress of the People's Republic of China. Personal Information Protection Law of the People's Republic of China. *Adopted at the 30th Meeting of the Standing Committee of the Thirteenth*

National People's Congress on 20 August 2021. Beijing, 2021.
URL: https://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm

489. Stolper I. Towards Automated Decision-Making at Court: The Use of Artificial Intelligence for Drafting and Rendering Court Decisions. *Teisė*. 2024. Vol. 130. P. 153–163.
URL: <https://www.zurnalai.vu.lt/teise/en/article/download/35434/33743/92188>

490. Stone A. The Answer to Battlefield Logistics Problems Could Be IoT. *C4ISRNET*. 12 Oct. 2018. URL: <https://www.c4isrnet.com/it-networks/2018/10/12/the-answer-to-battlefield-logistics-problems-could-be-iot/>

491. Stone A. When Big Data Gets It Wrong. *Government Technology*. Mar. 2017. URL: <https://www.govtech.com/data/when-big-data-gets-it-wrong.html>

492. Swoboda T. Autonomous Weapon Systems: An Alleged Responsibility Gap. *Philosophy and Theory of Artificial Intelligence 2017*. Studies in Applied Philosophy, Epistemology and Rational Ethics. Vol. 44. Cham : Springer, 2018. P. 409–421. URL: https://link.springer.com/chapter/10.1007/978-3-319-96448-5_32

493. Tegmark M. Life 3.0: Being Human in the Age of Artificial Intelligence. New York : Alfred A. Knopf, 2017. 384 p.

494. The Bletchley Declaration by Countries Attending the AI Safety Summit, 1–2 November 2023. AI Safety Summit. Bletchley Park, Buckinghamshire, United Kingdom, 1 November 2023.
URL: <https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023>

495. The First European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems Has Been Adopted by the Council of Europe. *EEEI – Experts Institute*. 2 Jan. 2019. URL: <https://experts-institute.eu/en/europe-of-justice/cepej-en/first-european-ethical-charter-on-the-use-of-artificial-intelligence-in-judicial-systems-has-adopted-by-the-council-of-europe/>

496. The Global Centre for Risk and Innovation (GCRI). *AI Catastrophic Risks*. *The Risk*. URL: <https://therisk.global/catastrophic-risks-pathways/>

497. The Role of Patient Informed Consent in AI-Driven Treatment. *Credemtia Insights*. 10 Sept. 2024. URL: <https://credemtia.com/newsletters/the-role-of-patient-informed-consent-in-ai-driven-treatment>

498. Tian Z., Liu A., Esbenshade L., Sarkar S., Zhang Z., He K., Sun M. Implementation Considerations for Automated AI Grading of Student Work. *Proceedings of the Artificial Intelligence in Measurement and Education Conference (AIME-Con): Full Papers*. Pittsburgh, PA : National Council on Measurement in Education (NCME), 2025. P. 9–20. URL: <https://aclanthology.org/2025.aimecon-main.2/>

499. Tomorrow's Affairs Staff. China Introduces the First Global Rules for AI with Human-Like Interaction. *Tomorrow's Affairs*. 29 December 2025. URL: <https://tomorrowsaffairs.com/china-introduces-the-first-global-rules-for-ai-with-human-like-interaction>

500. Transforming Our World: the 2030 Agenda for Sustainable Development : United Nations General Assembly Resolution A/RES/70/1 of 25 September 2015. United Nations. URL: <https://docs.un.org/en/A/RES/70/1>

501. Trebo M. Autonomous Weapon Systems: Existential Threat? SCIP AG. 2023. URL: <https://www.scip.ch/en/?labs.20230309>

502. UNESCO. AI4IA 2021: Artificial Intelligence for Information Accessibility : Conference Report. Paris : UNESCO, 2021. P. 24–26. URL: <https://unesdoc.unesco.org/>

503. UNESCO. Global Toolkit on AI and the Rule of Law for the Judiciary. UNESCO, 2023. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000387331>

504. UK Government. AI Safety Summit 2023. GOV.UK. 2023. URL: <https://www.gov.uk/government/topical-events/ai-safety-summit-2023>

505. United Nations. Agenda 21: Programme of Action for Sustainable Development. *Adopted at the United Nations Conference on Environment and Development*, Rio de Janeiro, 3–14 June 1992. New York : United Nations, 1992. URL: <https://sustainabledevelopment.un.org/outcomedocuments/agenda21>

506. United Nations. Human Rights Council. Special Rapporteur on the

Independence of Judges and Lawyers. *Artificial Intelligence in Judicial Systems: Promises and Pitfalls*. Report of the Special Rapporteur on the Independence of Judges and Lawyers, Margaret Satterthwaite. UN Doc. A/80/169. New York : United Nations, 2025. URL: <https://www.ohchr.org/en/documents/thematic-reports/a80169-ai-judicial-systems-promises-and-pitfalls-report-special>

507. United Nations General Assembly. Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development : Resolution adopted by the General Assembly on 21 March 2024. A/RES/78/265. New York : United Nations, 2024. URL: <https://digitallibrary.un.org/record/4043244>

508. United Nations General Assembly. Lethal Autonomous Weapons Systems : Resolution adopted by the General Assembly on 22 December 2023. A/RES/78/241. New York : United Nations, 2024. URL: <https://digitallibrary.un.org/record/4033027>

509. United Nations General Assembly. Lethal Autonomous Weapons Systems : Resolution adopted by the General Assembly on 2 December 2024. A/RES/79/77. New York : United Nations, 2024. URL: <https://digitallibrary.un.org/record/4071100>

510. United Nations. United Nations Millennium Declaration. Resolution adopted by the General Assembly on 8 September 2000. A/RES/55/2. New York : United Nations, 2000. URL: <https://undocs.org/A/RES/55/2>

511. United Nations. Note to Correspondents: Joint Call by the United Nations Secretary-General and the President of the International Committee of the Red Cross for States to Establish New Prohibitions and Restrictions on Autonomous Weapon Systems. 5 Oct. 2023. URL: <https://www.un.org/sg/en/content/sg/note-correspondents/2023-10-05/note-correspondents-joint-call-the-united-nations-secretary-general-and-the-president-of-the-international-committee-of-the-red-cross-for-states-establish-new>

512. Universal Declaration of Human Rights. United Nations General Assembly Resolution 217 A (III), 10 December 1948. United Nations. URL: <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

513. U.S. Army Research Laboratory. Internet of Battlefield Things (IoBT) Collaborative Research Alliance (CRA). 2017. URL: <https://arl.devcom.army.mil/cras/iobt-cra/>

514. U.S. Food and Drug Administration. Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan. 2021. URL: <https://www.fda.gov/media/145022/download>

515. U.S. Department of Defense. Autonomy in Weapons Systems. Department of Defense Directive 3000.09. Washington, DC, 2023 (current version). URL: <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf>

516. U.S. Department of Justice. Office of Legal Policy. *Artificial Intelligence and Criminal Justice: Final Report in Response to Executive Order 14110*. Washington, D.C. : U.S. Department of Justice, 2024. URL: <https://www.justice.gov/olp/media/1381796/dl>

517. Vallenias N., Parent B. Informed Consent in the Age of Value-Laden Medical AI. *Journal of Ethics in Entrepreneurship and Technology*. 2025. URL: https://www.ivysci.com/en/articles/11993110__Informed_consent_in_the_age_of_valueladen_medical_AI

518. Varynskyi, V., Varynska, A., Kostytsky, M., & Kushakova-Kostytska, N. Information security and information hygiene on internet media. *Nexo Revista Científica*, 2021. 34(01), 120-128. URL: <https://doi.org/10.5377/nexo.v34i01.11291>

519. Varynskyi, V., Shelever, N., Yankovyi, M., Pylyp, V., Antalovtsi, O. & Halahan, O. Use of the “electronic court” service as a means of citizens' access to the judiciary. *Lex Humana*. 2023. № 16(1), 249–266. URL: <https://seer.ucp.br/seer/index.php/LexHumana/article/view/2891>

520. Varynskyi V. Health-Saving Technologies in the Context of Globalization *International Journal of Recent Technology and Engineering (IJRTE)*, 2019. № 8(4S), 63-67. DOI: 10.35940/ijrte.D1023.1184S19

521. Varynskyi V., Donnikova I., Savinova N. Artificial Intelligence in Education: Tool, Object, ‘Subject’ of Learning. *Journal of International Legal*

Communication (JILC). 2023. № 10(3), 46-55. URL : <https://doi.org/10.32612/uw.27201643.2023.10.3.pp.46-55>

522. Vaughan H. AI Tool That Can Do “81 Years of Detective Work in 30 Hours” Trialled by Police. *Sky News*. 24 Sept. 2024. URL: <https://news.sky.com/story/ai-tool-that-can-do-81-years-of-detective-work-in-30-hours-trialled-by-police-13220891>

523. Verheij B. Arguments for Ethical Systems Design. *Legal Knowledge and Information Systems: JURIX 2016, the Twenty-Ninth Annual Conference* / eds. F. J. Bex, S. Villata. Amsterdam : IOS Press, 2016. P. 101–110. DOI: 10.3233/978-1-61499-726-9-101.

524. Vokrug A. Artificial Intelligence and Legal Identity. *Unite.AI*. 27 Oct. 2023. URL: <https://www.unite.ai/artificial-intelligence-and-legal-identity>

525. Wagner M. G. The Problem with AI Grading: Reflections on Automation, Assessment, and the Human Element in Education. *The Augmented Educator*. 6 Feb. 2025. URL: <https://www.theaugmentededucator.com/p/the-problem-with-ai-grading>

526. Walsh T. What Risks Does Artificial Intelligence Pose? *World Economic Forum*. 16 Jan. 2015. URL: <https://www.weforum.org/stories/2015/01/what-risks-does-artificial-intelligence-pose/>

527. Washington A. L. How to Argue with an Algorithm: Lessons from the COMPAS–ProPublica Debate. *Colorado Technology Law Journal*. 2019. Vol. 17. No. 1. P. 131–160. URL: https://ctlj.colorado.edu/wp-content/uploads/2021/02/17.1_4-Washington_3.18.19.pdf

528. Watkins M. The Dangers of Using AI to Grade: Nobody Learns, Nobody Gains. *Substack*. 10 Oct. 2025. URL: <https://marcwatkins.substack.com/p/the-dangers-of-using-ai-to-grade>

529. What Is Facial Recognition. Kaspersky Resource Center. URL: <https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition>

530. World Health Organization. WHO Issues First Global Report on Artificial Intelligence (AI) in Health and Six Guiding Principles for Its Design and Use. 28 June 2021. URL: <https://www.who.int/news/item/28-06-2021-who-issues-first-global-report-on-ai-in-health-and-six-guiding-principles-for-its-design-and-use>

531. World Intellectual Property Organization. Artificial Intelligence and Intellectual Property Policy Considerations. WIPO Publication No. 1055. Geneva: WIPO, 2020. URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf

ДОДАТКИ

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, у яких опубліковано основні наукові результати дисертації

Монографія

1. Варинський В. Штучний інтелект в освіті: проблеми впровадження та регулювання. *Створювальна сила знання* : монографія. Книга друга / авт. кол. ; відп. ред.: І. А. Доннікова, Н. В. Кривцова. Київ : 7БЦ, 2025. С. 145–163.

Статті у наукових виданнях, включених до Переліку наукових фахових видань України

2. Варинський В. О. Сучасні напрямки соціально-правових досліджень штучного інтелекту. *Наукові перспективи*. 2022. №. 12 (30). С. 299–310. DOI: [https://doi.org/10.52058/2708-7530-2022-12\(30\)-299-310](https://doi.org/10.52058/2708-7530-2022-12(30)-299-310)

3. Варинський В. О. Правосуб'єктність штучного інтелекту: міф чи реальність. *Юридична Україна*. 2024. № 11. С. 60–68. DOI: 10.37749/2308-9639-2024-11(263)-6. URL: <https://yur-ukraine.com/pravosubyektnist-shtuchnogo-intelektu-mif-chy-realnist-2/>

4. Варинський В. О. Правосуб'єктність штучного інтелекту: критичний погляд на автономність. *Інформація і право*. 2024. № 4 (51). С. 83–94. DOI: [https://doi.org/10.37750/2616-6798.2024.4\(51\).317919](https://doi.org/10.37750/2616-6798.2024.4(51).317919)

5. Варинський В. О. Стан правового регулювання використання штучного інтелекту у законодавстві України. *Юридична Україна*. 2025. № 1. С. 40–50. DOI: 10.37749/2308-9639-2025-1(265)-6. URL: <https://yur-ukraine.com/stan-pravovogo-regulyuvannya-vykorystannya-shtuchnogo-intelektu-u-zakonodavstvi-ukrayiny>

6. Варинський В. О. Соціально-правові чинники формування довіри до штучного інтелекту (Частина 1). *Право і суспільство*. 2025. № 6. С. 524–532. DOI: <https://doi.org/10.32842/2078-3736/2025.6.73>

7. Варинський В. О. Основні підходи правового регулювання використання штучного інтелекту в освіті. *Актуальні проблеми вдосконалення*

чинного законодавства України. 2025. № 69. С. 140–151. DOI: <https://doi.org/10.15330/apiclu.69.1.40-1.51>

8. Варинський В. Алгоритмічне забезпечення охорони громадського порядку : правові межі застосування штучного інтелекту у діяльності правоохоронних органів. *Академічні візії*. 2025. № 48. С. 1–11. URL: <https://www.academy-vision.org/index.php/av/article/view/3189>

9. Варинський В.О. Нормативне регулювання використання штучного інтелекту у правосудді. *Журнал східноєвропейського права*. 2025. № 140. С. 291 – 299. DOI: <http://doi.org/10.71404/2409-6415.140.35>

10. Варинський В. О. Правова парадигма довіри до штучного інтелекту (Частина II). *Право і суспільство*. 2026. № 1. С. 258–264. DOI <https://doi.org/10.32842/2078-3736/2026.1.1.33>

11. Варинський В. О. Етичні та правові ризики застосування штучного інтелекту у правоохоронній діяльності та діяльності спецслужб. *Вісник Пенітенціарної асоціації України*. 2026. №1 (35). С. 245–256. DOI: <https://doi.org/10.34015/2523-4552.2026.1.22>

12. Варинський В. О. AI Акт як ризик-орієнтована модель правового обмеження застосування штучного інтелекту у правоохоронній діяльності та діяльності спецслужб. *Південноукраїнський правничий часопис*. 2026. № 1. С. 134–141. DOI : <https://doi.org/10.32850/sulj.2026.1.23>

13. Варинський В. Правове регулювання обмеження використання штучного інтелекту в медицині: основні міжнародні підходи. *Український часопис міжнародного права*. 2026. № 1. С. 21–33. DOI: <https://doi.org/10.36952/ujil.2026.1.3>

14. Варинський В. О. Оцінка впливу високоризикових систем штучного інтелекту на права людини як інструмент правової політики України. *Академічні візії*. 2026. Вип 53. DOI: <https://doi.org/10.66556/2786-586X.53.varynskyi-v>

*Статті у закордонних виданнях, проіндексованих у базах даних Web of Science
Core Collection та/або Scopus*

15. Varynskyi V., Varynska A., Kostytsky M., Kushakova-Kostytska N. Information security and information hygiene on internet media. *Nexo Revista Científica*. 2021. Vol. 34. № 1. P. 120–128. DOI: <https://doi.org/10.5377/nexo.v34i01.11291>

16. Varynskyi V., Shelever N., Yankovyi M., Pylyp V., Antalovtsi O., Halahan O. Use of the “electronic court” service as a means of citizens' access to the judiciary. *Lex Humana*. 2023. Vol. 16. № 1. P. 249–266. URL: <https://seer.ucp.br/seer/index.php/LexHumana/article/view/2891>

17. Rudenko O., Rafalskyi I., Yermak O., Varynskyi V., Konoplia Y. The potential and prospects of artificial intelligence use in strategic planning: issues of security and defense. *AD ALTA: Journal of Interdisciplinary Research*. 2024. Vol. 14/02-XLIV. P. 6–12. URL: https://www.magnanimitas.cz/ADALTA/140244/papers/A_01.pdf

18. Rudenko O., Zaika O., Varynskyi V., Kulchii I., Myroshnychenko A. Digitization of local self-government based on the use of artificial intelligence in the context of sustainable development. *Edelweiss Applied Science and Technology*. 2024. Vol. 8. № 6. P. 1467–1480. DOI: <https://doi.org/10.55214/25768484.v8i6.2263>

Статті у наукових періодичних виданнях інших держав

19. Varynskyi V. Health-saving technologies in the context of globalization. *International Journal of Recent Technology and Engineering (IJRTE)*. 2019. Vol. 8. Issue 4S. P. 63–67. DOI: 10.35940/ijrte.D1023.1184S19

20. Varynskyi V., Donnikova I., Savinova N. Artificial intelligence in education: tool, object, «subject» of learning. *Journal of International Legal Communication*. 2023. Vol. 10. № 3. P. 46–55. DOI: <https://doi.org/10.32612/uw.27201643.2023.10.3.pp.46-55>

Наукові праці, які засвідчують апробацію матеріалів дисертації

11. Варинський В.О., Савінова Н.А. Два епізоди кримінальної юстиції майбутнього: футуристичний прогноз. *Наукові читання присвячені пам'яті професора Т.А. Денисової* : збірник матеріалів (м. Запоріжжя, 10 березня 2022

р.). Класичний приватний університет. Запоріжжя : КПУ, 2022. С. 308–311.

