УДК 340.13:004.056.5(477)
DOI 10.32755/sjlaw.2025.03.058

Пузирний В. Ф.,
доктор юридичних наук, професор,
директор Навчально-наукового інституту права,
правоохоронної діяльності та психології,
Пенітенціарна академія України, м. Чернігів, Україна
ORCID: 0000-0002-5692-2990;
Захарчук І. В.,
старший викладач кафедри правознавства,
Північноукраїнський інститут ім. Героїв Крут
ПрАТ «ВНЗ «МАУП»,
м. Чернігів, Україна
ORCID: 0000-0001-6957-9004

ПРАВОВІ АСПЕКТИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ КІБЕРБЕЗПЕКИ: РЕГУЛЮВАННЯ ТА ЕТИЧНІ ДИЛЕМИ

Стаття присвячена аналізу правових аспектів застосування штучного інтелекту у сфері кібербезпеки. Розглянуто проблеми, пов'язані з визначенням відповідальності за дії автономних систем, забезпеченням прозорості алгоритмів та дотриманням етичних стандартів. Запропоновано шляхи вдосконалення правового регулювання ШІ в Україні з урахуванням сучасних викликів.

Ключові слова: *штучний інтелект, кібербезпека, інформаційне право, юридична відповідальність, автономні системи, етика штучного інтелекту, алгоритмічна прозорість, правове регулювання.*

Постановка проблеми. У сучасну епоху цифровізації стрімке впровадження штучного інтелекту у сферу кібербезпеки породжує як значні переваги, так і правові виклики. Штучний інтелект дозволяє виявляти та запобігати кіберзагрозам у режимі реального часу, автоматизувати реагування на атаки, проте водночас створює ризики зловживань, дискримінації, порушення прав людини та підвищує складність встановлення юридичної відповідальності. Особливо актуальним це питання стає для України в умовах кібергібридної війни, де штучний інтелект може відігравати як оборонну, так і наступальну роль. Відсутність чітких норм правового регулювання використання штучного інтелекту в кібербезпеці ставить перед юристами

та законодавцями низку нормативних і етичних дилем, які потребують комплексного дослідження.

Аналіз останніх досліджень і публікацій. В українському науково-правовому дискурсі тема правового регулювання використання штучного інтелекту, зокрема в контексті кібербезпеки, почала активно розвиватися лише в останні роки. Попри відсутність великої кількості комплексних досліджень, спостерігається зростання інтересу до цієї проблематики з боку правників, фахівців з інформаційного права, кібербезпеки та інтелектуальних технологій.

На сьогодні дослідженню питань, які пов'язані з технологіями штучного інтелекту, присвячені праці низки українських учених, серед яких Ю. В. Акулов [1], О. А. Баранов [2], І. М. Городиський [3], К. В. Єфремова [4], Т. Г. Каткова [5], М. В. Карчевський [6], О. О. Посикалюк [7], О. А. Теличко [8], К. В. Яровий [9] та інші. Їхні напрацювання переважно стосуються загальних підходів до правового регулювання новітніх цифрових технологій, зокрема концептуального осмислення місця штучного інтелекту в сучасній правовій системі.

Загалом більшість науковців погоджуються, що правове регулювання штучного інтелекту в Україні перебуває лише на етапі становлення, що й обумовлює високу актуальність подальших досліджень. Поки що в національному праві не існує єдиного нормативного підходу до кваліфікації дій систем штучного інтелекту, визначення відповідальних суб'єктів або механізмів контролю за прозорістю рішень, ухвалених алгоритмами та нейромережами. Така ситуація зумовлює необхідність більш глибокого теоретико-правового розроблення цієї сфери з урахуванням досвіду міжнародних організацій та європейського законодавства.

Мета статті. Метою статті є аналіз правових аспектів використання штучного інтелекту у сфері кібербезпеки, виявлення ключових проблем регулювання та етичних дилем, а також формулювання пропозицій щодо вдосконалення національного законодавства України у цій сфері.

Виклад основного матеріалу. Передусім потрібно дати визначення штучному інтелекту. Для вітчизняного законодав-

ства термін є новим, спеціальних нормативно-правових актів у цій сфері поки що немає, проте у 2020 році розпорядженням Кабінету Міністрів України було схвалено Концепцію розвитку штучного інтелекту в Україні, яка, однак, має декларативний характер. Проте в Концепції серед інших дефініцій також є визначення ШІ: «штучний інтелект – організована 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 ухвалення рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань» [10].

Аналогічне визначення дається і в Концепції Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року, яка була схвалена урядом в 2024 році [11]. Це дає змогу припустити, що подібне визначення можливо згодом буде використано під час створення спеціального закону щодо правового регулювання ШІ.