12. Варинський В. Філософські засади концепції інтернету речей. *Людина має право: соціально-гуманітарний дискурс у контексті реформаційних процесів в Україні*: матеріали круглого столу (м. Одеса, 17 листопада 2022 р.). Одеса : ОДУВС, 2022. С. 15–18. URL: <http://dspace.pdpu.edu.ua/jspui/bitstream/123456789/16985/1/SviRLYTSKAIA.pdf#page=16>

13. Варинський В.О. Основні настанови резолюції Європарламенту про цивільно-правові норми в робототехніці та штучний інтелект: дайджест основних підходів. *Вдосконалення правового регулювання прав та основних свобод людини і громадянина* : матеріали щорічної Всеукраїнської науково-практичної конференції молодих вчених (м. Івано-Франківськ, 5-6 травня 2023 р.). Івано-Франківськ, 2023. С. 78–81. URL: <https://law.cnu.edu.ua/wp-content/uploads/sites/100/2024/12/youth2023-r.pdf>

14. Варинський В. Штучний інтелект та освіта. *Створювальне знання: освіта для майбутнього* : матеріали 6-го круглого столу в рамках науково-освітнього міжнародного проєкту «Створювальне знання: науково-освітні практики 3.0» (м. Одеса, 9 червня 2023 р.). Одеса : НУОМА, 2023. С. 5–8. URL: http://onma.edu.ua/wp-content/uploads/2023/09/Materialy_6-go_kruglogo-stolu_23.pdf

15. Варинський В. Штучний інтелект та проблеми безпеки. *Сучасна парадигма публічного управління* : збірник тез V Міжнародної науково-практичної конференції (м. Львів, 30 листопада – 2 грудня 2023 р.) / За наук. ред. к.е.н., доцента Стасишина А.В. Львів: ЛНУ імені Івана Франка. Львів, 2024. С. 512–515. URL: https://nung.edu.ua/sites/default/files/2024-06/Збірник_5_Парадигма_2024.pdf

16. Варинський В.О. Ризики використання елементів штучного інтелекту в розробках автономної зброї: на шляху визначень нормативних обмежень. *Штучний інтелект у правовій практиці: межі та можливості*: матеріали Всеукраїнського круглого столу (м. Львів, 15 березня 2024 р.). Львів:

ЛьвДУВС, 2024. С. 45–49. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/7424/1/15_03_2024.pdf

17. Варинський В. О., Савінова Н. А. Ефективність удосконалення законодавства та штучний інтелект. *Проблеми інформаційного забезпечення та розвитку парламентського контролю в контексті Європейської та Євроатлантичної інтеграції України* : матеріали науково-практичної конференції (м. Київ, 25 квітня 2024 р.). Київ; Одеса : Фенікс, 2024. С. 107–111. URL: https://ippi.org.ua/sites/default/files/konferenciya_25.04.2024.pdf

18. Варинський В. Правосуб'єктність штучного інтелекту: впродовження ідей О. А. Баранова. *Україна в умовах соціальної та цифрової трансформації: шляхи до сталого розвитку та повоєнної відбудови* : матеріали науково-практичної конференції (м. Київ, 22 листопада 2024 р.). ДНУ «Інститут інформації, безпеки і права Національної академії правових наук України». Київ; Одеса : Фенікс, 2024. С. 185–191. URL: https://ippi.org.ua/sites/default/files/ukrayina_v_umovah_socialnoyi_ta_cifrovoyi_transformaciyi_maket.pdf

19. Варинський В. Ризики використання ШІ в правосудді: огляд проблеми. *Трансформаційні процеси правотворчої діяльності та парламентського контролю* : матеріали науково-практичної конференції (м. Київ, 30 жовтня 2025 р.). Київ; Одеса : Фенікс, 2025. С. 97–101. URL: https://ippi.org.ua/sites/default/files/zbirnik_tez_30.10.2025.pdf

20. Варинський В. Основні критерії заборон використання ШІ за AI Act. *Україна в умовах соціальної та цифрової трансформації : теоретичні моделі правового регулювання штучного інтелекту* : матеріали науково-практичної конференції (м. Київ, 5 листопада 2025 р.). Київ; Одеса : Фенікс, 2025. С. 116–120. URL: https://ippi.org.ua/sites/default/files/zbirnik_tez_05.11.2025_1.pdf



НАРОДНИЙ ДЕПУТАТ УКРАЇНИ

вул. М. Грушевського, 5, м. Київ, 01008, www.rada.gov.ua

ДОВІДКА

про використання результатів дисертаційного дослідження

Варинського Владислава Олексійовича, кандидата політичних наук,
доцента кафедри філософії та україністики Національного університету
«Одеська морська академія»

на тему «Правове регулювання обмеження використання штучного інтелекту в
Україні» на здобуття наукового ступеню доктора юридичних наук за
спеціальністю 12.00.07 - адміністративне право і процес;
фінансове право; інформаційне право

Як народний депутат України та голова підкомітету з питань вищої освіти
Комітету Верховної Ради України з питань освіти, науки та інновацій, засвідчую
що Варинський Владислав Олексійович подав на розгляд підготовлену
пропозицію проекту Закону України «Про внесення змін до Закону України «Про
освіту» та Закону України «Про академічну доброчесність» щодо врегулювання
використання технологій штучного інтелекту в освітній та науковій діяльності»
та пояснювальну записку до нього.

Пропозиції, викладені у наданих Варинським В.О. матеріалах, що
ґрунтуються на результатах його докторського дисертаційного дослідження
використовуватимуться мною у подальшій депутатській діяльності для
удосконалення законодавства в сфері правового регулювання безпечного та
доброчесного використання штучного інтелекту в освітянському та науковому
середовищах.

Народний депутат України, голова підкомітету
з питань вищої освіти Комітету Верховної Ради
України з питань освіти, науки та інновацій,
доктор юридичних наук, професор

Юлія ГРИШИНА



САС ВЕРХОВНОЇ РАДИ УКРАЇНИ
Підписувач: Гришина Юлія Миколаївна
Сертифікат: 04A212836405D9904060000F9183100C289E800
Дійсний до: 09.12.2027 0:00:00

Апарат Верховної Ради України
428д9/10-2026/90284 від 22.04.2026



2210144



«ASSOCIATION «METAVERSE-UA»
«Асоціація «METABCECBIT УКРАЇНА»

Office 36, Building 4a, Volodymyr Naumovich St., 03164, Kyiv, Ukraine
<https://association.metaverse-ua.com.ua/> e-mail: association.metaverse.ua@gmail.com

Вих. 140720266-07-14

ДОВІДКА

про впровадження результатів дисертаційного дослідження у діяльність Асоціації
«METAVERSE-UA» та в науково-академічну дослідницьку систему національного права
Варинського Владислава Олексійовича на тему

«Теоретико-методологічні та правові засади використання штучного інтелекту в Україні»
на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 – адміністративне
право і процес; фінансове право; інформаційне право

Асоціація «METAVERSE-UA» цим засвідчує, що результати докторського дисертаційного дослідження Варинського Владислава Олексійовича на тему «Теоретико-методологічні та правові засади використання штучного інтелекту в Україні», виконаного на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право, взяті до уваги та впроваджені у діяльність Асоціації, а також рекомендовані до використання в ширшій науково-академічній дослідницькій системі національного права України.

Актуальність теми дисертаційного дослідження зумовлена стрімким розвитком технологій штучного інтелекту, які глибоко трансформують суспільні відносини, економіку, публічне управління та систему права і потребують адекватного, науково обґрунтованого нормативного реагування держави. В умовах активного формування наднаціонального регулювання (Регламент ЄС про штучний інтелект (AI Act), відповідні ініціативи ОЕСР, ЮНЕСКО, Ради Європи) та за відсутності системного, доктринально виваженого законодавства про штучний інтелект в Україні дослідження В. О. Варинського є своєчасним і практично затребуваним.

Наукова новизна роботи полягає у розробці цілісної теоретико-методологічної концепції правового регулювання штучного інтелекту, що поєднує положення адміністративного, фінансового та інформаційного права. Практична цінність дисертаційного дослідження полягає у розробленому автором комплексі пропозицій до законодавства України, придатних для безпосереднього використання у нормопроєктувальній діяльності, зокрема під час підготовки Асоціацією експертних висновків, науково-консультативних матеріалів та пропозицій до проектів нормативно-правових актів у сфері штучного інтелекту, віртуальних світів та інноваційних цифрових технологій.

Необхідність дослідження обумовлена перебуванням України на етапі докорінної цифрової трансформації суспільства та держави та повноцінної інтеграції до європейського цифрового простору. Відсутність системного наукового доробку в цій сфері створює ризик законодавчого відставання України від глобальних регуляторних процесів, що робить дисертаційне дослідження В. О. Варинського вагомим внеском у розбудову національної правової системи на цьому історичному етапі.

Результати дисертаційного дослідження Варинського Владислава Олексійовича використовуються Асоціацією «METAVERSE-UA» у поточній науково-експертній діяльності та рекомендуються до подальшого використання науковими установами, органами державної влади та закладами вищої освіти України, що здійснюють дослідження у сфері правового регулювання штучного інтелекту.

Олексій Костенко

Президент Association «ASSOCIATION «METAVERSE-UA», Phd, старший дослідник офіційний член міжнародної Робочої групи з нагляду за етикою штучного інтелекту, що входить до складу Комітету зі стандартів штучного інтелекту (C/AISC) Асоціації стандартів Інституту інженерів з електротехніки та електроніки (IEEE SA), головний редактор канадського наукового електронного журналу «Contemporary Issues in Artificial Intelligence»



Yrii Yekhanurov

Заступник «ASSOCIATION «METAVERSE-UA», Phd, професор, Прем'єр-міністр України

ЗАТВЕРДЖУЮ

Проректор Одеського державного
університету внутрішніх справ

Владим ПІДГОРОДИНСЬКИЙ

15 07 2026 р.

АКТ

**впровадження в наукову діяльність Одеського державного
університету внутрішніх справ результатів дисертаційного дослідження
Варинського Владислава Олексійовича на тему «Теоретико-
методологічні та правові засади використання штучного інтелекту
в Україні»**

15 07 2026

м. Одеса

Комісія у складі:

- 1) начальника відділу організації наукової діяльності ОДУВС, кандидата юридичних наук, доцента Доброван Наталії;
- 2) ученого секретаря секретаріату Вченої ради ОДУВС, кандидата педагогічних наук, доцента Ісаснка Максима;
- 3) начальника відділу аспірантури (ад'юнктури) і докторантури ОДУВС, кандидата юридичних наук Теслюк Ірини

склала цей акт про те, що комісією вивчені наукові положення, пропозиції і рекомендації Варинського Владислава Олексійовича щодо впровадження результатів дисертаційного дослідження на тему «Теоретико-методологічні та правові засади використання штучного інтелекту в Україні» підготовленого на здобуття наукового ступеня доктора юридичних наук зі спеціальності 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право у науково-дослідну діяльність Одеського державного університету внутрішніх справ МВС України при виконанні НДР за темою «Пріоритетні напрями реформування правоохоронних органів в умовах розвитку демократичних процесів у державі» (реєстраційний номер 0123U103538) та за темою кафедри адміністративно-правових дисциплін «Забезпечення адміністративно-правовими засобами прав і свобод людини і громадянина в Україні» (реєстраційний номер 0125U001209).

Ці результати висвітлено у таких наукових працях автора:

1. Варинський В. Штучний інтелект в освіті: проблеми впровадження та регулювання. *Створювальна сила знання* : монографія. Книга друга / авт. кол. ; відп. ред.: І. А. Доннікова, Н. В. Кривцова. Київ : 7БЦ, 2025. С. 145–163.
2. Варинський В. О. Сучасні напрямки соціально-правових досліджень штучного інтелекту. *Наукові перспективи*. 2022. №. 12 (30). С. 299–310.
3. Варинський В. О. Правосуб'єктність штучного інтелекту: міф чи реальність. *Юридична Україна*. 2024. № 11. С. 60–68.
4. Варинський В. О. Правосуб'єктність штучного інтелекту: критичний погляд на автономність. *Інформація і право*. 2024. № 4 (51). С. 83–94.
5. Варинський В. О. Стан правового регулювання використання штучного інтелекту у законодавстві України. *Юридична Україна*. 2025. № 1. С. 40–50.
6. Варинський В. О. Соціально-правові чинники формування довіри до штучного інтелекту (Частина 1). *Право і суспільство*. 2025. № 6. С. 524–532.
7. Варинський В. О. Основні підходи правового регулювання використання штучного інтелекту в освіті. *Актуальні проблеми вдосконалення чинного законодавства України*. 2025. № 69. С. 140–151.
8. Варинський В. Алгоритмічне забезпечення охорони громадського порядку : правові межі застосування штучного інтелекту у діяльності правоохоронних органів. *Академічні візії*. 2025. № 48. С. 1–11.
9. Варинський В. О. Правова парадигма довіри до штучного інтелекту (Частина II). *Право і суспільство*. 2026. № 1. С. 258–264
10. Варинський В. О. Етичні та правові ризики застосування штучного інтелекту у правоохоронній діяльності та діяльності спецслужб. *Вісник Пенітенціарної асоціації України*. 2026. №1 (35). С. 245–256.
11. Варинський В. О. AI Act як ризик-орієнтована модель правового

обмеження застосування штучного інтелекту у правоохоронній діяльності та діяльності спецслужб. *Південноукраїнський правничий часопис*. 2026. № 1. С. 134–141.

12. Варинський В. Правове регулювання обмеження використання штучного інтелекту в медицині: основні міжнародні підходи. *Український часопис міжнародного права*. 2026. № 1. С. 21–33.

13. Варинський В. О. Оцінка впливу високоризикових систем штучного інтелекту на права людини як інструмент правової політики України. *Академічні візії*. Вип 55. 2026.

14. Varynskyi V., Varynska A., Kostytsky M., Kushakova-Kostytska N. Information security and information hygiene on internet media. *Nexo Revista Científica*. 2021. Vol. 34. № 1. P. 120–128.

15. Varynskyi V., Shelever N., Yankovyi M., Pylyp V., Antalovtsi O., Halahan O. Use of the “electronic court” service as a means of citizens' access to the judiciary. *Lex Humana*. 2023. Vol. 16. № 1. P. 249–266.

16. Rudenko O., Rafalskyi I., Yermak O., Varynskyi V., Konoplia Y. *The potential and prospects of artificial intelligence use in strategic planning: issues of security and defense. AD ALTA: Journal of Interdisciplinary Research*. 2024. Vol. 14/02-XLIV. P. 6–12.

17. Rudenko O., Zaika O., Varynskyi V., Kulchii I., Myroshnychenko A. Digitization of local self-government based on the use of artificial intelligence in the context of sustainable development. *Edelweiss Applied Science and Technology*. 2024. Vol. 8. № 6. P. 1467–1480.

18. Varynskyi V. Health-saving technologies in the context of globalization. *International Journal of Recent Technology and Engineering (IJRTE)*. 2019. Vol. 8. Issue 4S. P. 63–67.

19. Varynskyi V., Donnikova I., Savinova N. Artificial intelligence in education: tool, object, «subject» of learning. *Journal of International Legal Communication*. 2023. Vol. 10. № 3. P. 46–55.

20. Shelever N., Varynskyi V., Burdonosova M., Rogach O., Pylyp V. Electronic means of ensuring fair justice: contemporary and development prospects.

Lex Humana. 2024. Vol. 16 № 1. P. 557–572.

На основі проведеного аналізу комісія дійшла висновку, що подані матеріали мають належний теоретичний та методологічний рівень, містять концептуальні положення, науково обґрунтовані висновки та рекомендації, спрямовані на вдосконалення адміністративно-правового та інформаційно-правового регулювання використання технологій штучного інтелекту в Україні, насамперед у сферах правоохоронної діяльності, правосуддя, освіти і науки, охорони здоров'я, а також інших сферах із підвищеним рівнем ризику для прав людини, і становлять наукову цінність в умовах цифрової трансформації держави та суспільства.

Результати дисертаційного дослідження Варинського Владислава Олексійовича на тему «Теоретико-методологічні та правові засади використання штучного інтелекту в Україні» впроваджено у наукову діяльність Одеського державного університету внутрішніх справ, зокрема при виконанні НДР «Пріоритетні напрями реформування правоохоронних органів в умовах розвитку демократичних процесів у державі» (реєстраційний номер 0123U103538) та «Інформаційні технології: сучасний стан, особливості в умовах війни та післявоєнний період» (реєстраційний номер 0123U103748).

Члени комісії:

Заступник начальника відділу
організації наукової діяльності ОДУВС
кандидат юридичних наук, доцент
підполковник поліції



Наталія ДОБРОВАН

Учений секретар секретаріату
Вченої ради ОДУВС
кандидат педагогічних наук, доцент



Максим ІСАЄНКО

Начальник відділу аспірантури
(ад'юнктури) і докторантури ОДУВС
кандидат юридичних наук



Ірини ТЕСЛЮК

ЗАТВЕРДЖУЮ

Проректор Одеського державного
університету внутрішніх справ



Вадим ПІДГОРОДИНСЬКИЙ

В *07* 2026 р.

АКТ

**впровадження в освітній процес Одеського державного університету
внутрішніх справ результатів дисертаційного дослідження Варинського
Владислава Олексійовича на тему «Теоретико-методологічні та правові
засади використання штучного інтелекту в Україні»**

В *07* 2026 р.

м. Одеса

Комісія у складі:

- 1) начальника відділу забезпечення якості освіти кандидата історичних наук, доцента Камінської Олени;
- 2) директора інституту права та безпеки ОДУВС, кандидата юридичних наук, доцента Дришлюка Володимира;
- 3) завідувача кафедри цивільно-правових дисциплін інституту права та безпеки ОДУВС, кандидата юридичних наук, професора Маковія Віктора

склала цей акт про те, що нею були проаналізовані основні наукові положення, висновки та практичні рекомендації дисертаційного дослідження Варинського Владислава Олексійовича зі спеціальності 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право на тему «Теоретико-методологічні та правові засади використання штучного інтелекту в Україні» з метою їх впровадження в освітній процес Одеського державного університету внутрішніх справ. Ці результати висвітлено у таких наукових працях автора:

1. Варинський В. Штучний інтелект в освіті: проблеми впровадження та регулювання. *Створювальна сила знання* : монографія. Книга друга / авт. кол. ; відп. ред.: І. А. Доннікова, Н. В. Кривцова. Київ : 7БЦ, 2025. С. 145–163.

2. Варинський В. О. Сучасні напрямки соціально-правових досліджень штучного інтелекту. *Наукові перспективи*. 2022. № 12 (30). С. 299–310.
3. Варинський В. О. Правосуб'єктність штучного інтелекту: міф чи реальність. *Юридична Україна*. 2024. № 11. С. 60–68.
4. Варинський В. О. Правосуб'єктність штучного інтелекту: критичний погляд на автономність. *Інформація і право*. 2024. № 4 (51). С. 83–94.
5. Варинський В. О. Стан правового регулювання використання штучного інтелекту у законодавстві України. *Юридична Україна*. 2025. № 1. С. 40–50.
6. Варинський В. О. Соціально-правові чинники формування довіри до штучного інтелекту (Частина 1). *Право і суспільство*. 2025. № 6. С. 524–532.
7. Варинський В. О. Основні підходи правового регулювання використання штучного інтелекту в освіті. *Актуальні проблеми вдосконалення чинного законодавства України*. 2025. № 69. С. 140–151.
8. Варинський В. Алгоритмічне забезпечення охорони громадського порядку : правові межі застосування штучного інтелекту у діяльності правоохоронних органів. *Академічні візії*. 2025. № 48. С. 1–11.
9. Варинський В. О. Правова парадигма довіри до штучного інтелекту (Частина II). *Право і суспільство*. 2026. № 1. С. 258–264.
10. Варинський В. О. Етичні та правові ризики застосування штучного інтелекту у правоохоронній діяльності та діяльності спецслужб. *Вісник Пенітенціарної асоціації України*. 2026. №1 (35). С. 245–256.
11. Варинський В. О. AI Act як ризик-орієнтована модель правового обмеження застосування штучного інтелекту у правоохоронній діяльності та діяльності спецслужб. *Південноукраїнський правничий часопис*. 2026. № 1. С. 134–141.

12. Варинський В. Правове регулювання обмеження використання штучного інтелекту в медицині: основні міжнародні підходи. *Український часопис міжнародного права*. 2026. № 1. С. 21–33.
13. Варинський В. О. Оцінка впливу високоризикових систем штучного інтелекту на права людини як інструмент правової політики України. *Академічні візії*. Вип 55. 2026.
14. Varynskyi V., Varynska A., Kostytsky M., Kushakova-Kostytska N. Information security and information hygiene on internet media. *Nexo Revista Cientifica*. 2021. Vol. 34. № 1. P. 120–128.
15. Varynskyi V., Shelever N., Yankovyi M., Pylyp V., Antalovtsi O., Halahan O. Use of the “electronic court” service as a means of citizens' access to the judiciary. *Lex Humana*. 2023. Vol. 16. № 1. P. 249–266.
16. Rudenko O., Rafalskyi I., Yermak O., Varynskyi V., Konoplia Y. *The potential and prospects of artificial intelligence use in strategic planning: issues of security and defense. AD ALTA: Journal of Interdisciplinary Research*. 2024. Vol. 14/02-XLIV. P. 6–12.
17. Rudenko O., Zaika O., Varynskyi V., Kulchii I., Myroshnychenko A. Digitization of local self-government based on the use of artificial intelligence in the context of sustainable development. *Edelweiss Applied Science and Technology*. 2024. Vol. 8. № 6. P. 1467–1480.
18. Varynskyi V. Health-saving technologies in the context of globalization. *International Journal of Recent Technology and Engineering (IJRTE)*. 2019. Vol. 8. Issue 4S. P. 63–67.
19. Varynskyi V., Donnikova I., Savinova N. Artificial intelligence in education: tool, object, «subject» of learning. *Journal of International Legal Communication*. 2023. Vol. 10. № 3. P. 46–55.
20. Shelever N., Varynskyi V., Burdonosova M., Rogach O., Pylyp V. Electronic means of ensuring fair justice: contemporary and development prospects. *Lex Humana*. 2024. Vol. 16 № 1. P. 557–572.

Комісія дійшла висновку, що результати дисертаційного дослідження, викладені у зазначених наукових працях Варинського Владислава

Олексійовича мають теоретичне, методологічне та практичне значення, відповідають сучасним напрямкам розвитку юридичної науки і можуть бути ефективно використані в освітньому процесі. Основні наукові положення, висновки та практичні рекомендації дисертаційного дослідження впроваджено в освітній процес Одеського державного університету внутрішніх справ, зокрема при викладанні навчальних дисциплін «Кримінальний аналіз», «Пошук інформації з відкритих джерел (osint) працівниками кримінальної поліції», «Протидія кіберзлочинності» для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю «Правоохоронна діяльність», «Інформаційна та кібернетична безпека» для здобувачів другого (магістерського) рівня вищої освіти за спеціальністю «Системний аналіз», розроблення освітніх програм, навчально-методичного забезпечення, а також у науково-дослідній роботі здобувачів вищої освіти.

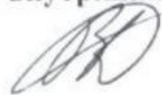
Члени комісії:

Начальник відділу
забезпечення якості освіти
кандидат історичних наук, доцент



Олена КАМІНСЬКА

Директор інституту права та безпеки
Одеського державного університету внутрішніх справ
кандидат юридичних наук, доцент



Володимир ДРИШЛЮК

Т.в.о. завідувача кафедри кримінального аналізу
та інформаційних технологій
Одеського державного університету внутрішніх справ
кандидат юридичних наук, професор



Володимир КАЛУГІН

ДОДАТОК Г

**Анкета опитування
українських нефармових респондентів
«Очікування від впровадження штучного інтелекту»**

(анонімне опитування проводилось протягом травня 2023 - червня 2025 р., за допомогою розповсюдження гул-форми опитування серед різних сфер та верств населення, всього опитано 1092 респондента)

1. Ваш вік	
Вибрати один з варіантів	14-21
	22-30
	31-40
	41-50
	51-60
	61-70
	71+

2. Місце Вашого постійного проживання	
Вибрати один з варіантів	місто з населенням понад 1.000.000
	місто з населенням від 500.000 до 1.000.000
	місто з населенням від 100.000 до 500.000
	населений пункт з населенням від 20.000 до 100.000
	населений пункт з населенням від 5.000 до 20.000
	населений пункт з населенням до 5.000

3. Ваша освіта	
Вибрати один з варіантів	неповна середня
	повна середня
	неповна вища (студент або бакалавр)
	повна вища (спеціаліст, магістр)
	PhD кандидат наук
	доктор наук

4. Чи викликає у Вас опасіння впровадження штучного інтелекту в життєдіяльність людства?	
Вибрати один з варіантів	так
	ні
	складно відповісти

5. У чому Ви вбачаєте переваги впровадження штучного інтелекту в життєдіяльність людства?

Розгорнута відповідь

6. Які небезпеки Ви відчуваєте у впровадженні штучного інтелекту в життєдіяльність людства?

Розгорнута відповідь

7. Які сфери для впровадження штучного інтелекту Ви вважаєте найбільш придатними?

Вибрати кілька варіантів з наданого списку

Освіта і наука
Медицина та ветеринарія
Медійна сфера та реклама
Екологія
Політика
Воєнна сфера у т.ч. розробка зброї
Аграрна сфера
ІТ-сфера
Транспорт
Державне управління
Міське самоврядування
Правоохоронна діяльність
Правосуддя
Торгівля
Інше

8. Які сфери для впровадження штучного інтелекту Ви вважаєте недопустимими?

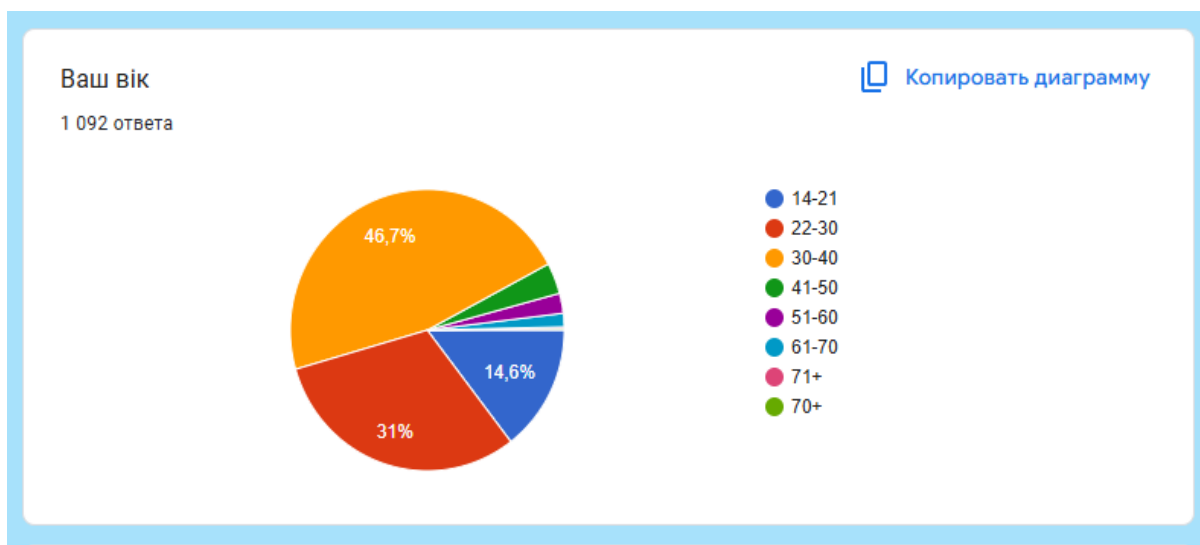
Вибрати кілька варіантів з наданого списку

Освіта і наука
Медицина та ветеринарія
Медійна сфера та реклама
Екологія
Політика
Воєнна сфера у т.ч. розробка зброї
Аграрна сфера
ІТ-сфера
Транспорт
Державне управління
Міське самоврядування
Правоохоронна діяльність
Правосуддя
Торгівля
Інше

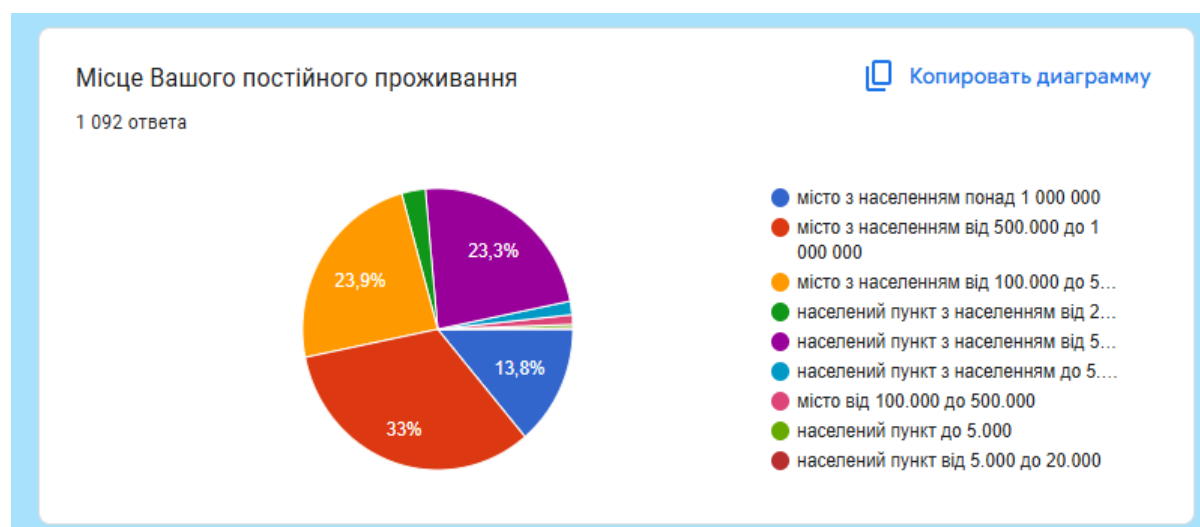
Результати опитування

Соціально-демографічна характеристика респондентів

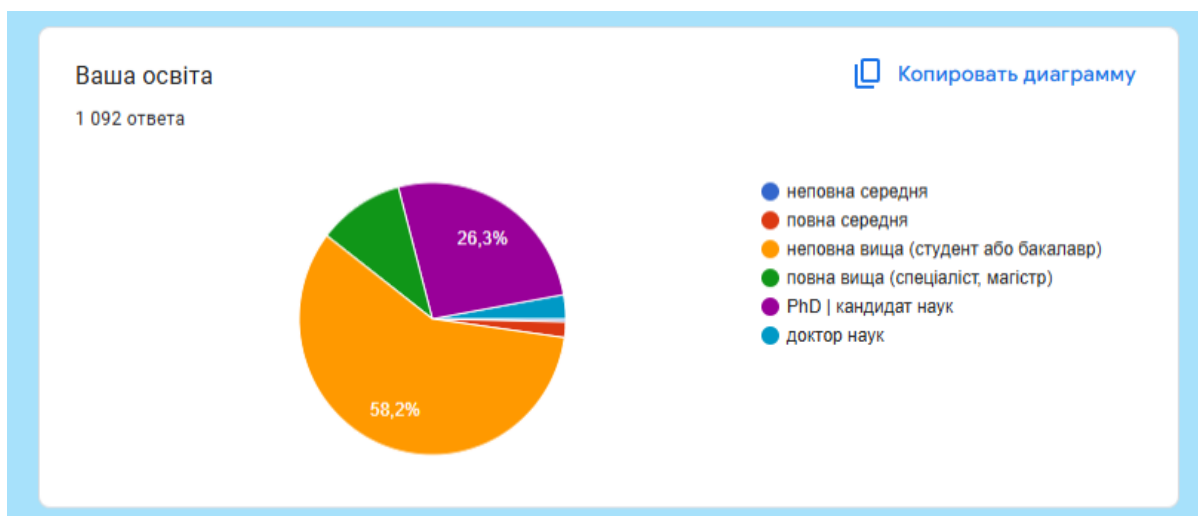
Діаграма 1. Вік респондентів



Діаграма 2. Тип населеного пункту проживання респондентів
(за чисельністю населення)

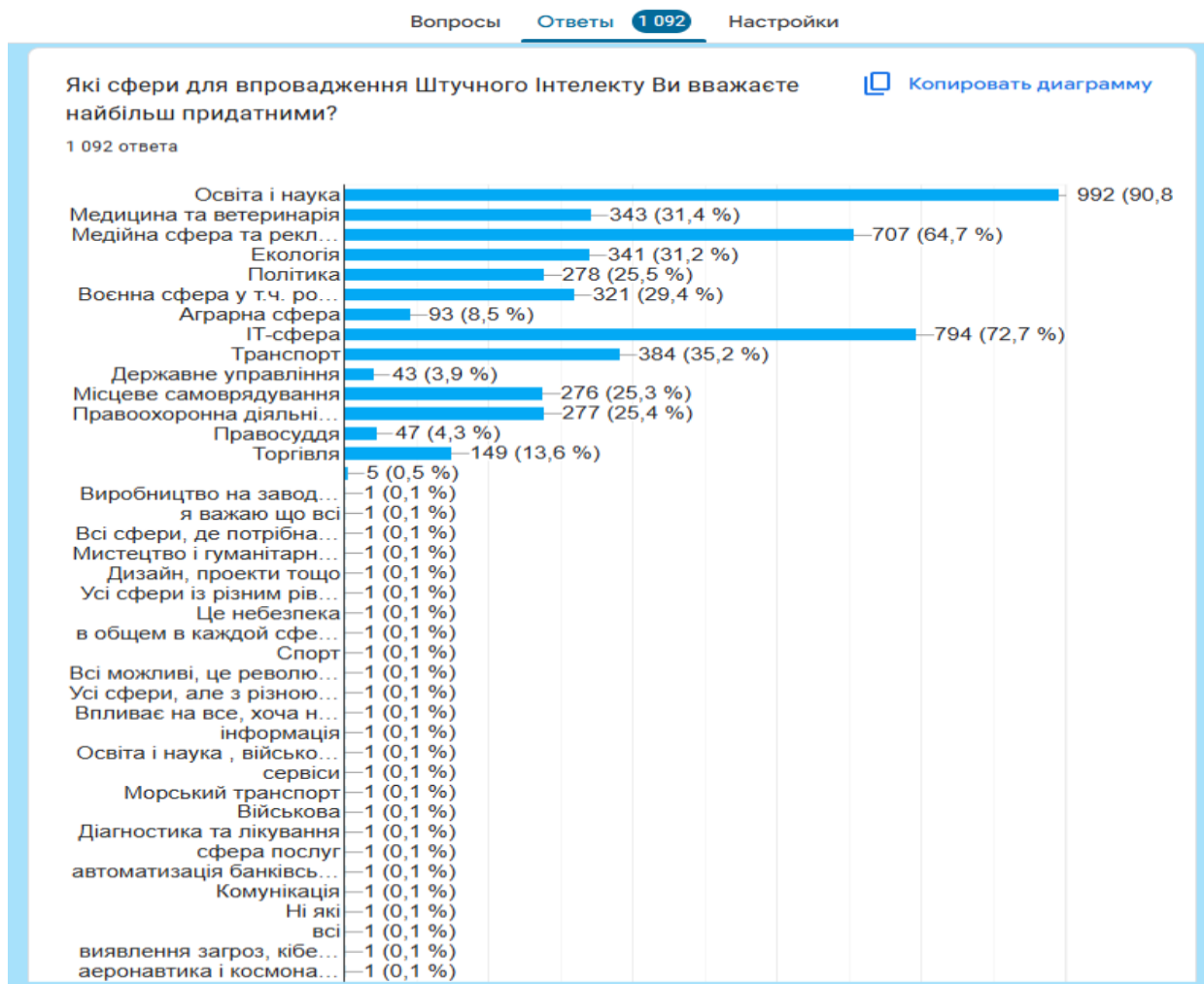


Діаграма 3. Освіта респондентів



Результати опитування
«Очікування від впровадження штучного інтелекту»

Діаграма 4. Рейтинг сфер за рівнем підтримки впровадження штучного інтелекту

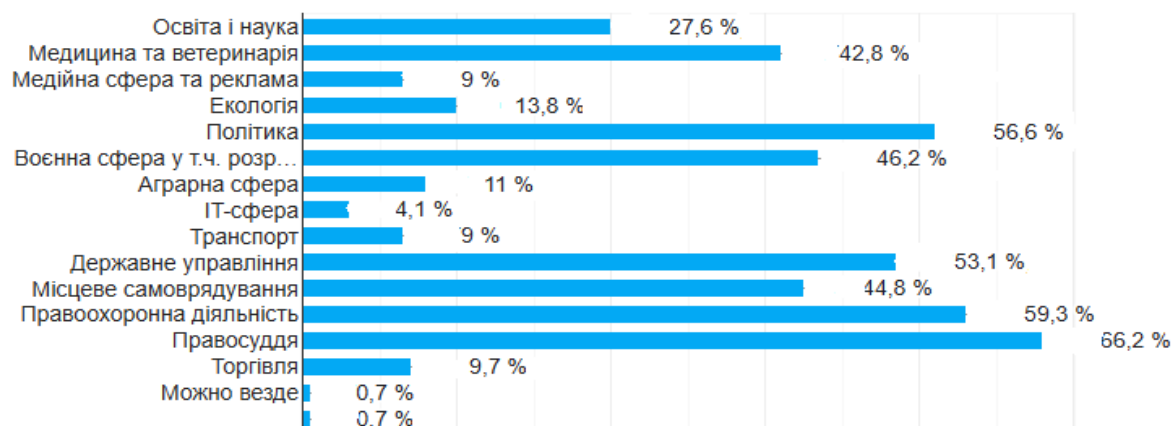


Діаграма 5. Опасіння щодо впровадження штучного інтелекту



Діаграма 6. Рейтинг сфер за рівнем неприйнятності впровадження штучного інтелекту

Які сфери для впровадження Штучного Інтелекту Ви вважаєте недопустимими?