Однак таке визначення не можна вважати беззаперечним. Науковці намагаються дати більш доречне визначення. Наприклад, О. А. Баранов пропонує таке визначення штучного інтелекту, яке вбачається універсальним та таким, що може бути закріплене в подальшому в законодавстві: «штучний інтелект – це певна сукупність методів, способів, засобів та технологій, насамперед, комп'ютерних, що імітує (моделює) когнітивні функції, які мають критерії, характеристики та показники, еквівалентні критеріям, характеристикам і показникам відповідних когнітивних функцій людини» [12, с. 46].

Як уже зазначалось вище, на сьогодні в Україні відсутній спеціальний нормативно-правовий акт, який би регламентував використання ШІ. Законодавство у сфері кібербезпеки фактично обмежується Законом України «Про основні засади забезпечення кібербезпеки України» [13], проте в тексті закону ШІ не згадується жодного разу. Закон також не містить норм, що враховують особливості застосування автономних або самонавчальних систем.

Відповідно, можемо сформувати авторське визначення ШІ в кібербезпеці. ШІ у кібербезпеці – це сукупність технологій, які дозволяють автоматизувати процеси виявлення, реагування та запобігання кіберзагрозам шляхом аналізу великих масивів даних, поведінкових патернів та системної активності.

Однак поява таких технологій ставить перед правовою системою низку принципово нових викликів. Відсутність належного правового регулювання, невизначеність статусу рішень, ухвалених системами ШІ, а також складність у встановленні юридичної відповідальності за їх дії створюють серйозні проблеми як на національному, так і на міжнародному рівні. Особливо гостро ці питання постають у сфері кібербезпеки, де використання штучного інтелекту може мати як позитивний, так і ризикований ефект: від ефективної протидії кіберзагрозам до потенційного зловживання автономними системами.

Таким чином, потреба у формуванні правових засад застосування штучного інтелекту у сфері кібербезпеки, а також у визначенні меж допустимості використання таких технологій, включно з етичними обмеженнями, постає як надзвичайно актуальна. Ці аспекти і становлять основну проблематику цього дослідження, що потребує комплексного аналізу – як з точки зору чинного українського законодавства, так і з урахуванням зарубіжного досвіду.

У цьому контексті проблемними залишаються:

– відсутність критеріїв оцінювання ризику ШІ-рішень у безпекових системах;

– неврегульованість процедур аудиту алгоритмів;

– нерозробленість етичних стандартів для розробників і користувачів ШІ.

Ці виклики посилюються стрімким впровадженням інтелектуальних технологій у практику кіберзахисту. До основних прикладів застосування ШІ у кібербезпеці вже сьогодні належать:

– системи виявлення аномалій (anomaly detection systems), що автоматично фіксують підозрілу поведінку в мережах;

– автоматизовані фаєрволи, здатні адаптивно реагувати на нові загрози без участі людини;

– аналіз логів за допомогою алгоритмів машинного навчання для виявлення прихованих шаблонів атаки;

– предиктивна аналітика загроз (threat intelligence), що дозволяє прогнозувати потенційні атаки ще до їх фактичної реалізації;

– автоматизація процесів реагування на інциденти (так звані SOAR-системи – Security Orchestration, Automation and Response), що значно скорочує час від виявлення до реагування.

Таким чином, практичне застосування ШІ у сфері кібербезпеки вже відбувається, однак його правове забезпечення значною мірою відстає від технологічного розвитку. Це створює потенційні загрози як для прав людини, так і для стабільності цифрового середовища.

Застосування ШІ суттєво підвищує ефективність захисту інформаційних систем, оскільки дозволяє в реальному часі виявляти раніше невідомі загрози. Проте водночас використання ШІ може створити нові ризики, зокрема коли автономні системи ухвалюють рішення без людського контролю або коли сам ШІ стає об'єктом атак.

Усе це й обумовлює потребу у правовому, етичному та технологічному переосмисленні цієї сфери.

Правові проблеми, що виникають у процесі використання ШІ в кібербезпеці, можна умовно поділити на такі три основні групи:

1. Визначення відповідальності. У разі помилки алгоритму або недієвості системи ШІ складно встановити, хто несе юридичну відповідальність: розробник, користувач, адміністратор чи самостійно чинний алгоритм. В українському праві відсутнє поняття «електронного суб'єкта» чи «автономного агента», що ускладнює регулювання таких ситуацій.

2. Проблема автономності. ШІ-системи можуть самостійно змінювати свою поведінку через процес навчання. Це ставить під сумнів традиційні уявлення про контроль з боку людини. З одного боку, держава повинна забезпечити належний нагляд, з іншого – надмірне регулювання може стримувати інновації.