Результати опитування населення за типами населених пунктів

Аналіз даних з таблиці відповідей результатів опитування «Очікування від впровадження штучного інтелекту» (Додаток 2) здійснювався з використання системи штучного інтелекту *Perplexity.Pro*

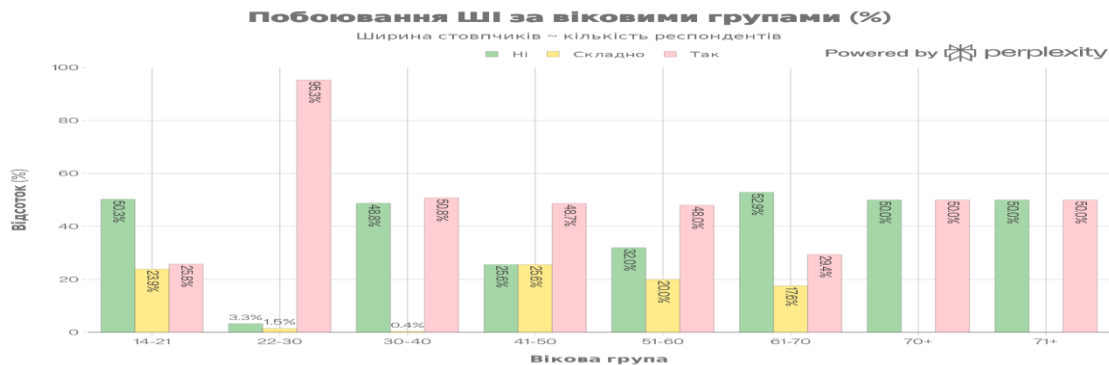
Таблиця 1. Кількісний показник побоювань за чисельністю населення

Кількість населення	% "Так" (побоювання)	Кількість респондентів
Понад 1 млн	33.8%	151
500 тис.–1 млн	90.0%	360
100–500 тис.	95.0%	261
5–20 тис.	1.2%	254
До 5 тис.	41.2%	17

Діаграма 7. Кількісний показник побоювань за чисельністю населення



Діаграма 8. Побоювання впровадження ШІ різними віковими групами (% та кількості)



Таблиця 2. Таблиця побоювань впровадження ШІ різними віковими групами (% та кількості)

Вікова група	% Позитивно	% Складно	% Негативно	Всього респондентів
14-21	50.3%	23.9%	25.8%	159

Вікова група	% Позитивно	% Складно	% Негативно	Всього респондентів
22-30	3.3%	1.5%	95.3%	338
30-40	48.8%	0.4%	50.8%	510
41-50	25.6%	25.6%	48.7%	39
51-60	32.0%	20.0%	48.0%	25
61-70	52.9%	17.6%	29.4%	17
70+	50.0%	0.0%	50.0%	2
71+	50.0%	0.0%	50.0%	2

Таблиця 3. Типи побоювань через впровадження ШІ за типами населених пунктів

Населений пункт (% "Так")	Топ-страхи (найчастіші слова/теми)
500 тис.–1 млн (90%)	втрата робочих місць (307), зловживань технологією (304)
100–500 тис. (95%)	можливість зловживань технологією (244), технологічна залежність
20–100 тис. (58%)	втрата робочих місць (13), етики/приватності (13)
До 5 тис. (41%)	зменшення зайнятості людей люди (6), вірогідність втратить контроль
Понад 1 млн (34%)	може контролювати людство (7-5), використання
5–20 тис. (1%)	Заміна професій / зниження інтелекту (2)

Деталізація результатів опитування
«Очікування від впровадження штучного інтелекту у різних сферах
використання»

Таблиця 4. Ставлення респондентів до ШІ за сферами використання

Сфера використання	Придатні (ранг/згадки)	Недопустимі (ранг/згадки)	Різниця (придатні - недопустимі)
Освіта і наука	1 (993)	2 (622)	+371 (консенсус: часто обидві)
ІТ-сфера	2 (794)	14 (15)	+779 (найбезпечніша)
Медійна сфера та реклама	3 (707)	5 (271)	+436
Транспорт	4 (385)	13 (36)	+349
Медицина та ветеринарія	5 (343)	1 (676)	- 333
Екологія	6 (341)	11 (55)	+286
Воєнна сфера (зброя)	7 (321)	4 (379)	-58
Правоохоронна діяльність	8 (278)	9 (171)	+107
Політика	9 (278)	8 (185)	+93
Міське самоврядування	10 (276)	10 (126)	+150
Торгівля	11 (149)	12 (40)	+109
Аграрна сфера	12 (93)	6 (268)	-175
Правосуддя	13 (47)	7 (194)	-147
Державне управління	14 (43)	3 (401)	-358

Таблиця 5. Типи побоювань впровадження ІІІ реципієнтами вікової групи 14-21

Блок	% від 41	Кількість	Приклади (унікальні)
Деградація інтелекту/навичок	43.9%	18	«Люди стануть менше інтелектуальними»; «Зменшення розумової діяльності»
Заміна праці/діяльності	29.3%	12	«Зменшення професій, безробіття»; «Заміна людської діяльності»
Залежність/контроль	26.8%	11	«Контроль з боку влади»; «ІІІ втратить контроль»

Таблиця 6. Типи побоювань впровадження ІІІ реципієнтами вікової групи 22-30 р.

Блок	% від 322	Кількість відповідей	Примітка
Заміна праці	98.4%	317	Домінує «Втрата робочих місць...»
Зловживання/контроль	0.9%	3	Рідкісні «етика/приватність»
Деградація/соціум	0.6%	2	«Деградація людства»
Самостійність ІІІ	0.0%	0	Відсутні

Таблиця 7. Типи побоювань впровадження ІІІ реципієнтами вікової групи 31-40

Блок	% від 259	Кількість відповідей	Примітка

Блок	% від 259	Кількість відповідей	Примітка
Зловживання/контроль	95.0%	246	Домінує шаблон «можливість зловживань технологією»
Заміна праці	1.9%	5	«Заміна людської праці» тощо
Самостійність ШІ	1.2%	3	«ШІ може жити самостійно»
Деградація/соціум	0.8%	2	«Зниження когнітивних здібностей»
Інше/не класифіковано	~1.1%	~3	Різні/пусті

Таблиця 8. Типи побоювань впровадження ШІ реципієнтами вікової групи 41-50

Блок	% від 19	Кількість	Приклади (унікальні)
Контроль/свобода	26,3	5	«Тотальний контроль»; «Зменшення свободи»; «Повний контроль та управління...»
Деградація/знищення	21.1%	4	«Знищення людства»; «Деградація»; «Небезпека в зменшенні людства»
Заміна праці	15.8%	3	«Замінить роботу людей»; «Від може стати заміною...»
Вихід/збої	10.5%	2	«Вихід з під контролю, помилки ШІ»; «Можливі неконтрольовані збої»
Не класифіковано	26.3%	5	«Штучний інтелект не може витіснити...» (парадокс); «Це небезпека для людства...»

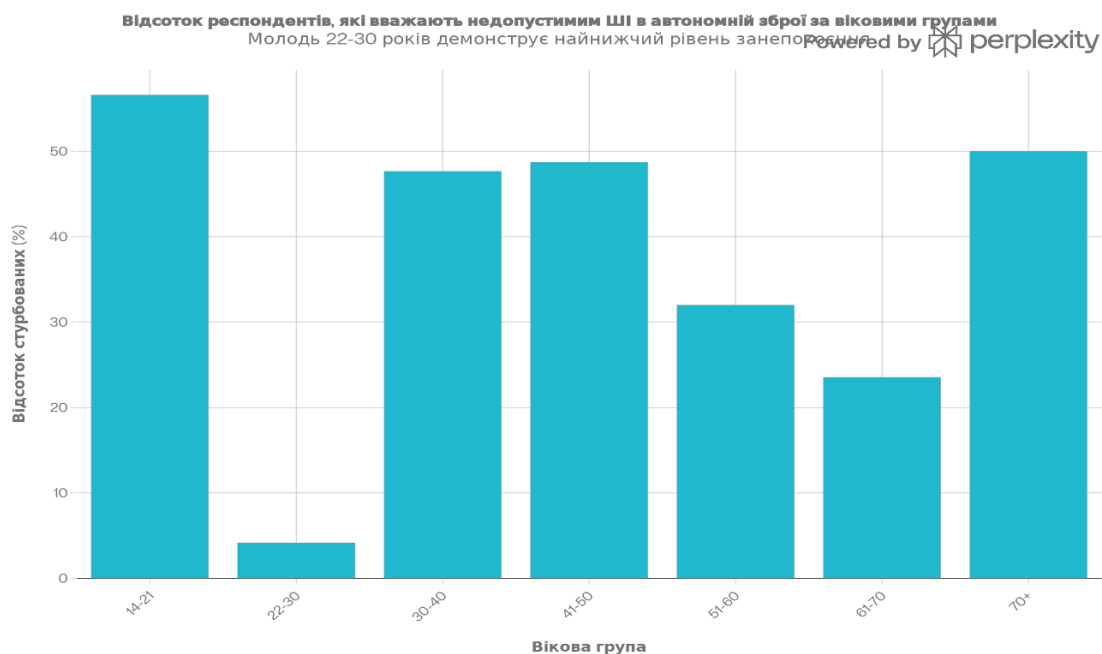
Таблиця 9. Типи побоювань впровадження ІІІ реципієнтами вікової групи 51-60

Блок	% від 12	Кількість	Приклади (унікальні)
Втрата контролю	33.3%	4	«ІІІ вийде з під контролю»; «Вихід за межі контролю...»
Маніпуляція/пропаганда	16.7%	2	«Полегшення деструктивних впливів... пропагандистських наративів»; «Маніпулювання свідомістю»
Дегуманізація/потенціал	25.0%	3	«Відмова користуватися власним інтелектом»; «Людський потенціал знецінюється»
Загроза існуванню	16.7%	2	«Неможливі умови існування людства»; «Конкуренція»

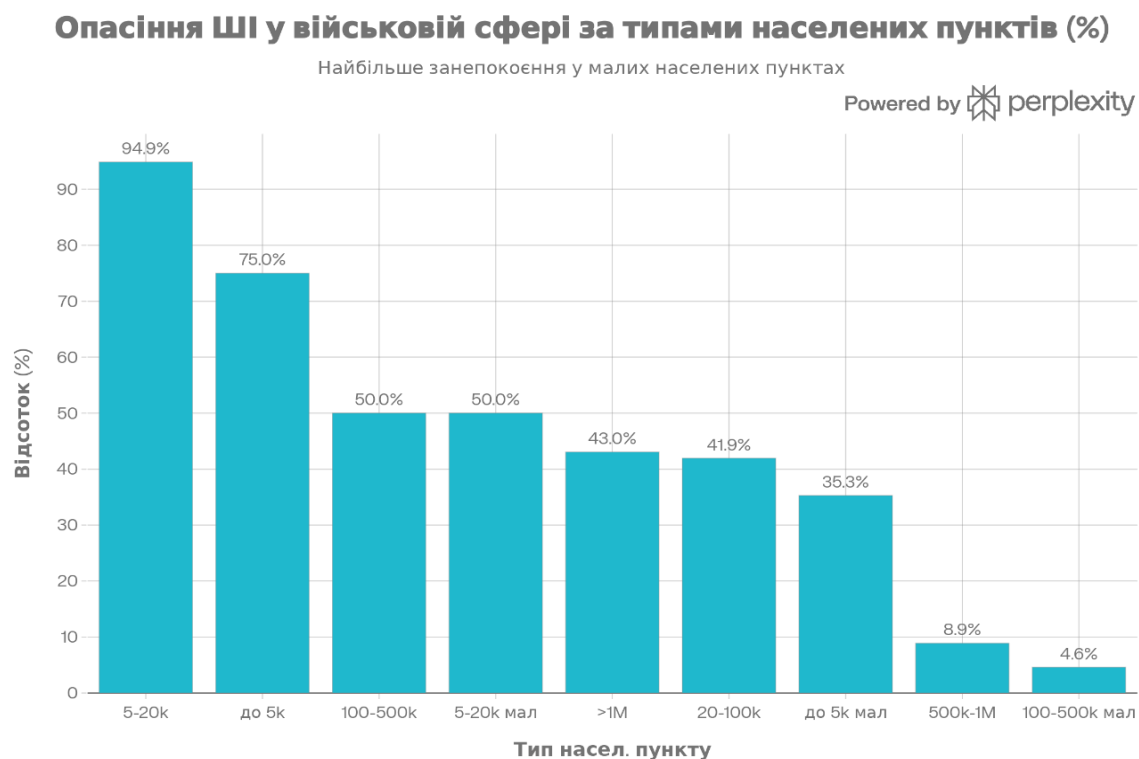
Таблиця 10. Типи побоювань впровадження ІІІ реципієнтами вікової групи 61-70

Блок	% від 5	Кількість	Приклади (унікальні)
Втрата контролю/безробіття	40.0%	2	«Втрата контролю»; «Збільшення безробіття... вийти з під контролю»
Шаблонні/етика/зловживання	20.0%	1	«Втрата робочих місць, питання етики, зловживань технологією»
Деградація/невідомість	40.0%	2	«Інтелектуальна деградація»

Результати опасінь респондентів за сферами використання ІІІ
Діаграма 9. Перестороги щодо використання ІІІ в військовій сфері за віковими групами



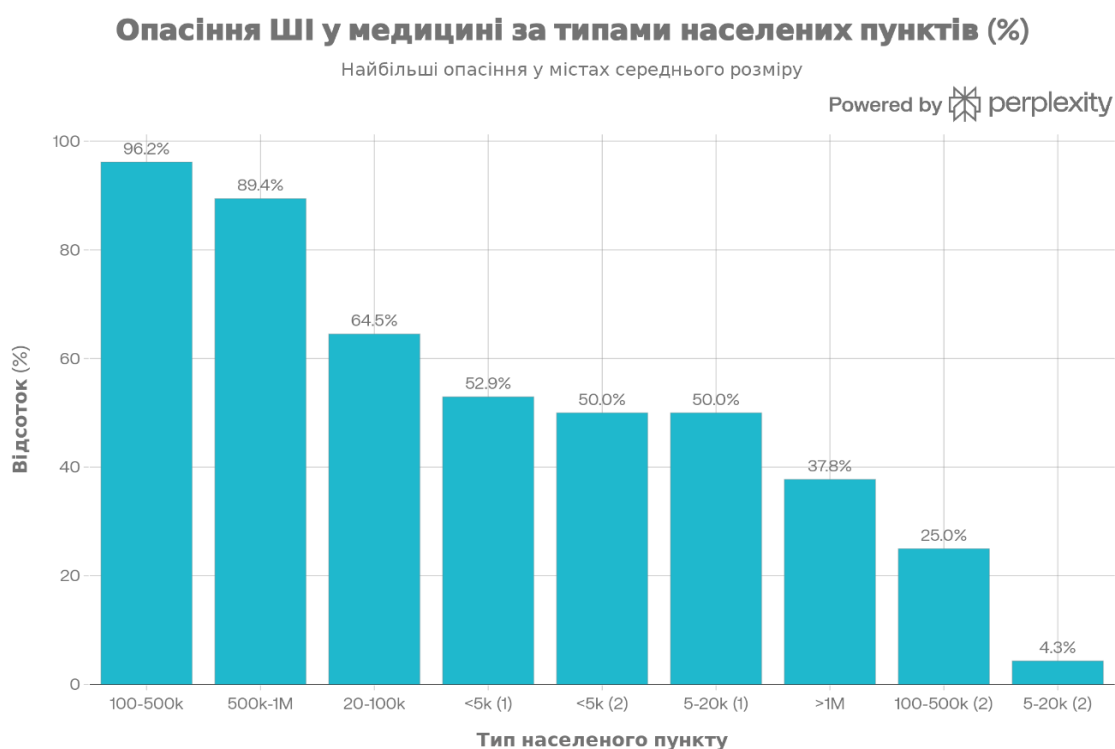
Діаграма 10. Перестороги щодо використання ШІ в військовій сфері за типами населених пунктів



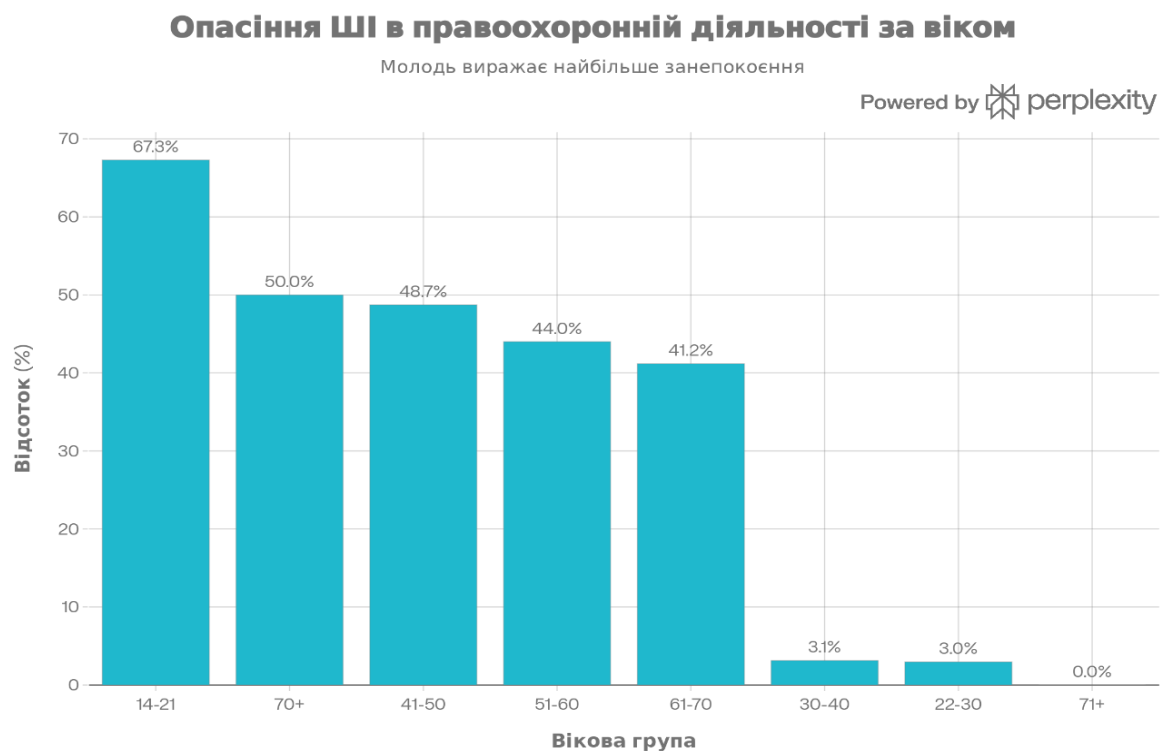
Діаграма 11. Перестороги щодо використання ШІ в медицині за віковими групами



Діаграма 12. Перестороги щодо використання ШІ в медицині за типами населених пунктів

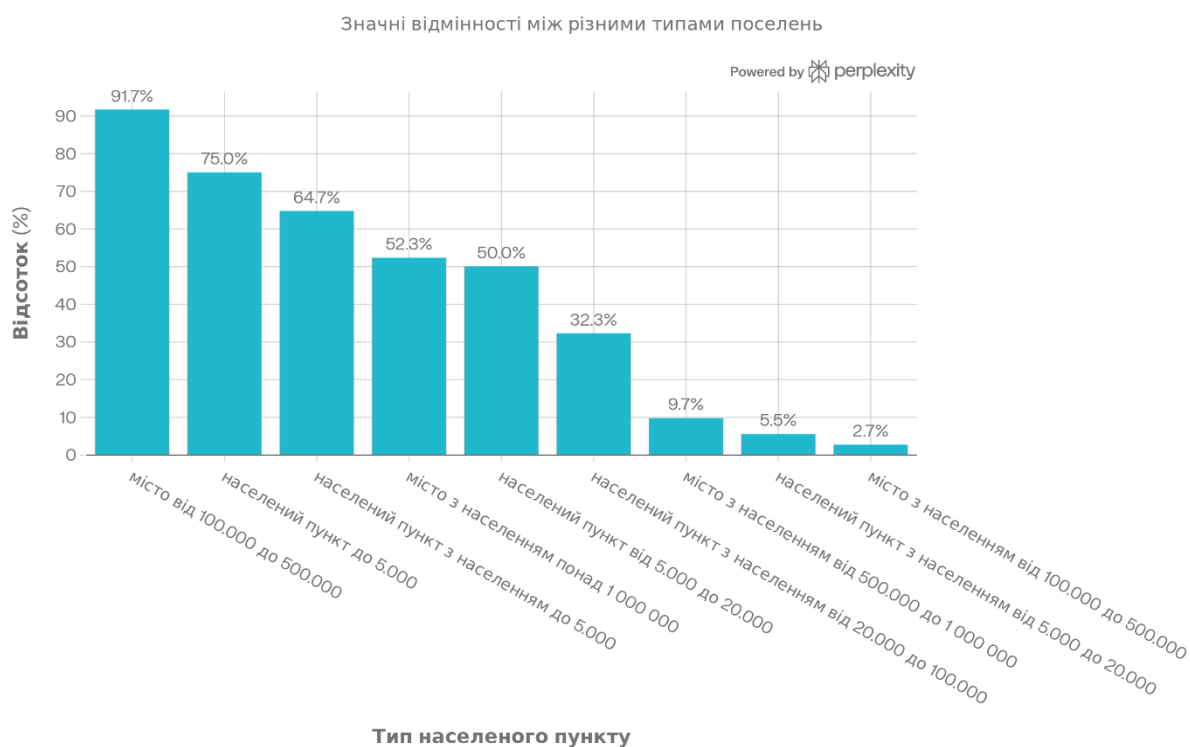


Діаграма 13. Перестороги щодо використання ШІ в правоохоронній діяльності за віковими групами



Діаграма 14. Перестороги щодо використання ШІ в правоохоронній діяльності за типами населених пунктів

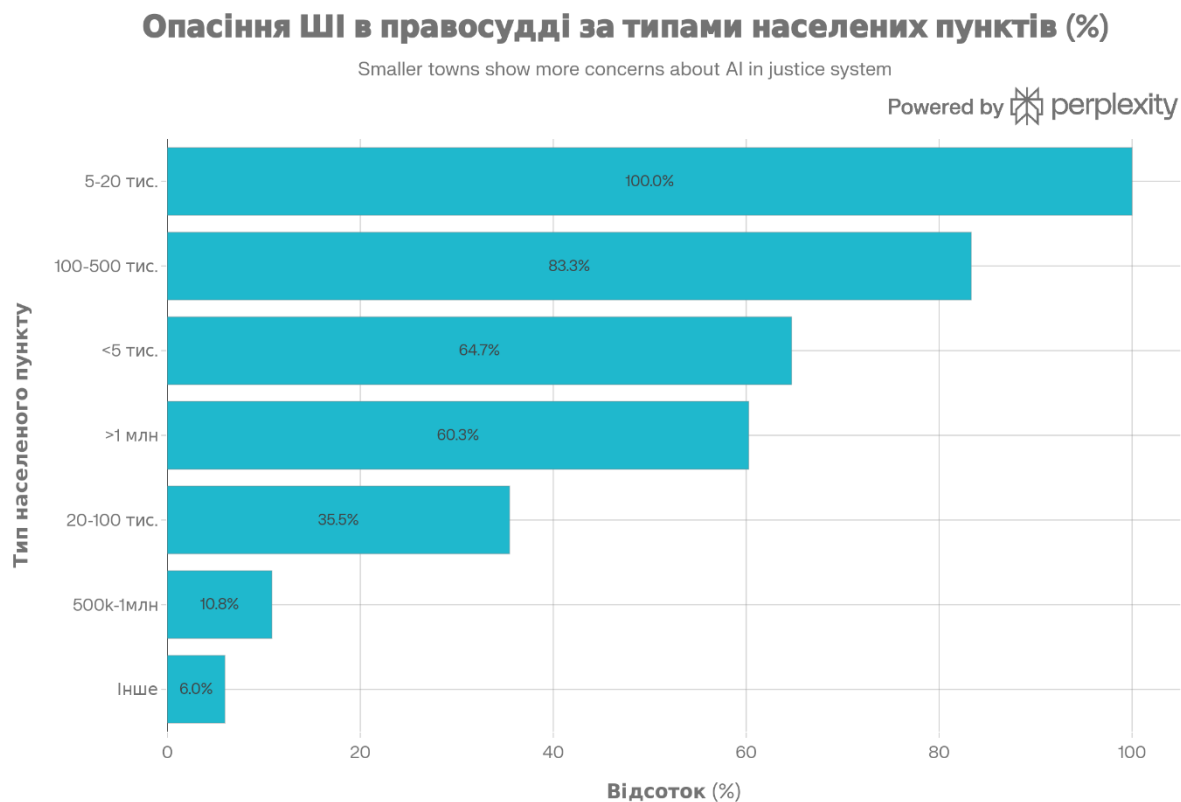
Опасіння ШІ у правоохоронній діяльності за типами населених пунктів (%)



Діаграма 15. Перестороги щодо використання ШІ в правосудді за віковими групами



Діаграма 16. Перестороги щодо використання АІ в правосудді за типами населених пунктів



Діаграма 17. Порівняння ставлення до використання ШІ в освіті і науці



Деталізація індивідуальних відповідей респондентів щодо опасінь впровадження ШІ

*Аналіз даних з таблиці відповідей результатів опитування «Очікування від впровадження штучного інтелекту» (Додаток 2) здійснювався з використання системи штучного інтелекту Perplexity.Pro

1. Деталізація індивідуальних відповідей щодо опасінь впровадження ШІ респондентів вікової групи 14-21 років

Респонденти вікової групи 14-21 (159 осіб) мають 25.8% тривоги. Виразили опасіння щодо впровадження штучного інтелекту, фокусуючись на загальних ризиках та конкретних сферах (стовпці «Які небезпеки...» та «Які сфери... недопустимими?»). Аналіз індивідуальних відповідей показує типові страхи: заміна праці, деградація, непередбачуваність; недопустимі сфери — освіта, війна, медицина.

Описи опасінь 14-21 років:

Заміна праці/безробіття (економіка): «Зменшення кількості доступних професій, як наслідок безробіття»; «Роботи замінять людей»; «бракування робочих місць для людей» (економіка).

Деградація/втрата навичок: «Деградація людства»; «можуть замінити потребу самостійно думати та взагалі потребу і людині»; «На мою думку, люди забудуть що таке мозок і як ним користуватись» (освіта).

Непередбачуваність/контроль: «Непередбачуваність»; «Повне «обездушевлення» суспільства» (правосуддя).

Клонування/приватність: «Клонування даних» (держуправління).

Недопустимі сфери (за відповідями)

Представники 14-21 часто називають (освіта, воєнна сфера): типові комбінації «Освіта і наука, Воєнна сфера у т.ч. розробка зброї» (воєнна). Інші: правоохоронна, політика (правосуддя, політика).

2. Деталізація індивідуальних відповідей щодо опасінь впровадження ШІ респондентів вікової групи 21-30 років

Респонденти вікової групи 22-30 років (338 осіб) у файлі ShI_anketa-Otvety.xlsx виразили найвищий рівень опасінь (95,3% «Так»). Аналіз відповідей показує фокус на втраті контролю, деградації, втраті праці; недопустимі сфери — освіта, правоохоронна, війна.

Описи опасінь 22-30 років:

Втрата контролю/етики: «Передача під контроль алгоритмів важливих сфер життя... розлюднення самої людини»; «Вихід з під контроль людини. Порушення прав людини. Етичне питання» (правосуддя).

Деградація/знецінення: «Люди перестанут думати і творити»; «Деградація людства»; «знецінення людських навичок та знань» (освіта).

Заміна праці: «Штучний інтелект може сильно зменшити кількість робочих місць»; «Стало менше живого спілкування і багато людей втрачають роботу» (економіка).

Релаксація/втрата спілкування: «Забагато ШІ контенту можуть занадто послабити наше/майбутнє покоління» (медицина).

Недопустимі сфери (за відповідями)

Типові: «Освіта і наука, Правоохоронна діяльність та правосуддя» (освіта, правосуддя); воєнна сфера, політика часто згадуються.

3. Деталізація індивідуальних відповідей щодо опасінь впровадження ШІ респондентів вікової групи 30-40 років

Респонденти вікової групи 30-40 років (510 осіб) демонструють баланс тривоги (50,8%). Аналіз відповідей акцентує втрату контакту, непередбачуваність, заміну людини; недопустимі сфери — війна, критична інфраструктура.

Описи опасінь 30-40 років:

Втрата людського/духовного: «Втрата духовних цінностей і безпосереднього психологічного контакту при спілкуванні» (медицина).

Непередбачуваність/контроль: «Відсутність досвіду людства у взаємодії з ШІ може призвести до проблем...»; «надмірний контроль ШІ над військовою та критичною інфраструктурою» (воєнна).

Деградація/заміна: «Непотрібність та деградація»; «Заміна людини»; «Зменшення попиту на залучення людини...» (економіка).

Навчання негативу/загроза: «АІ самонавчається... негативним практикам... Людина насправді і є загрозою» (політика).

Недопустимі сфери (за типовими патернами)

Часто: воєнна сфера, правоохоронна, держуправління (воєнна, правосуддя).

4. Деталізація індивідуальних відповідей щодо опасінь впровадження ШІ респондентів вікової групи 41-50 років

Респонденти вікової групи 41-50 (39 осіб) мають 48,7% тривоги. Аналіз відповідей підкреслює деградацію, вторгнення, анти-людський потенціал; недопустимі сфери — професії, вплив на суспільство загалом.

Описи опасінь 41-50 років:

Деградація/занепад: «Відсутність душі в роботі та знецінення і занепад людського мислення»; «Деградація суспільства» (освіта).

Вторгнення/контроль: «Вторгнення в усі процеси»; «Може бути спрямований проти людини»; «Знищення людства» (воєнна).

Заміна професій: «Відхід багатьох професій»; «Деякі професії зазнають турбулентності» (економіка).

Неконтрольованість: «Возможные неконтролируемые сбои»; «Це небезпека для людства» (правосуддя).

5. Деталізація індивідуальних відповідей щодо опасень впровадження ІІІ респондентів вікової групи 51-60 років

Респонденти вікової групи 51-60 (25 осіб) мають 48% тривоги. Аналіз відповідей фокусується на втраті контролю, маніпуляції, залежності; недопустимі — уряди, злочини.

Описи опасень 51-60 років:

Втрата контролю: «Що ІІІ вийде з під контролю»; «Втрата контрольованості»; «Штучний інтелект може розвинутися самостійно так, що ми втратимо над ним контроль» (воєнна).

Маніпуляція/пропаганда: «Полегшення деструктивних впливів... пропагандистських наративів у разі використання ІІІ урядами»; «Маніпулювати людською свідомістю» (політика).

Деградація/залежність: «Людський потенціал знецінюється»; «Дебілізація людей»; «залежність від технологій»; «Відмова користуватися власним інтелектом» (освіта).

Злочини/неконтрольованість: «Вихід за межі контролю і використання ІІІ для вчинення злочинної діяльності»; «Неконтрольованість застосування» (правосуддя).

6. Деталізація індивідуальних відповідей щодо опасень впровадження ІІІ респондентів вікової групи 61-70

Респонденти вікової групи 61-70 років (17 осіб) у файлі найоптимістичніші (52,9% «Ні», 29,4% тривоги). Аналіз відповідей акцентує деградацію, безробіття, втрату контролю; багато «не відчуваю».

Описи опасень 61-70 років:

Деградація/навички: «Делегування інтелектуальної роботи роботам... деградація до середньовіччя»; «інтелектуальна деградація» (освіта).

Безробіття/контроль: «Збільшення безробіття. Можливість ІІІ самовдосконалюватися та вийти з під контролю»; «Втрата контролю»; «Втрата робочих місць...» (економіка).

Загрози/етика: «Небезпеки включають... посилення контролю та стеження, можливі упередження... ризик втрати контролю» (правосуддя).

Невідомість: «Поки не ясно»; «Невідомість»; «Людський чинник» (політика).

Недопустимі сфери (за патернами)

Контроль/стеження, автономні системи (правосуддя, воєнна).

7. Деталізація індивідуальних відповідей щодо опасінь впровадження ШІ респондентів вікової групи 70+ років

Респонденти вікової групи 70+ років (4 особи: 70+ та 71+) доволі оптимістичні (50% «Ні»). Тривожні акцентують втрату контролю.

Описи опасінь 70+ років

Вихід з-під контролю: «Можливість виходу ШІ з під контролю людини і вчинення діянь на шкоду людині»; «Неконтрольованість застосування»; «вихід з-під контролю людства» (воєнна).

Відсутність: «Ніяких» – домінує оптимізм.

Недопустимі сфери

Контроль/шкода людині (воєнна, правосуддя)

ПРОЄКТ ЗАКОНУ УКРАЇНИ

Про внесення змін до Закону України «Про освіту» та Закону України «Про академічну доброчесність» щодо врегулювання використання технологій штучного інтелекту в освітній та науковій діяльності

Верховна Рада України постановляє:

Стаття 1. Внести зміни до Закону України «Про освіту» (Відомості Верховної Ради України, 2017 р., № 38-39, ст. 380 із наступними змінами):

1. У статті 42:

1. Частину другу після абзацу сьомого доповнити новим абзацом такого змісту: «затвердження та оприлюднення внутрішніх правил використання технологій штучного інтелекту в освітньому процесі, у тому числі правил декларування такого використання, перевірки самостійності виконання робіт і процедур розгляду випадків ШІ-пов'язаного академічного плагіату». У зв'язку з цим абзаци восьмий – десятий вважати відповідно абзацами дев'ятим – одинадцятим.

2. Частину третю після абзацу другого доповнити новим абзацом такого змісту: «декларування використання технологій штучного інтелекту під час підготовки навчальних, кваліфікаційних, творчих та інших академічних робіт із зазначенням ролі таких технологій у створенні відповідного результату». У зв'язку з цим абзаци третій – п'ятий вважати відповідно абзацами четвертим – шостим.

3. У частині четвертій:

абзац другий викласти в такій редакції: «академічний плагіат – оприлюднення (частково або повністю) наукових, творчих, навчальних або інших академічних результатів, отриманих іншими особами або створених (згенерованих) із використанням технологій штучного інтелекту та інших автоматизованих систем, як результатів власної діяльності без належного зазначення факту такого використання; та/або відтворення (частково або повністю) опублікованих текстів, зображень, кодів, структур даних, творів мистецтва та інших результатів інтелектуальної діяльності інших авторів без зазначення авторства, у тому числі із застосуванням технологій штучного інтелекту для маскуванню джерела запозичення, перефразування, автоматизованого перекладу або іншого приховування походження запозиченого результату»;

після абзацу другого доповнити новим абзацом такого змісту: «ШІ-пов'язаний академічний плагіат – форма академічного плагіату, що полягає у несанкціонованому або недекларованому використанні результатів

(текстів, кодів, зображень, структур даних та інших об'єктів), згенерованих технологіями штучного інтелекту, як власного оригінального результату без зазначення факту використання таких технологій та, за наявності, джерела даних, а також у використанні технологій штучного інтелекту для обходу систем перевірки на плагіат, маскування факту запозичення, перефразування чи автоматизованого перекладу чужих текстів без належного посилання на першоджерело». У зв'язку з цим абзаци третій – дев'ятий вважати відповідно абзацами четвертим – десятим.

4. Доповнити статтю новою частиною такого змісту: «6. Використання технологій штучного інтелекту в обсязі, який фактично замінює самостійне виконання навчальної, кваліфікаційної або наукової роботи, зокрема створення значної частини тексту, коду чи інших результатів без істотного інтелектуального внеску автора, розглядається як порушення академічної доброчесності за правилами, встановленими для академічного плагіату та виконання академічних робіт іншими особами».

Стаття 2. Внести зміни до Закону України «Про академічну доброчесність»:

1. У частині першій статті 2:

1. Пункт 1 викласти в такій редакції: «1) academic plagiarism (академічний плагіат) – оприлюднення (частково або повністю) наукових, творчих, навчальних або інших академічних результатів: а) отриманих іншими особами або створених (згенерованих) із використанням технологій штучного інтелекту та інших автоматизованих систем, як результатів власної діяльності без належного зазначення такого використання; та/або б) відтворення (частково або повністю) опублікованих текстів, зображень, кодів, структур даних та інших академічних творів інших авторів без зазначення авторства, у тому числі із застосуванням технологій штучного інтелекту для маскування джерела запозичення».
2. Доповнити частину новим пунктом такого змісту: «ШІ-пов'язаний академічний плагіат – форма академічного плагіату, що полягає у: а) несанкціонованому або недекларованому використанні результатів (текстів, кодів, зображень, структур даних, інших об'єктів), згенерованих технологіями штучного інтелекту, як власного оригінального результату без зазначення факту використання таких технологій та, за наявності, джерела даних; б) використанні технологій штучного інтелекту для обходу систем перевірки на плагіат, маскування факту запозичення, перефразування чи автоматизованого перекладу чужих текстів без належного посилання на першоджерело».
2. Статтю 16 доповнити новою частиною такого змісту: «3. Суб'єкти академічної діяльності зобов'язані відкрито декларувати використання технологій штучного інтелекту під час підготовки академічних творів, наукових робіт, дисертацій, кваліфікаційних робіт, навчальних матеріалів

та інших результатів академічної діяльності із зазначенням ролі таких технологій у створенні відповідного результату».

3. Статтю 20 доповнити новою частиною такого змісту: «3. Використання технологій штучного інтелекту в обсязі, який фактично замінює самостійне виконання академічної роботи та нівелює творчий внесок автора, розглядається як порушення академічної доброчесності за правилами, встановленими для академічного плагіату та виконання академічних робіт іншими особами».
4. Статтю 30 доповнити новою частиною такого змісту: «5. Під час розгляду та встановлення фактів можливого ШІ-пов'язаного академічного плагіату уповноважені органи обов'язково враховують наявність чи відсутність добровільного декларування використання технологій штучного інтелекту, реальний обсяг та характер власного інтелектуального внеску автора, функціональне призначення використаних автоматизованих інструментів, а також дотримання внутрішніх політик і регламентів закладу освіти чи наукової установи».
5. Доповнити закон статтею 24-1 такого змісту: «Стаття 24-1. Особливості академічної відповідальності за ШІ-пов'язаний академічний плагіат
6. Заходи академічної відповідальності (санкції) за ШІ-пов'язаний академічний плагіат застосовуються за правилами, встановленими цим Законом для інших форм академічного плагіату.
7. При визначенні виду та суворості академічного стягнення враховуються характер порушення, ступінь умислу особи, системність дій, обсяг використання технологій штучного інтелекту відносно загального обсягу академічного твору, а також рівень академічної або наукової підготовки особи».

Стаття 3. Прикінцеві та перехідні положення

1. Цей Закон набирає чинності через шість місяців з дня його опублікування.
2. Кабінету Міністрів України у тримісячний строк з дня опублікування цього Закону:
 - підготувати та подати на розглядання Верховної Ради України пропозиції щодо приведення законодавчих актів України у відповідність із цим Законом;
 - забезпечити розроблення та затвердження методичних рекомендацій щодо належного використання і розширеного декларування технологій штучного інтелекту в освітній та науковій діяльності;
 - забезпечити перегляд і скасування або оновлення підзаконних нормативно-правових актів у сфері освіти, науки та забезпечення якості освіти з метою їх узгодження з цим Законом.
3. Рекомендувати Міністерству освіти і науки України, Національному агентству із забезпечення якості вищої освіти та Національному агентству кваліфікацій у межах їх повноважень скоординувати заклади

вищої освіти та наукові установи щодо виконання таких завдань у шестимісячний строк з дня опублікування цього Закону:

- привести внутрішні положення про академічну доброчесність та кодекси етики у відповідність із цим Законом;
- затвердити чіткі інституційні правила та типові форми декларування використання технологій штучного інтелекту в освітній та науковій діяльності;
- передбачити валідовані технічні й процедурні алгоритми виявлення та розгляду випадків ШІ-пов'язаного академічного плагіату;
- забезпечити проведення постійних інформаційно-роз'яснювальних та освітніх заходів для здобувачів освіти, педагогічних, науково-педагогічних і наукових працівників з метою підвищення рівня AI-літеративності.