3. Прозорість і пояснюваність рішень. Часто алгоритми працюють як «чорні скриньки» (black boxes), де зрозуміти логіку ухвалення рішень неможливо навіть для розробників. Це створює загрозу як для прав людини, зокрема права на інформацію, оскільки особа може не знати, чому система ухвали-

ла те чи інше рішення, так і загалом для результатів тих або інших дій, які можуть бути вчинені ШІ.

До кожної із виділених груп проблем можна запропонувати низку пропозицій щодо їх розв'язання, правового та іншого характеру, враховуючи те, що сфера ШІ та кібербезпеки дуже тісно пов'язує право та технології.

Проблему невизначеності суб'єкта відповідальності у випадку помилкових або шкідливих рішень систем ШІ варто розв'язувати діями в таких напрямах:

– запровадження правового режиму «розширеної відповідальності» для розробників, користувачів або власників ШІ-систем. Аналогічні підходи вже застосовуються в Європейському Союзі в контексті «ризикових» технологій;

– розгляд концепції електронної (цифрової) правосуб'єктності, зокрема у вигляді тестової або обмеженої автономії (подібно до правосуб'єктності юридичних осіб);

– законодавче закріплення принципу презумпції відповідальності оператора системи ШІ з можливістю перекласти відповідальність за наявності доказів вини розробника або іншої сторони;

– розроблення окремої глави у Цивільному кодексі України, що стосується дій автономних інтелектуальних систем і відповідальності за шкоду, ними завдану.

Проблему відсутності чітких меж самостійності (автономності) ШІ та контролю за його діями слід розв'язувати таким чином:

– встановлювати обов'язкові критерії контролю за автономними системами, включно з вимогами до технічної можливості втручання людини на всіх етапах;

– запроваджувати «правила допустимого навчання», тобто алгоритми не повинні виходити за межі встановленого функціоналу без дозволу або підтвердження людини;

– надавати статус сертифікованого доступу до високорівневих ШІ-систем лише тим суб'єктам, які пройшли спеціалізовану підготовку та перевірку з боку державного органу або незалежної інституції;

– провести вдосконалення державного нагляду через створення окремого органу або підрозділу з питань контролю за системами ШІ в безпековому секторі.

Проблему відсутності доступу до логіки або обґрунтування рішень, які ухвалює ШІ, потрібно розв'язувати діями в таких напрямах:

– законодавче закріплення принципу пояснюваності рішень ШІ як обов'язкового елементу під час використання в критичних сферах, зокрема кібербезпеці;

– розроблення технічних та правових стандартів щодо аудиту алгоритмів, у тому числі з боку незалежних фахівців та державних структур;

– встановлення обов'язкової документації щодо функціонування системи ШІ, яка б фіксувала зміну алгоритмів, джерела навчальних даних, критерії ухвалення рішень тощо;

– заборона використання повністю непрозорих (недокументованих або незрозумілих) моделей у державному або безпековому секторі без спеціального дозволу.

Враховуючи наведені проблеми та пропозиції щодо їх можливого розв'язання, варто зробити таке:

– розробити спеціальний закон про штучний інтелект, який містив би базові поняття, принципи функціонування, права і обов'язки суб'єктів, а також положення щодо безпеки та кібербезпеки, етики та відповідальності;

– створити спеціальні регуляторні органи або підрозділи у вже наявних органах, які відповідатимуть за моніторинг впровадження і використання ШІ. Це можуть бути спеціалізовані департаменти в межах уже наявних органів, таких як Державна служба спеціального зв'язку та захисту інформації України, або ж нові структури, наприклад, Національне агентство з питань штучного інтелекту [14, с. 75];

– імплементувати рекомендації Європейського Союзу щодо регулювання ШІ, зокрема з урахуванням підходів, закладених в Artificial Intelligence Act, що регулює ШІ в Європейському Союзі [15];

– підготувати Етичний кодекс розробника і користувача ШІ в Україні на основі міжнародних стандартів і з особливим ак-

центом на недопущенні дискримінації, порушення приватності та прав людини.