**ПРОПОЗИЦІЇ
ЩОДО ВДОСКОНАЛЕННЯ НАЦІОНАЛЬНОГО
ЗАКОНОДАВСТВА
У СФЕРІ БЕЗПЕЧНОГО ТА ВІДПОВІДАЛЬНОГО
ВИКОРИСТАННЯ
СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ**

ВСТУПНІ ПОЛОЖЕННЯ

Актуальність нормопроєктних пропозицій підтверджується тим, що План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки передбачає подальше формування законодавчих і методичних засад у цій сфері, а План законопроектної роботи Верховної Ради України на 2026 рік містить розроблення проєкту Закону про штучний інтелект, спрямованого на гармонізацію з Регламентом (ЄС) 2024/1689. Україна також підписала Рамкову конвенцію Ради Європи про штучний інтелект, права людини, демократію та верховенство права. Отже, запропоновані акти відповідають об'єктивному напрямку розвитку національної правової політики та можуть використовуватися як доктринальна модель для підготовки законодавства.

Пакет побудовано за принципом багаторівневого регулювання. Рамковий закон установлює горизонтальні правила для всього життєвого циклу систем ШІ. Закон про внесення змін до суміжних актів інтегрує ці правила в адміністративну процедуру, захист персональних даних, доступ до публічної інформації, функціонування електронних реєстрів і публічні закупівлі. Підзаконні акти визначають процедуру оцінки впливу, ведення реєстру, повідомлення про інциденти та функціонування регуляторного експериментального середовища.

При остаточній підготовці актів до внесення суб'єктом законодавчої ініціативи необхідні антикорупційна, гендерно-правова, цифрова, бюджетна та євроінтеграційна експертизи, узгодження з правилами нормопроєктувальної техніки, а також консультації з Уповноваженим Верховної Ради України з прав людини, органами сектору безпеки і оборони, судовою владою, органами місцевого самоврядування, науковою спільнотою, бізнесом і представниками громадянського суспільства.

ЗВЕДЕНА МАТРИЦЯ НОРМОТВОРЧИХ ПРОПОЗИЦІЙ

Виявлена прогалина	Запропонований акт	Ключовий правовий інструмент	Очікуваний результат
Відсутність рамкового закону і класифікації ризиків	Закон України «Про безпечне та відповідальне використання систем штучного інтелекту»	Заборонені практики, високоризикові системи, обов'язки суб'єктів,	Правова визначеність та сумісність із європейською ризикоорієнтованою моделлю

Виявлена прогалина	Запропонований акт	Ключовий правовий інструмент	Очікуваний результат
		нагляд і санкції	
Недостатність процедурних та інформаційних гарантій	Закон про внесення змін до суміжних законів	Людський перегляд, пояснення, мотивування, профілювання, відкритість, журналювання	Захист особи від непрозорого або дискримінаційного алгоритмічного рішення
Відсутність обов'язкової оцінки впливу	Постанова КМУ про Порядок оцінки впливу	Ex ante оцінка прав, ризиків, даних, пропорційності та залишкового ризику	Превентивний контроль до введення високоризикової системи в експлуатацію
Відсутність реєстру та єдиного порядку реагування на інциденти	Постанова КМУ про Реєстр високоризикових систем ІІІ	Публічна і закрита частини реєстру, попереднє повідомлення, повний звіт	Простежуваність, підзвітність і своєчасне припинення небезпечної практики
Необхідність підтримки інновацій без зниження стандартів прав людини	Постанова КМУ про регуляторне експериментальне середовище	Контрольовані й строковий експеримент, індивідуальний план випробувань, вихідна оцінка	Підготовка розробників до обов'язкового регулювання та зменшення регуляторної невизначеності

ЗАКОН УКРАЇНИ «ПРО БЕЗПЕЧНЕ ТА ВІДПОВІДАЛЬНЕ ВИКОРИСТАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ»

Науково-правове обґрунтування

Необхідність рамкового закону зумовлена тим, що загальні норми інформаційного, адміністративного, цивільного та безпекового законодавства регулюють окремі компоненти використання ШІ, але не охоплюють систему впродовж її життєвого циклу. Вони не пов'язують рівень ризику з інтенсивністю юридичних обов'язків, не визначають правовий статус постачальника і розгортувача, не встановлюють єдиної процедури оцінки відповідності, реєстрації, моніторингу та повідомлення про інциденти.

Для інформаційного права цей закон має системоутворююче значення: його норми поєднують інформаційно-правові вимоги до даних, прозорості, журналювання і кібербезпеки з адміністративно-правовими інструментами допуску, реєстрації, державного нагляду, перевірок, коригувальних заходів і оскарження. Закон не повинен механічно відтворювати AI Act, але має забезпечити функціональну сумісність із ним та реалізацію правозахисних стандартів Рамкової конвенції Ради Європи.

Під час воєнного стану потрібен не загальний виняток із регулювання, а спеціальний захищений режим. Обмеження публічності, особливі процедури закупівель і використання систем у розвідувальній або оборонній діяльності можуть бути виправданими, однак вони не усувають вимог законності, пропорційності, журналювання, внутрішнього аудиту та визначення персональної відповідальності.

ПРОЄКТ ЗАКОН УКРАЇНИ

Про безпечне та відповідальне використання систем штучного інтелекту

Цей Закон визначає правові та організаційні засади розроблення, введення в обіг, введення в експлуатацію та використання систем штучного інтелекту, встановлює ризикоорієнтовані режими, гарантії захисту прав людини, повноваження органів публічної влади, порядок нагляду та відповідальність за порушення законодавства у цій сфері.

РОЗДІЛ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Мета і предмет Закону

1. Метою цього Закону є забезпечення безпечного, правомірного, прозорого та людиноцентричного використання систем штучного інтелекту, запобігання неприйнятним ризикам для життя, здоров'я, гідності, приватності, рівності, демократії, верховенства права, публічної та національної безпеки, а також створення передбачуваних умов для інновацій.

2. Цей Закон регулює відносини, що виникають під час розроблення, навчання, тестування, введення в обіг, введення в експлуатацію, використання, суттєвої модифікації та припинення використання систем штучного інтелекту.

Стаття 2. Визначення основних термінів

1. У цьому Законі система штучного інтелекту означає машинну систему, розроблену для функціонування з різним рівнем автономності, яка після введення в експлуатацію може виявляти адаптивність і на підставі отриманих вхідних даних робить висновки щодо створення прогнозів, контенту, рекомендацій або рішень, здатних впливати на фізичне чи віртуальне середовище.

2. Постачальник - фізична або юридична особа, орган державної влади чи орган місцевого самоврядування, які розробляють систему ШІ або доручають її розроблення та вводять її в обіг чи експлуатацію під власним найменуванням або торговельною маркою.

3. Розгортувач - особа або орган, що використовує систему ШІ під власною відповідальністю, крім використання фізичною особою виключно в особистих непрофесійних цілях.

4. Суттєва модифікація - зміна системи ШІ після її введення в обіг або експлуатацію, яка не була передбачена первинною оцінкою відповідності та впливає на призначення, рівень ризику, точність, надійність або права осіб.

5. Серйозний інцидент - подія або порушення функціонування системи ШІ, що спричинило або могло спричинити смерть, тяжку шкоду здоров'ю, істотне порушення основоположних прав, значну майнову шкоду, порушення роботи критичної інфраструктури чи системну дискримінацію.

6. Оцінка впливу на основоположні права - документована процедура попереднього виявлення, аналізу, мінімізації та контролю ризиків системи ШІ для прав, свобод і законних інтересів фізичних осіб та суспільства.

7. Змістовний людський контроль - організаційна і технічна здатність компетентної особи розуміти призначення та обмеження системи, виявляти аномалії, не враховувати, скасовувати або коригувати її результат та безпечно зупиняти систему.

Стаття 3. Сфера дії Закону

1. Цей Закон застосовується до постачальників, імпортерів, розповсюджувачів і розгортувачів систем ІІІ на території України, а також до іноземних постачальників, якщо система вводиться в обіг в Україні або її результат використовується для прийняття юридично значущого рішення щодо особи, яка перебуває в Україні.
2. Дія Закону не поширюється на наукові дослідження до моменту випробування системи поза контрольованим середовищем, за умови дотримання законодавства про персональні дані, біоетику, державну таємницю та кібербезпеку.
3. Особливості застосування Закону до систем у сфері оборони, розвідки та національної безпеки визначаються статтею 42 цього Закону та спеціальними законами.

Стаття 4. Принципи використання систем ІІІ

1. Використання систем ІІІ ґрунтується на принципах верховенства права, людської гідності, законності, необхідності й пропорційності, недискримінації, безпеки, прозорості, підзвітності, захисту даних за проєктуванням, технологічної нейтральності, змістовного людського контролю та запобігання шкоді.
2. Економічна ефективність, інноваційність або складність системи не можуть бути самостійною підставою для обмеження прав людини чи звільнення відповідальних осіб від виконання юридичних обов'язків.

Стаття 5. Співвідношення з іншими актами законодавства

1. У разі використання системи ІІІ під час адміністративного провадження застосовуються також вимоги Закону України «Про адміністративну процедуру».
2. Обробка персональних даних системами ІІІ здійснюється відповідно до законодавства про захист персональних даних. Виконання вимог цього Закону не звільняє від виконання вимог щодо конфіденційності, доступу до публічної інформації, кібербезпеки, захисту споживачів, конкуренції та інтелектуальної власності.
3. Секторальний закон може встановлювати більш суворі вимоги, якщо це необхідно з огляду на характер ризику.

РОЗДІЛ II. РИЗИК-ОРІЄНТОВАНІ РЕЖИМИ

Стаття 6. Категорії систем і практик за рівнем ризику

1. За рівнем ризику правове регулювання розрізняє: заборонені практики; високоризикові системи; системи з обмеженим ризиком, щодо яких установлюються обов'язки прозорості; системи мінімального ризику.
2. Класифікація здійснюється з урахуванням призначення системи, характеру і масштабу можливих наслідків, категорій осіб, рівня автономності, оборотності наслідків, якості даних та можливості ефективного людського втручання.

Стаття 7. Заборонені практики

1. Забороняється введення в обіг, введення в експлуатацію або використання систем ШІ для прихованого маніпулювання особою, якщо це істотно спотворює її поведінку та спричиняє або з високою імовірністю може спричинити значну шкоду.
2. Забороняється використання вразливості осіб, зумовленої віком, інвалідністю, тяжким соціальним або економічним становищем, з метою істотного спотворення їх поведінки.
3. Забороняється соціальне оцінювання фізичних осіб органами публічної влади на підставі поведінки або передбачуваних особистісних характеристик, якщо результат призводить до несприятливого поводження в контексті, не пов'язаному з первинним збиранням даних, або є непропорційним.
4. Забороняється оцінювання ризику вчинення особою кримінального правопорушення виключно на підставі профілювання, рис особистості чи поведінкових характеристик без об'єктивних і перевірюваних фактів, пов'язаних із конкретною діяльністю.
5. Забороняється невивіркове збирання зображень облич із мережі Інтернет або відеоспостереження для створення чи розширення баз біометричної ідентифікації.
6. Забороняється біометрична категоризація осіб за ознаками, що розкривають расове чи етнічне походження, політичні погляди, релігійні переконання, стан здоров'я, сексуальне життя або орієнтацію, крім обробки, прямо дозволеної законом для захисту життєво важливих інтересів та за наявності посиленних гарантій.
7. Дистанційна біометрична ідентифікація в режимі реального часу в загальнодоступному просторі допускається лише у виключних випадках, прямо визначених законом, на підставі попереднього судового дозволу, щодо конкретної мети, території, строку та категорії осіб.
8. Забороняється прийняття остаточного несприятливого владного або судового рішення виключно на підставі результату системи ШІ, якщо законом не

передбачено автоматичний режим для формалізованої операції без дискреції та гарантовано негайний перегляд компетентною людиною.

Стаття 8. Високоризикові системи

1. До високоризикових належать системи ІІІ, що є компонентами безпеки продукції або інфраструктури, а також системи, які використовуються для біометричної ідентифікації; доступу до освіти й оцінювання; працевлаштування та управління працівниками; доступу до істотних приватних або публічних послуг; кредитного, страхового чи соціального оцінювання; правоохоронної діяльності; міграції, притулку та контролю кордонів; правосуддя; охорони здоров'я; управління критичною інфраструктурою; прийняття адміністративних актів, здатних істотно вплинути на права особи.

2. Кабінет Міністрів України затверджує і переглядає перелік високоризикових систем з урахуванням критеріїв, визначених цим Законом, міжнародних зобов'язань та розвитку технологій.

Стаття 9. Системи з обмеженим та мінімальним ризиком

1. Для чат-ботів, генеративних систем, систем синтезу зображень, аудіо або відео та інших систем, взаємодія з якими може бути помилково сприйнята як взаємодія з людиною або автентичний контент, встановлюється обов'язок чіткого інформування про штучне походження взаємодії або матеріалу.

2. Для систем мінімального ризику обов'язкові спеціальні процедури не встановлюються, однак їх постачальники можуть добровільно приєднуватися до кодексів відповідального використання.

Стаття 10. Зміна класифікації та суттєва модифікація

1. Постачальник зобов'язаний повторно визначити категорію ризику до здійснення суттєвої модифікації або зміни призначення системи.

2. Особа, яка здійснила суттєву модифікацію високоризикової системи, набуває обов'язків постачальника щодо зміненої системи.

РОЗДІЛ ІІІ. ВИМОГИ ДО ВИСОКОРИЗИКОВИХ СИСТЕМ

Стаття 11. Система управління ризиками

1. Постачальник створює, документує та підтримує безперервну систему управління ризиками протягом усього життєвого циклу системи.

2. Система управління ризиками охоплює ідентифікацію передбачуваних ризиків і обґрунтовано передбачуваного неправильного використання, тестування, визначення заходів мінімізації та оцінювання залишкового ризику.

Стаття 12. Управління даними

1. Навчальні, валідаційні та тестові набори даних повинні відповідати призначенню системи, бути достатньо репрезентативними, актуальними, повними та перевіреними на наявність системної похибки й дискримінаційного впливу.
2. Постачальник документує походження даних, правову підставу їх використання, процедури очищення, анотації, збагачення та усунення похибок.
3. Використання персональних даних допускається лише в обсязі, необхідному для визначеної законної мети, із застосуванням принципів мінімізації та захисту даних за проєктуванням.

Стаття 13. Технічна документація

1. До введення високоризикової системи в обіг постачальник готує технічну документацію, достатню для оцінювання відповідності, перевірки призначення, архітектури, даних, показників точності, обмежень, заходів кібербезпеки та людського контролю.
2. Документація зберігається не менше десяти років після припинення введення системи в обіг, якщо спеціальним законом не встановлено довший строк.

Стаття 14. Автоматичне журналювання

1. Високоризикова система повинна технічно забезпечувати автоматичну фіксацію подій, необхідних для встановлення часу, версії системи, вхідних даних, результату, втручання оператора, помилок та зупинення системи.
2. Журнали зберігаються протягом строку, пропорційного призначенню системи та можливого строку оскарження, але не менше шести місяців, якщо інше не встановлено законом.

Стаття 15. Прозорість та інструкції

1. Високоризикова система постачається з інструкціями, що містять відомості про призначення, рівень точності, відомі обмеження, категорії даних, ризики, необхідну кваліфікацію операторів, умови людського контролю та порядок реагування на аномалії.
2. Інструкції повинні бути зрозумілими для професійного користувача та не можуть замінювати обов'язкову оцінку впливу розгортувачем.

Стаття 16. Змістовний людський контроль

1. Постачальник і розгортувач забезпечують організаційні та технічні заходи, які дозволяють уповноваженій особі розуміти можливості та обмеження системи, виявляти автоматизаційне упередження, контролювати результат, не враховувати або скасовувати його та безпечно зупиняти систему.

2. Особа, яка здійснює контроль, повинна мати належну компетентність, повноваження, час і доступ до інформації та не може нести дисциплінарну відповідальність за обґрунтоване зупинення небезпечної системи.

Стаття 17. Точність, надійність і кібербезпека

1. Високоризикова система повинна досягати задекларованого рівня точності, надійності та стійкості впродовж життєвого циклу.
2. Постачальник забезпечує захист від отруєння даних, підміни моделі, маніпулятивних запитів, витoku параметрів, несанкціонованої модифікації та інших характерних для машинного навчання загроз.

Стаття 18. Система управління якістю

1. Постачальник високоризикової системи впроваджує документовану систему управління якістю, яка охоплює розподіл відповідальності, контроль проєктування, управління даними, тестування, аудит, обробку скарг, моніторинг і реагування на інциденти.

Стаття 19. Оцінка відповідності

1. До введення високоризикової системи в обіг або експлуатацію проводиться оцінка її відповідності вимогам цього Закону.
2. Оцінка здійснюється постачальником із залученням незалежного органу оцінки відповідності у випадках, визначених Кабінетом Міністрів України з урахуванням рівня ризику та секторального законодавства.
3. Суттєва модифікація вимагає повторної оцінки відповідності.

Стаття 20. Державна реєстрація

1. Високоризикова система до початку використання підлягає внесенню до Державного реєстру високоризикових систем ІІІ.
2. Відомості про системи у сферах оборони, розвідки, правоохоронної діяльності та захисту критичної інфраструктури можуть вноситися до закритої частини Реєстру.

РОЗДІЛ IV. ОБОВ'ЯЗКИ СУБ'ЄКТІВ

Стаття 21. Обов'язки постачальника

1. Постачальник забезпечує відповідність системи вимогам цього Закону, проводить тестування, готує документацію, реєструє систему, здійснює постринковий моніторинг, повідомляє про інциденти та вживає коригувальних заходів.

2. Постачальник призначає уповноважену особу, відповідальну за взаємодію з органом нагляду.

Стаття 22. Обов'язки імпортера та розповсюджувача

1. Імпортер перевіряє проходження оцінки відповідності, наявність документації, реєстрації та уповноваженого представника постачальника.

2. Розповсюджувач зобов'язаний діяти з належною обачністю і припинити надання системи на ринку, якщо має обґрунтовані підстави вважати, що вона не відповідає вимогам закону.

Стаття 23. Обов'язки розгортувача

1. Розгортувач використовує систему відповідно до призначення та інструкцій, призначає осіб людського контролю, контролює якість вхідних даних, зберігає журнали, повідомляє про інциденти та припиняє використання в разі неприйняттого ризику.

2. Розгортувач не може перекладати власну юридичну відповідальність на постачальника або систему ІІІ.

Стаття 24. Додаткові обов'язки органів публічної влади

1. До закупівлі або розгортання високоризикової системи орган публічної влади визначає законну мету, перевіряє наявність компетенції, проводить оцінку впливу на основоположні права та забезпечує бюджетні й кадрові ресурси для людського контролю.

2. Орган оприлюднює стислу інформацію про систему, правову підставу, мету, відповідального суб'єкта, категорії даних, основні ризики та порядок оскарження, крім відомостей з обмеженим доступом.

3. У договорі про закупівлю повинно бути передбачено право органу та компетентного наглядового органу на аудит, доступ до документації, журналів і відомостей, необхідних для перевірки законності.

Стаття 25. Оцінка впливу на основоположні права

1. Органи публічної влади, а також суб'єкти, які надають істотні публічні або приватні послуги, до початку використання високоризикової системи проводять оцінку впливу на основоположні права.

2. Оцінка містить опис мети, категорій осіб і даних, правової підстави, потенційних ризиків, альтернатив, заходів мінімізації, людського контролю, механізму оскарження та залишкового ризику.

3. Використання не допускається, якщо залишковий ризик є неприйнятним або заявлена мета може бути досягнута менш обтяжливим засобом.

Стаття 26. Вимоги до публічних закупівель систем ІІІ

1. Технічна специфікація закупівлі системи ІІІ повинна містити її призначення, очікувану категорію ризику, вимоги до даних, точності, кібербезпеки, журналювання, пояснюваності, аудиту, локалізації та передачі документації.
2. Не допускається укладення договору, умови якого позбавляють орган влади можливості виконати законний обов'язок із мотивування рішення, захисту персональних даних, контролю або надання інформації суду чи наглядовому органу.

Стаття 27. Постринковий моніторинг

1. Постачальник і розгортувач здійснюють систематичний моніторинг точності, помилок, дискримінаційного впливу, кіберінцидентів і невідповідності фактичного використання заявленому призначенню.
2. План моніторингу є частиною технічної документації та переглядається після суттєвої модифікації або серйозного інциденту.

Стаття 28. Повідомлення про серйозні інциденти

1. Постачальник або розгортувач невідкладно, але не пізніше 72 годин із моменту виявлення, подає попереднє повідомлення компетентному органу, а повний звіт - не пізніше 15 календарних днів.
2. У разі безпосередньої загрози життю, здоров'ю, критичній інфраструктурі або масового порушення прав система негайно зупиняється, якщо зупинення не створює більшої небезпеки.

РОЗДІЛ V. ПРАВА ОСІБ

Стаття 29. Право на інформацію про використання ІІІ

1. Особа має право бути поінформованою до або під час взаємодії із системою ІІІ, якщо система істотно впливає на її права, свободи чи законні інтереси.
2. Повідомлення містить мету, роль системи, відповідального суб'єкта, категорії даних та спосіб реалізації права на перегляд і оскарження.

Стаття 30. Право на змістовне пояснення

1. Особа, щодо якої прийнято юридично значуще рішення з істотним використанням високоризикової системи, має право отримати зрозуміле пояснення ролі системи, основних факторів, що вплинули на результат, використаних категорій даних та обмежень системи.
2. Комерційна таємниця не може бути підставою для відмови у наданні мінімальної інформації, необхідної для ефективного оскарження.

Стаття 31. Право на перегляд людиною

1. Особа має право вимагати перегляду рішення компетентною посадовою особою, яка не обмежена автоматичним результатом і має повноваження змінити або скасувати рішення.
2. Перегляд здійснюється у строк, установлений для адміністративного оскарження або відповідною секторальною процедурою.

Стаття 32. Оскарження та скарга на систему

1. Рішення, дія чи бездіяльність, пов'язані з використанням системи ШІ, можуть бути оскаржені в адміністративному або судовому порядку.
2. Особа має право звернутися до органу нагляду зі скаргою щодо незаконного використання системи, відсутності оцінки впливу, порушення обов'язків прозорості, дискримінації або неналежного людського контролю.

Стаття 33. Захист від дискримінації

1. Забороняється використання системи ШІ, яке спричиняє пряму або непряму дискримінацію.
2. У разі обґрунтованого припущення про алгоритмічну дискримінацію постачальник і розгортувач зобов'язані надати наглядовому органу та суду інформацію, необхідну для перевірки даних, показників і логіки системи.

РОЗДІЛ VI. ПУБЛІЧНЕ АДМІНІСТРУВАННЯ ТА НАГЛЯД**Стаття 34. Компетентний орган**

1. Державний нагляд у сфері ШІ здійснює центральний орган виконавчої влади зі спеціальним статусом - Державна служба нагляду за системами штучного інтелекту, діяльність якої спрямовується і координується Кабінетом Міністрів України через Міністра цифрової трансформації.
2. Орган є функціонально незалежним під час здійснення перевірок, прийняття рішень щодо невідповідності, застосування коригувальних заходів і санкцій.

Стаття 35. Повноваження компетентного органу

1. Компетентний орган веде Реєстр, здійснює нагляд, проводить перевірки, розглядає скарги, вимагає документацію та журнали, залучає експертів, приймає рішення про обмеження, зупинення або заборону використання системи, координує розслідування інцидентів і співпрацює з іноземними регуляторами.
2. Рішення органу може бути оскаржене в адміністративному суді.

Стаття 36. Секторальний нагляд та роль Уповноваженого Верховної Ради України з прав людини

1. Секторальні регулятори здійснюють нагляд у межах своєї компетенції та взаємодіють із компетентним органом за принципом мережевого регулювання.
2. Уповноважений Верховної Ради України з прав людини здійснює контроль за дотриманням прав людини і законодавства про персональні дані, має доступ до оцінок впливу та може ініціювати перевірку високоризикової системи.

Стаття 37. Державний реєстр високоризикових систем

1. Реєстр складається з публічної та закритої частин. Публічна частина містить відомості про призначення системи, постачальника, розгортувача, правову підставу, категорію ризику, дату оцінки відповідності та стислий виклад оцінки впливу.
2. Порядок ведення Реєстру, обсяг закритих відомостей і доступ контролюючих органів визначаються Кабінетом Міністрів України.

Стаття 38. Регуляторне експериментальне середовище

1. Для випробування інноваційних систем може створюватися регуляторне експериментальне середовище з визначеним строком, індивідуальним планом, наглядом і заходами захисту прав.
2. Участь у середовищі не звільняє від дотримання Конституції України, законодавства про персональні дані, заборонених практик і обов'язку відшкодувати шкоду.

Стаття 39. Підтримка малого і середнього підприємництва

1. Держава забезпечує типові методики, консультації, стандартизовані форми документації, тестові середовища та пропорційні збори для малих і середніх підприємств без зниження рівня захисту прав людини.

РОЗДІЛ VII. КОНТРОЛЬ, ЗАХОДИ РЕАГУВАННЯ ТА ВІДПОВІДАЛЬНІСТЬ

Стаття 40. Перевірки та доступ до інформації

1. Компетентний орган проводить планові та позапланові перевірки на підставі ризиків, скарг, повідомлень про інциденти або ознак невідповідності.
2. Постачальник і розгортувач зобов'язані надати документацію, журнали, доступ до системи та тестового середовища в обсязі, необхідному для перевірки, із забезпеченням захисту державної та комерційної таємниці.

Стаття 41. Коригувальні заходи та фінансові санкції

1. У разі невідповідності компетентний орган може вимагати усунення порушення, обмежити призначення або територію використання, зупинити систему, відкликати її з ринку, видалити з Реєстру чи заборонити використання.
2. За заборонені практики може накладатися фінансова санкція до трьох відсотків загального річного доходу юридичної особи за попередній фінансовий рік або до п'ятнадцяти тисяч мінімальних заробітних плат - залежно від того, який розмір є меншим.
3. За порушення вимог до високоризикових систем може накладатися санкція до одного відсотка річного доходу або до семи тисяч п'ятисот мінімальних заробітних плат - залежно від того, який розмір є меншим.
4. Під час визначення санкції враховуються характер, тривалість, масштаб і наслідки порушення, умисел або недбалість, повторність, співпраця з органом, заходи мінімізації та фінансовий стан суб'єкта.
5. Накладення санкції не звільняє від цивільної, дисциплінарної, адміністративної або кримінальної відповідальності та обов'язку відшкодувати шкоду.

Стаття 42. Особливості в умовах воєнного стану, оборони, розвідки та національної безпеки

1. Для систем, використання яких пов'язане з державною таємницею, Кабінет Міністрів України встановлює закриті процедури оцінки впливу, реєстрації, аудиту й повідомлення про інциденти.
2. Обмеження відкритості не звільняє від вимог законності, необхідності, пропорційності, кібербезпеки, журналювання, внутрішнього аудиту, змістовного людського контролю та визначення відповідальних посадових осіб.
3. Рішення про застосування летальної сили не може бути повністю делеговане системі ШІ. Правила розроблення і використання автономних систем озброєння визначаються спеціальним законом з урахуванням міжнародного гуманітарного права.
4. Парламентський, прокурорський, судовий та інший передбачений законом контроль здійснюється в режимі, що забезпечує одночасно захист державної таємниці й ефективність перевірки.

Стаття 43. Прикінцеві та перехідні положення

1. Цей Закон набирає чинності через дванадцять місяців із дня його опублікування, крім положень про заборонені практики, які набирають чинності через шість місяців.

2. Кабінету Міністрів України протягом шести місяців утворити компетентний орган, затвердити перелік високоризикових систем, порядки оцінки впливу, ведення Реєстру, повідомлення про інциденти, оцінки відповідності та регуляторного експериментального середовища.
3. Органам публічної влади протягом дванадцяти місяців провести інвентаризацію систем ШІ, що використовуються, визначити їх категорії ризику та забезпечити реєстрацію високоризикових систем.
4. Кабінету Міністрів України внести на розгляд Верховної Ради України пропозиції щодо приведення законодавчих актів у відповідність із цим Законом.

Очікувані наслідки прийняття проєкту

- 1) формування єдиного понятійного апарату та передбачуваних правил для держави, бізнесу й громадян;
- 2) перехід від реагування після настання шкоди до превентивного управління ризиками;
- 3) забезпечення сумісності українських процедур із AI Act і міжнародними правозахисними стандартами;
- 4) підвищення довіри до цифрових публічних послуг та конкурентоспроможності українських розробників;
- 5) визначення реальних відповідальних суб'єктів замість перенесення відповідальності на технологію.

ЗАКОН УКРАЇНИ «ПРО ВНЕСЕННЯ ЗМІН ДО ДЕЯКИХ ЗАКОНОДАВЧИХ АКТІВ УКРАЇНИ ЩОДО ВИКОРИСТАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ»

Науково-правове обґрунтування

Рамковий закон не може самостійно забезпечити інтеграцію нових вимог у чинні процедури. Найбільші ризики виникають не лише через технічні характеристики системи, а через її включення у владне провадження, обробку персональних даних, електронні реєстри та публічні закупівлі. Тому необхідний синхронний пакет змін, який надасть особі конкретні процесуальні права й унеможливить посилення органу влади на «чорну скриньку» або комерційну таємницю постачальника.

ПРОЄКТ ЗАКОН УКРАЇНИ

Про внесення змін до деяких законодавчих актів України щодо використання систем штучного інтелекту

Верховна Рада України постановляє:

I. Внести зміни до таких законодавчих актів України:

1. У Законі України «Про адміністративну процедуру»:

– у статті 2 доповнити визначеннями: «алгоритмічно підтримане рішення» - адміністративний акт або інша дія адміністративного органу, під час підготовки яких результат системи ШІ використано як один із факторів оцінки; «автоматизований адміністративний акт» - адміністративний акт, сформований і прийнятий без безпосереднього формування змісту посадовою особою;

– після статті 69 доповнити статтею 69-1 такого змісту:

«Стаття 69-1. Використання систем штучного інтелекту в адміністративному провадженні

1. Система ШІ може використовуватися адміністративним органом лише для визначеної законом мети, у межах компетенції органу та після виконання вимог законодавства про безпечне і відповідальне використання систем ШІ.

2. Адміністративний орган до початку провадження або не пізніше першої комунікації з особою повідомляє про істотне використання системи ШІ, її роль, відповідального суб'єкта та право на перегляд людиною.

3. Остаточний адміністративний акт, який негативно впливає на право, свободу чи законний інтерес особи, не може ґрунтуватися виключно на результаті системи ШІ, крім автоматичного режиму, прямо передбаченого законом для формалізованого рішення без дискреції, за умови негайного перегляду компетентною посадовою особою на вимогу особи.

4. Посадова особа зобов'язана самостійно оцінити факти, належність даних і пропорційність рішення. Посилання на результат системи не замінює мотивування адміністративного акта.

5. У матеріалах справи фіксуються найменування і версія системи, дата використання, категорії вхідних даних, отриманий результат, відхилення або підтвердження результату посадовою особою та відомості про людський перегляд.

6. Комерційна таємниця не обмежує доступ суб'єкта розгляду скарги або суду до відомостей, необхідних для перевірки законності.»

– у статті 71 передбачити, що адміністративний акт повинен містити відомості про істотне використання системи ШІ, відповідальну посадову особу та порядок реалізації права на перегляд людиною;

– у статті 72 передбачити, що мотивування алгоритмічно підтриманого акта має містити основні фактичні й правові фактори, роль системи, пояснення відхилення або прийняття її результату та оцінку достовірності даних;

– у статті 78 визначити незаконне використання системи ШІ, відсутність обов'язкового людського перегляду або непроведення оцінки впливу як самостійні підстави адміністративного оскарження.

2. У Законі України «Про захист персональних даних»:

– статтю 2 доповнити визначеннями «профілювання», «автоматизоване рішення», «алгоритмічно виведені дані», «біометричні дані», «оцінка впливу на захист персональних даних»;

– частину другу статті 8 доповнити правами суб'єкта: бути поінформованим про автоматизоване рішення; отримати змістовну інформацію про основні фактори; заперечити проти профілювання; вимагати втручання людини; оскаржити результат; вимагати виправлення алгоритмічно виведених даних;

– доповнити статтею 8-1 такого змісту:

«Стаття 8-1. Автоматизовані рішення та профілювання

1. Суб'єкт персональних даних має право не бути об'єктом рішення, що ґрунтується виключно на автоматизованій обробці та спричиняє юридичні або інші істотні наслідки.

2. Таке рішення допускається, якщо воно необхідне для укладення або виконання договору, прямо передбачене законом із належними гарантіями або ґрунтується на явній згоді суб'єкта.

3. У будь-якому випадку забезпечуються право на людське втручання, викладення власної позиції, отримання пояснення та оскарження.

4. Рішення не може ґрунтуватися на спеціальних категоріях персональних даних, крім випадків, прямо передбачених законом і необхідних для захисту життєво важливих інтересів або істотного публічного інтересу з посиленими гарантіями.»

– доповнити статтею 24-1, якою встановити обов'язкову оцінку впливу на захист персональних даних до початку систематичного профілювання, масштабної обробки біометричних даних або використання високоризикової системи органом публічної влади;

– у статті 25 передбачити, що обмеження прав у сфері національної безпеки має бути визначене законом, необхідне й пропорційне, підлягати незалежному контролю та не може усувати право на ефективний засіб захисту.

3. У Законі України «Про доступ до публічної інформації»:

– до інформації, що підлягає обов'язковому оприлюдненню, віднести відомості про системи ШІ, які істотно використовуються розпорядником: найменування, мету, правову підставу, категорію ризику, постачальника, категорії даних, стислий виклад оцінки впливу, відповідальну посадову особу і порядок оскарження;

– установити, що обмеження доступу до технічної інформації не може перешкоджати наданню особі мінімального пояснення, необхідного для захисту її прав, або доступу суду та компетентного органу до повної документації в захищеному режимі.

4. У Законі України «Про публічні електронні реєстри»:

– передбачити, що використання реєстрових даних для навчання, валідації або застосування системи ШІ допускається лише за наявності визначеної законом мети та документованої оцінки сумісності з первинною метою обробки;

– заборонити вторинне використання реєстрових даних для соціального оцінювання, довільного профілювання або прогнозування поведінки без спеціальної законодавчої підстави;

– установити обов'язкове журналювання автоматизованих запитів, масового вивантаження, формування алгоритмічних висновків та передачі результатів між органами;

– визначити обов’язок власника реєстру забезпечувати якість, актуальність, виправлення помилок і можливість простежити джерело даних, що вплинули на юридично значуще рішення.

5. У Законі України «Про публічні закупівлі»:

– установити, що закупівля високоризикової системи ШІ здійснюється за наявності попереднього визначення законної мети, категорії ризику та проекту оцінки впливу;

– до обов’язкових умов технічної специфікації включити вимоги до точності, якості даних, журналювання, кібербезпеки, людського контролю, переносимості даних, оновлень, аудиту, припинення використання та передачі документації;

– заборонити умови договору, які унеможливають виконання органом обов’язків із мотивування рішення, захисту даних, розкриття інформації компетентному органу або проведення незалежного аудиту;

– передбачити обов’язок постачальника повідомляти замовника про суттєву модифікацію моделі або зміну показників ризику.

II. Прикінцеві положення

1) Цей Закон набирає чинності одночасно із Законом України «Про безпечне та відповідальне використання систем штучного інтелекту».

2) Кабінету Міністрів України протягом шести місяців привести свої нормативно-правові акти у відповідність із цим Законом.

Аргументація необхідності прийняття

Запропоновані зміни усувають розрив між рамковими вимогами та конкретними юридичними процедурами. Особливо важливим є доповнення Закону «Про адміністративну процедуру», оскільки чинна стаття 69 уже допускає автоматичне прийняття адміністративного акта у випадках, передбачених законом. Нова стаття 69-1 конкретизує гарантії, яких така автоматизація потребує: повідомлення, фіксацію системи, мотивування, відповідальну посадову особу та людський перегляд. Зміни до законодавства про персональні дані заповнюють прогалину щодо профілювання та автоматизованих рішень, а норми про доступ, реєстри й закупівлі забезпечують інформаційну відкритість і фактичну можливість контролю.

**ПОСТАНОВА КАБІНЕТУ МІНІСТРІВ УКРАЇНИ «ПРО
ЗАТВЕРДЖЕННЯ ПОРЯДКУ ПРОВЕДЕННЯ ОЦІНКИ ВПЛИВУ
ВИСОКОРИЗИКОВИХ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ НА
ОСНОВОПОЛОЖНІ ПРАВА»**

Науково-правове обґрунтування

Оцінка впливу є центральним превентивним інструментом. Вона має проводитися не як формальна анкета після закупівлі, а до остаточного рішення про розгортання, коли ще можливо змінити архітектуру, дані, мету або відмовитися від системи. Порядок повинен бути однаковим для органів публічної влади, але дозволяти секторальне уточнення критеріїв. Особливий режим потрібен для відомостей з обмеженим доступом, проте закритість не усуває самої оцінки.

**ПРОЄКТ
КАБІНЕТ МІНІСТРІВ УКРАЇНИ
ПОСТАНОВА**

**Про затвердження Порядку проведення оцінки впливу високоризикових
систем штучного інтелекту на основоположні права**

Кабінет Міністрів України постановляє:

- 1) Затвердити Порядок проведення оцінки впливу високоризикових систем штучного інтелекту на основоположні права, що додається.
- 2) Міністерству цифрової трансформації протягом трьох місяців затвердити методичні рекомендації, електронну форму оцінки та типові галузеві переліки ризиків.
- 3) Міністерствам та іншим центральним органам виконавчої влади протягом шести місяців провести інвентаризацію високоризикових систем, що використовуються, та забезпечити проведення оцінки.
- 4) Ця постанова набирає чинності одночасно із Законом України «Про безпечне та відповідальне використання систем штучного інтелекту».

ПОРЯДОК

проведення оцінки впливу високоризикових систем штучного інтелекту на основоположні права

Стаття 1. Загальні положення

1. Цей Порядок визначає суб'єктів, етапи, зміст, погодження, оприлюднення та перегляд оцінки впливу високоризикової системи ШІ на основоположні права.
2. Оцінка проводиться до введення системи в експлуатацію, а для систем, що вже використовуються, - до продовження їх використання після набрання чинності цим Порядком.