Етичні питання є невід'ємною складовою дискусії про правове регулювання ШІ. У сфері кібербезпеки найважливішими з них є:

– конфлікт між безпекою та приватністю. Системи ШІ для виявлення загроз можуть порушувати право на приватність, якщо вони збирають надмірну кількість персональних даних або аналізують комунікації користувачів;

– упередженість алгоритмів. Алгоритмічні системи можуть відтворювати або навіть посилювати соціальні упередження. Наприклад, виявлення «підозрілої» активності може базуватися на стереотипах;

– невизначеність щодо автономного ухвалення рішень. Наявність ШІ в процесах оборони від кібератак може спричинити дії без попереднього людського втручання, що порушує принципи пропорційності та обґрунтованості втручання в інформаційні права;

– можливості використання ШІ для наступальних цілей. Український правовий простір наразі не має чітких обмежень щодо застосування ШІ в наступальних кібервтручаннях, що може порушувати міжнародні норми щодо ведення гібридної війни.

Етичні принципи повинні бути закладені на рівні стратегічних документів, а не лише залишатися декларативними. Вони мають бути адаптовані до українського правового середовища та міститись у майбутніх нормативних актах, які будуть ухвалені для правового регулювання ШІ.

Висновки. Використання штучного інтелекту у сфері кібербезпеки є неминучим етапом цифрової трансформації, який нині відбувається у всьому світі та має як позитивні аспекти, так і загрози правового характеру. Аналіз свідчить, що наявні нормативні підходи не встигають за темпами розвитку технологій, а етичні питання залишаються відкритими. Українське законодавство потребує адаптації до нових реалій з урахуванням міжнародного досвіду, зокрема практик Європейського Союзу щодо прозорості, підзвітності та ризик-орієнтованого регулювання. Удосконалення нормативної бази має відбуватися із залученням міждисциплінарних підходів, які враховують як юридичні, так і технологічні, філософські аспекти розвитку штучного інтелекту.

Список використаних джерел

1. Акулов Ю. В. Принципи державного управління у сфері цифрових інновацій та AI-розробок. *Академічні візії*. 2024. № 36. С. 1–7.

2. Баранов О. А. Правові аспекти національних стратегій розвитку штучного інтелекту. *Юридична Україна*. 2019. № 7. С. 21–38.

3. Городиський І. М. Вплив AI Act ЄС на глобальне регулювання штучного інтелекту. *Право та інноваційне суспільство*. 2023. № 2 (15). С. 53–58.

4. Єфремова К. В. Правове регулювання штучного інтелекту в епоху цифрової економіки. *Приватне право і підприємництво*. 2020. Вип. 20. С. 142–147.

5. Каткова Т. Г. Штучний інтелект в Україні: правові аспекти. *Право і суспільство*. 2020. № 6. С. 46–57.

6. 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. 32–36.

7. Посикалюк О. О. Штучний інтелект: пошук правових конструкцій введення у цивільний обіг. *Право України*. 2022. № 6. С. 139–148.

8. 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. 310–313. URL: http://www.lsej.org.ua/2_2021/77.pdf (дата звернення: 13.06.2025).

9. Яровий К. В. Штучний інтелект як інструмент протидії злочинності. *Юридичний вісник*. 2024. № 2 С. 68–76.

10. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020%D1%80#Text (дата звернення: 10.06.2025).

11. 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 13.04.2024 № 320-р. URL: https://zakon.rada.gov.ua/laws/show/320-2024-%D1%80#Text (дата звернення: 10.06.2025).

12. Баранов О. А. Визначення терміна «штучний інтелект». *Інформація і право*. 2023. № 1 (44). С. 32–49.

13. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

14. Boldyreva V., Zakharchuk I. Current state and prospects for improving the legal regulation of information technology and artificial intelligence as an element of improving the quality of life in Ukraine. *Exploring Quality of Life Amid Global and Local Transformations: monograph* / Tadeusz Pokusa, Tetyana Nestorenko, Dominika Kalita (eds.), Publishing House of the Academy of Applied Sciences – Academy of Management and Administration in Opole. 2024. Part 1.7. P. 70–76.

15. Artificial Intelligence Act, Regulation № 2024/1689, European Union. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (дата звернення: 10.06.2025).

Puzyrnyi V.,
Doctor of Sciences Law, Professor, Director of the Educational and Research Institute of Law, Law-Enforcement and Psychology, Penitentiary Academy of Ukraine, Chernihiv, Ukraine
ORCID: 0000-0002-5692-2990;

Zakharchuk I.,
Senior Lecturer of the Department of Law, North Ukrainian Institute named after Heroes of Kruty, PJSC "IAPM", Chernihiv, Ukraine
ORCID: 0000-0001-6957-9004

LEGAL ASPECTS OF USING ARTIFICIAL INTELLIGENCE IN CYBERSECURITY: REGULATION AND ETHICAL DILEMMAS

The article is devoted to the analysis of legal aspects of artificial intelligence (AI) implementation in the field of cybersecurity. In the context of rapid technological development, AI has become an integral tool in identifying and countering cyber threats through anomaly detection systems, automated firewalls, machine learning–based log analysis, threat intelligence, and incident response automation. However, the deployment of such technologies reveals a number of unresolved legal and ethical dilemmas that require urgent regulatory attention.

The research identifies three core groups of legal issues: determination of liability, challenges of system autonomy, and the transparency of AI decision-making. The absence of a legal framework for assigning responsibility in cases where AI malfunctions or acts autonomously complicates the process of legal evaluation. The article emphasizes that Ukrainian legislation lacks a definition of "autonomous

agent" or "electronic subject," making it difficult to apply traditional norms of civil and administrative law.

The problem of autonomy is particularly relevant, as modern AI systems can modify their behavior independently through machine learning processes. This raises questions about human oversight and the balance between innovation and regulatory control. Additionally, many AI systems function as "black boxes," making it difficult – even for developers – to understand the logic behind certain decisions. This threatens the protection of human rights, including the right to information and due process.

To address these challenges, the article proposes several legal and policy measures, such as the introduction of a dedicated law on AI, adoption of explainable AI principles, implementation of algorithmic audit standards, and development of ethical guidelines for AI developers and users.

Key words: *artificial intelligence, cybersecurity, information law, legal responsibility, autonomous systems, artificial intelligence ethics, algorithmic transparency, legal regulation.*

References

1. Akulov, Y. V. (2024), "Principles of public administration in the field of digital innovations and AI developments", *Academic visions*, № 36, pp. 1–7.

2. Baranov, O. A. (2019), "Legal aspects of national strategies for the development of artificial intelligence", *Yurydychna Ukraina*, № 7, pp. 21–38.

3. Gorodissky, I. M. (2023), "The impact of the EU AI Act on the global regulation of artificial intelligence", *Law and innovative society*, № 2 (15), pp. 53–58.

4. Efremova, K. V. (2020), "Legal regulation of artificial intelligence in the digital economy", *Private Law and Entrepreneurship*, Issue 20, pp. 142–147.

5. Katkova, T. G. (2020), "Artificial Intelligence in Ukraine: Legal Aspects", *Law and Society*, № 6, pp. 46–57.

6. Karchevskyi, M. V. (2020), "Artificial intelligence and combating crime", *The use of artificial intelligence technologies in combating crime* : materials of the scientific and practical online seminar (Kharkiv, 5 November 2020), Pravo, Kharkiv, pp. 32–36.

7. Posykaliuk, O. O. (2022), "Artificial Intelligence: Search for Legal Constructions of Introduction into Civil Circulation", *Law of Ukraine*, № 6, pp. 139–148.

8. Telychko, O. A., Rekun, V. A., Chabanenko, Y. S. (2021), "Problems of definition and regulatory consolidation of the concept of "artificial intelligence" in the legislation of foreign countries and Ukraine", *Legal scientific electronic journal*, № 2, pp. 310–313, available at: http://www.lsej.org.ua/2_2021/77.pdf (accessed 13 June 2025).

9. Yarovyi, K. V. (2024), "Artificial intelligence as a tool for combating crime", *The Legal Bulletin*, № 2, pp. 68–76.

10. Ukraine (2020), *On Approval of the Concept of Artificial Intelligence Development in Ukraine* : Order, Conception, Cabinet of Ministers of Ukraine, Kyiv, available at: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (accessed 10 June 2025).

11. Ukraine (2024), *On Approval of the Concept of the State Targeted Scientific and Technical Program for the Use of Artificial Intelligence Technologies in Priority Sectors of the Economy for the Period up to 2026* : Order, Conception, Cabinet of Ministers of Ukraine, Kyiv, available at: https://zakon.rada.gov.ua/laws/show/320-2024-%D1%80#Text (accessed 10 June 2025).

12. Baranov, O. A. (2023), "Definition of the term „artificial intelligence”", *Information and law*, No 1 (44), pp. 32–49.

13. Ukraine (2017), *On the Basic Principles of Cybersecurity in Ukraine* : Law of Ukraine, Verkhovna Rada of Ukraine, Kyiv.

14. Boldyreva, V., Zakharchuk, I. (2024), "Current state and prospects for improving the legal regulation of information technology and artificial intelligence as an element of improving the quality of life in Ukraine", in Pokusa, T., Nestorenko, T., Kalita, D. (Eds.), *Exploring Quality of Life Amid Global and Local Transformations* : monograph, Publishing House of the Academy of Applied Sciences – Academy of Management and Administration in Opole, pp. 70–76.

15. European Union (2024), *Artificial Intelligence Act* : Regulation, European Parliament and Council, Brussels, available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (accessed 10 June 2025).