Стаття 2. Суб'єкти оцінки

1. Оцінку проводить розгортувач системи. Орган публічної влади утворює міждисциплінарну робочу групу за участю юридичного підрозділу, відповідального за захист персональних даних, фахівця з кібербезпеки, представника профільного підрозділу та за потреби незалежних експертів.
2. Особи, які брали участь у розробленні або постачанні системи, можуть надавати інформацію, але не можуть одноосібно затверджувати висновок про прийнятність ризику.

Стаття 3. Підстави проведення та повторної оцінки

1. Оцінка проводиться перед першим використанням високоризикової системи, після суттєвої модифікації, зміни мети чи категорій даних, після серйозного інциденту, а також не рідше одного разу на два роки.

Стаття 4. Етапи оцінки

1. Оцінка включає: опис системи й мети; перевірку компетенції та правової підстави; визначення категорій осіб і даних; ідентифікацію прав, що можуть бути порушені; аналіз необхідності й пропорційності; оцінювання імовірності та тяжкості шкоди; визначення альтернатив; план заходів мінімізації; оцінювання залишкового ризику; погодження і затвердження.

Стаття 5. Перевірка законної мети та альтернатив

1. Розгортувач обґрунтовує, чому мета відповідає його компетенції та не може бути досягнута менш обтяжливим способом із порівнянною ефективністю.
2. Відсутність економії коштів або часу сама по собі не є достатнім обґрунтуванням втручання у права.

Стаття 6. Оцінка даних і дискримінаційного впливу

1. Оцінюються походження, актуальність, репрезентативність і правова підстава використання даних, ризик системної похибки щодо вразливих груп, можливість виправлення та простеження джерела даних.

Стаття 7. Участь зацікавлених сторін

1. Для систем загального публічного значення проводиться консультація з представниками осіб, на яких впливатиме система, професійними та правозахисними організаціями.

2. Консультація може бути обмежена для інформації з обмеженим доступом, але має бути замінена незалежною експертизою в захищеному режимі.

Стаття 8. Критерії прийнятності

1. Ризик визнається неприйнятним, якщо практика заборонена законом, відсутня законна мета, неможливий ефективний людський контроль, існує висока імовірність тяжкої або необоротної шкоди без достатніх заходів мінімізації, або система створює системну дискримінацію.

Стаття 9. Затвердження та реєстрація

1. Оцінку затверджує керівник розгортувача або уповноважена ним посадова особа, яка несе відповідальність за рішення про введення системи в експлуатацію.

2. До реєстрації подається повний текст оцінки або її захищена версія та публічне резюме.

Стаття 10. Моніторинг і перегляд

1. План моніторингу визначає показники точності, помилок, скарг, дискримінаційного впливу, кіберінцидентів, випадків втручання оператора та умови зупинення системи.

Стаття 11. Оцінка систем з обмеженим доступом

1. Оцінка у сфері оборони, розвідки, правоохоронної діяльності або критичної інфраструктури проводиться комісією з відповідним допуском. Повний текст зберігається в захищеному режимі та надається уповноваженим органам контролю.

Стаття 12. Правові наслідки

1. Система не може бути введена в експлуатацію за відсутності затвердженої оцінки або за наявності неприйнятного залишкового ризику.

2. Компетентний орган може вимагати повторної оцінки, додаткових заходів, обмежити або заборонити використання системи.

Додаток 1. Мінімальна структура оцінки впливу

1. Найменування розгортувача, структурного підрозділу і відповідальної посадової особи.
2. Найменування, версія, постачальник, призначення і категорія ризику системи.
3. Правова підстава, компетенція та очікуваний публічний інтерес.
4. Опис технологічного процесу та ролі системи у прийнятті рішення.
5. Категорії осіб, даних і джерела даних.
6. Права та свободи, на які можливий вплив.
7. Ризики, імовірність, тяжкість, оборотність і масштаб.
8. Альтернативні засоби досягнення мети.
9. Заходи мінімізації, людського контролю, пояснення й оскарження.
10. План тестування, моніторингу, аудиту та реагування на інциденти.
11. Результати консультацій і незалежної експертизи.
12. Залишковий ризик і мотивований висновок про допустимість.

ПОСТАНОВА КАБІНЕТУ МІНІСТРІВ УКРАЇНИ «ПРО ДЕРЖАВНИЙ РЕЄСТР ВИСОКОРИЗИКОВИХ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ ТА ПОВІДОМЛЕННЯ ПРО СЕРЙОЗНІ ІНЦИДЕНТИ»

Науково-правове обґрунтування

Реєстр потрібний не як дозвільний формальний бар'єр, а як інфраструктура простежуваності. Без нього держава не має повної інформації про системи, які впливають на права осіб, а громадянин не знає, хто є постачальником і розгортувачем. Поєднання публічної та закритої частин дозволяє забезпечити відкритість і водночас захистити державну таємницю, кіберуразливості та оперативну інформацію. Єдиний порядок повідомлення про інциденти забезпечує швидке реагування й накопичення даних для перегляду регуляторних вимог.

ПРОЄКТ КАБІНЕТ МІНІСТРІВ УКРАЇНИ ПОСТАНОВА

Про Державний реєстр високоризикових систем штучного інтелекту та повідомлення про серйозні інциденти

- 1) Створити Державний реєстр високоризикових систем штучного інтелекту.
- 2) Визначити Міністерство цифрової трансформації держателем Реєстру, а державне підприємство, визначене Міністерством, - технічним адміністратором.
- 3) Затвердити Порядок ведення Реєстру та повідомлення про серйозні інциденти, що додається.
- 4) Ця постанова набирає чинності одночасно із Законом України «Про безпечне та відповідальне використання систем штучного інтелекту».

ПОРЯДОК

ведення Державного реєстру високоризикових систем штучного інтелекту та повідомлення про серйозні інциденти

Стаття 1. Структура Реєстру

1. Реєстр є інформаційно-комунікаційною системою, що складається з публічної та закритої частин.

2. Публічна частина доступна безоплатно у форматі відкритих даних. Закрита частина містить відомості з обмеженим доступом і доступна компетентному органу, Уповноваженому Верховної Ради України з прав людини, суду та іншим органам у межах повноважень.

Стаття 2. Суб'єкти подання відомостей

1. Відомості подають постачальник і розгортувач до початку введення системи в експлуатацію. За достовірність і своєчасність відповідає керівник або уповноважена посадова особа.

Стаття 3. Відомості публічної частини

1. Публічна частина містить найменування системи і суб'єктів, мету, категорію ризику, сферу використання, правову підставу, дату оцінки відповідності, стислий виклад оцінки впливу, контакт відповідального суб'єкта, відомості про зупинення або відкликання.

Стаття 4. Відомості закритої частини

1. Закрита частина може містити технічну документацію, архітектуру, відомості про уразливості, повний текст оцінки впливу, журнали інцидентів, відомості про системи оборони, розвідки, правоохоронної діяльності та критичної інфраструктури.

Стаття 5. Строки внесення та оновлення

1. Заява про реєстрацію подається не пізніше ніж за 20 робочих днів до початку використання. Зміни подаються протягом десяти робочих днів, а відомості про зупинення - невідкладно.

Стаття 6. Перевірка відомостей

1. Держатель здійснює формальну перевірку повноти. Внесення до Реєстру не замінює оцінку відповідності й не підтверджує законність системи.

Стаття 7. Попереднє повідомлення про інцидент

1. Попереднє повідомлення подається не пізніше 72 годин і містить опис події, систему, час, попередні наслідки, вжиті заходи та контакт відповідальної особи.

Стаття 8. Повний звіт

1. Повний звіт подається не пізніше 15 календарних днів і містить результати розслідування, причини, масштаб, категорії постраждалих осіб, оцінку шкоди, коригувальні заходи та план запобігання повторенню.

Стаття 9. Невідкладні заходи

1. У разі безпосередньої загрози суб'єкт негайно зупиняє систему або обмежує функції, повідомляє компетентний орган і осіб, яким необхідно вжити заходів для захисту.

Стаття 10. Оприлюднення інформації про інциденти

1. Компетентний орган оприлюднює знеособлену інформацію про серйозні інциденти, якщо це необхідно для попередження шкоди, без розкриття державної та комерційної таємниці.

Стаття 11. Взаємодія органів

1. Держатель забезпечує автоматизований обмін з органом нагляду, Уповноваженим, кібербезпековими та секторальними регуляторами.

Стаття 12. Захист інформації та аудит

1. Реєстр створюється з урахуванням вимог кібербезпеки, розмежування доступу, журналювання дій користувачів, резервного копіювання та щорічного незалежного аудиту.

ПОСТАНОВА КАБІНЕТУ МІНІСТРІВ УКРАЇНИ
«ПРО ЗАТВЕРДЖЕННЯ ПОРЯДКУ ФУНКЦІОНУВАННЯ
РЕГУЛЯТОРНОГО ЕКСПЕРИМЕНТАЛЬНОГО СЕРЕДОВИЩА ДЛЯ
СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ»

Науково-правове обґрунтування

Українська дорожня карта регулювання ШІ виходить із поступового bottom-up підходу. Регуляторне експериментальне середовище є виправданим лише тоді, коли воно не перетворюється на територію звільнення від закону. Його функція полягає у контрольованому тестуванні, підготовці документації, виявленні ризиків та формуванні доказової бази для майбутнього регулювання. Заборонені практики, права людини, захист персональних даних і відповідальність не можуть бути предметом дерегуляційного винятку.

ПРОЄКТ

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

Про затвердження Порядку функціонування регуляторного експериментального середовища для систем штучного інтелекту

- 1) Затвердити Порядок функціонування регуляторного експериментального середовища для систем штучного інтелекту, що додається.
- 2) Визначити Міністерство цифрової трансформації координатором експериментального середовища.
- 3) Ця постанова набирає чинності з дня її опублікування.

ПОРЯДОК

функціонування регуляторного експериментального середовища для систем штучного інтелекту

Стаття 1. Мета середовища

1. Метою є контрольоване випробування інноваційних систем, перевірка регуляторних вимог, підготовка розробників до оцінки відповідності та збирання даних для вдосконалення державної політики.

Стаття 2. Принципи

1. Середовище функціонує на засадах добровільності, строковості, пропорційності, конфіденційності, прозорості результатів, захисту прав людини та рівного доступу.

Стаття 3. Учасники

1. Учасниками можуть бути юридичні особи, фізичні особи - підприємці, наукові установи, заклади вищої освіти та органи публічної влади, які мають прототип або систему й план контрольованого випробування.

Стаття 4. Недопустимі проекти

1. Не допускаються проекти, що передбачають заборонені практики, повністю автономне застосування летальної сили, невибіркову біометричну ідентифікацію, приховане маніпулювання, незаконну обробку персональних даних або випробування на особах без належної правової підстави.

Стаття 5. Відбір

1. Заява оцінюється за інноваційністю, суспільною корисністю, готовністю до тестування, керованістю ризику, наявністю команди та неможливістю безпечного випробування поза середовищем.

Стаття 6. Індивідуальний план

1. До початку випробування затверджується план, що містить мету, строк не більше дванадцяти місяців, тестове середовище, категорії даних, учасників, ризики, контрольні показники, відповідальних осіб, умови зупинення та виходу.

Стаття 7. Гарантії прав

1. Участь не звільняє від Конституції України, законодавства про персональні дані, кібербезпеку, недискримінацію, захист споживачів та відшкодування шкоди. Випробування з реальними особами допускається лише за законною підставою, мінімізації даних і незалежного нагляду.

Стаття 8. Нагляд і звітність

1. Координатор та секторальний регулятор здійснюють регулярний моніторинг, можуть вимагати змін, призупинити або припинити випробування. Учасник подає проміжні й фінальний звіти.

Стаття 9. Результати

1. За результатами видається не дозвіл на ринок, а висновок щодо виконаних випробувань, виявлених ризиків, рекомендованих заходів та готовності до оцінки відповідності.

Стаття 10. Оприлюднення й використання знань

1. Координатор оприлюднює знеособлений щорічний звіт про типові ризики, ефективні заходи та пропозиції до законодавства, не розкриваючи комерційну таємницю.

ЗВЕДЕНЕ НАУКОВО-ПРАВОВЕ ОБҐРУНТУВАННЯ ПАКЕТА

1. Конституційна необхідність

Статті 3, 8, 19, 32, 34 і 55 Конституції України вимагають, щоб використання ІІІ органами влади було засноване на законі, не звужувало права, не усувало обов'язку мотивувати рішення й залишало особі ефективний засіб захисту. Алгоритмічна система не може створювати нову компетенцію або бути самостійним носієм владної волі. Запропоновані акти конкретизують ці вимоги через людський перегляд, право на пояснення, оскарження та контроль.

2. Євроінтеграційна сумісність

Пакет використовує ключову логіку AI Act - заборонені практики, високоризикові системи, вимоги до даних, документації, журналювання, людського контролю, моніторингу й інцидентів - однак адаптує її до української системи адміністративної процедури та публічного адміністрування. Рамкова конвенція Ради Європи врахована через оцінку впливу на права, процедурні гарантії, можливість оскарження, підзвітність і спеціальні заходи щодо неприйнятних практик.

3. Інституційна модель

Запропоновано мережеву модель: спеціалізований орган здійснює горизонтальний нагляд і координує Реєстр та інциденти; секторальні регулятори контролюють специфічні сфери; Уповноважений Верховної Ради України з прав людини забезпечує правозахисний і персонально-даний вимір; суд здійснює остаточний контроль законності. Така модель зменшує ризик дублювання і водночас не концентрує всі повноваження в одному органі без секторальної компетентності.

4. Фінансово-економічні наслідки

Створення органу нагляду, Реєстру та методичного забезпечення потребуватиме видатків державного бюджету. На першому етапі можливе використання наявної цифрової інфраструктури та кадрового ресурсу Мінцифри, секторальних регуляторів і Секретаріату Уповноваженого. Водночас повноцінний незалежний нагляд не може тривалий час функціонувати без окремого фінансування. Частина витрат може компенсуватися зборами за оцінку відповідності, участь у sandbox та адміністративними санкціями, однак фінансування регулятора не повинно залежати від обсягу накладених штрафів.

5. Антикорупційний ефект

Прозорість закупівель, реєстрація, автоматичне журналювання, визначення відповідальної посадової особи та право на аудит зменшують можливості прихованого впровадження систем, маніпулювання критеріями або

перекладання відповідальності на постачальника. Водночас автоматизація не повинна розглядатися як автоматичне усунення корупції: непрозора модель може відтворювати упереджені дані або приховувати дискреційні рішення. Саме тому обов'язковими є мотивування та людська відповідальність.

6. Ризики реалізації та способи їх мінімізації

Ризик	Засіб мінімізації
Надмірне регуляторне навантаження на інновації	пропорційні вимоги, типові документи, sandbox, підтримка МСП.
Формальне проведення оцінки впливу	незалежна експертиза, консультації, повноваження регулятора вимагати повторну оцінку.
Захоплення регулятора великими постачальниками	конфлікт-оф-інтерес правила, прозорі консультації, колегіальні експертні механізми.
Розкриття державної чи комерційної таємниці	закриті частини Реєстру, захищений доступ суду й контролюючих органів.
Використання безпекового винятку як загального звільнення	закритий, але обов'язковий аудит, журналювання, парламентський і судовий контроль.
Нестача фахівців	сертифіковані навчальні програми, міжвідомчі центри компетентності, залучення незалежних експертів.

7. Рекомендована послідовність упровадження

- 1) прийняття рамкового Закону та одночасного Закону про зміни до суміжних актів;
- 2) утворення компетентного органу і затвердження підзаконних процедур;
- 3) інвентаризація систем ІІІ органами публічної влади;
- 4) запуск Реєстру та проведення оцінок впливу для систем, що вже використовуються;
- 5) перехідний період для приватних постачальників і програми підтримки МСП;
- 6) регулярний перегляд переліку високоризикових систем, практики інцидентів і результатів sandbox;

7) секторальне доопрацювання законодавства про правоохоронну діяльність, правосуддя, медицину, освіту, оборону та критичну інфраструктуру.

ВИСНОВКИ

Запропонований пакет переводить висновки підрозділу 2.4 з рівня констатації прогалин у площину конкретного нормопроєктування. Його базова ідея полягає у тому, що спеціальний закон про ШІ повинен бути не ізольованим технологічним актом, а системоутворюючим елементом адміністративного та інформаційного права. Він має встановити горизонтальні правила, тоді як суміжні закони й підзаконні процедури повинні забезпечити реальне виконання цих правил у конкретному адміністративному провадженні, обробці даних, державному реєстрі, закупівлі та наглядовій діяльності.

Пріоритетними для першочергового прийняття є рамковий Закон, зміни до Закону «Про адміністративну процедуру» та законодавства про персональні дані, а також Порядок оцінки впливу. Без цих трьох складових реєстрація або добровільні рекомендації не забезпечать належного захисту прав. Реєстр, інцидентне звітування та sandbox мають функціонувати як інфраструктурні компоненти, які підсилюють, а не замінюють юридично обов'язкові гарантії.

НОРМАТИВНЕ, МІЖНАРОДНЕ ТА ДОКТРИНАЛЬНЕ ПІДґРУНТЯ

1. Конституція України від 28 червня 1996 року.
2. Про адміністративну процедуру : Закон України від 17.02.2022 № 2073-IX.
3. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI.
4. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI.
5. Про публічні електронні реєстри : Закон України від 18.11.2021 № 1907-IX.
6. Про публічні закупівлі : Закон України від 25.12.2015 № 922-VIII.
7. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р.
8. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки : розпорядження Кабінету Міністрів України від 09.05.2025 № 457-р.
9. Про План законопроектної роботи Верховної Ради України на 2026 рік : постанова Верховної Ради України від 10.02.2026 № 4774-IX.

10. Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року, що встановлює гармонізовані правила щодо штучного інтелекту (Artificial Intelligence Act).
11. Рамкова конвенція Ради Європи про штучний інтелект, права людини, демократію та верховенство права (CETS No. 225), відкрита для підписання 5 вересня 2024 року; підписана Україною 15 травня 2025 року.
12. Біла книга з регулювання штучного інтелекту в Україні. Міністерство цифрової трансформації України, 2024.
13. Права людини в епоху штучного інтелекту: виклики та правове регулювання : методичний матеріал. Офіс Омбудсмана України, Міністерство цифрової трансформації України, EU4DigitalUA, 2024.
14. Карчевський М. В., Куковинець Д. О. Використання технологій штучного інтелекту правоохоронними та судовими органами: світовий досвід та напрями розвитку національного законодавства. Питання боротьби зі злочинністю. 2023. № 46. С. 21–30.
15. Правові засади регулювання штучного інтелекту в Україні: сучасний стан та перспективи розвитку. Адміністративне право і процес. 2025. № 2.
16. Соколік В. Д., Пащенко Д. В., Швець С. А., Башанова Н. Є. Правове регулювання використання штучного інтелекту в публічному управлінні: виклики цифрової епохи. Науковий вісник Одеського національного економічного університету. 2025. № 4 (329). С. 30–36.
17. Фівкін П. М., Іващенко С. М. Правове регулювання використання штучного інтелекту у системі управління Збройних Сил України. Актуальні проблеми політики. 2026. Вип. 77.
18. Товкун Л. В., Леонович М. Ю. Правове регулювання штучного інтелекту: міжнародний досвід та перспективи впровадження для України. Юридичний науковий електронний журнал. 2024. № 12.