

Бегун А.В.,

к.е.н., професор кафедри системного аналізу та кібербезпеки,
КНЕУ імені Вадима Гетьмана

Старіна Е. І.,

студентка 4 курсу за освітньо-професійною програмою
«Системний аналіз»,
КНЕУ імені Вадима Гетьмана

Biehun A.V.,

PhD in Economics, professor of the department of system analysis and cyber security, KNEU named after Vadym Hetman

Starina E.I.,

4th-year student of educational professional program «System Analysis»,
KNEU named after Vadym Hetman

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОГО ПРАВА В КОНТЕКСТІ ШТУЧНОГО ІНТЕЛЕКТУ

FEATURES OF INFORMATION LAW IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE

Анотація. Велика кількість письмової, графічної, аудіо- та відеоінформації поширюється завдяки широкій доступності недорогих і безкоштовних інструментів, що генерують штучний інтелект. Значна частина контенту, створеного системами штучного інтелекту, може бути нешкідливою або навіть корисною для деяких аудиторій. Проте ці платформи також сприяють поширенню екстремально небезпечних матеріалів. Наприклад, провокаційні, небезпечні, упереджені, неточні або оманливі матеріали можуть і будуть поширюватися за допомогою генеративних методів штучного інтелекту. В статті викладено аналіз думок фахівців і науковців на існуючі аспекти взаємодії інформаційного права та штучного інтелекту, виявлення майбутніх етичних проблем та викликів, пошук раціональних правових рішень. Життєво необхідним є ефективне законодавство, яке б забезпечувало захист прав і свобод людини, знижуючи при цьому ризики, пов'язані з використанням штучного інтелекту. Закон про застосування штучного інтелекту повинен мати кілька ключових компонентів, які ґрунтуються на чітко визначених критеріях.

Ключові слова: інформаційне право; штучний інтелект; безпека даних; етика; законність; загрози; зловживання.

Abstract. A large amount of written, graphic, audio and video information is distributed thanks to the wide availability of inexpensive and free tools that generate artificial intelligence. Much of the content generated by artificial intelligence systems may be harmless or even useful to some audiences. However, these platforms also facilitate the distribution of extremely dangerous material. For example, provocative, dangerous, biased, inaccurate or misleading material can and will be disseminated using generative artificial intelligence techniques. The article presents an analysis of the opinions of

specialists and scientists on the existing aspects of the interaction of information law and artificial intelligence, the identification of future ethical problems and challenges, and the search for rational legal solutions. Effective legislation that would ensure the protection of human rights and freedoms while reducing the risks associated with the use of artificial intelligence is vital. The law on the application of artificial intelligence should have several key components, which are based on clearly defined criteria.

Keywords: *information law; Artificial Intelligence; data security; ethics; legality; threats; abuse.*

Вступ. Штучний інтелект (ШІ), як подія, став невід’ємним компонентом повсякденного життя трансформації відносини людини з ІТ- технологіями. ШІ надає безмежний потенціал, оскільки його функціонал пронизує багато аспектів життя: від інтелектуальних персональних помічників до рішень проблем автоматизації бізнес-процесів. Але впровадження штучного інтелекту також створює нові проблеми і занепокоєння, зокрема, у сферах інформаційного права, безпеки даних, етики та законності.

З огляду на цей факт виникає необхідність у визначенні сучасних особливостей інформаційного права в процесах застосування штучного інтелекту. Незважаючи на незаперечні переваги, які існують і продовжують з’являтися у зв’язку з впровадженням ШІ, у середовищі застосування останнього почали виникати нові загрози та небезпеки. Ці проблеми включають: різноманітні можливості зловживань, створення оманливих «глибоко підроблених» аудіо записів, вплив на зайнятість (наприклад, «робозвільнення»), моральні проблеми, пов’язані з втручанням в приватне життя тощо. Тому залучення інформаційного законодавства, в якому правила захисту, обміну та використання даних, безумовно має важливе значення для забезпечення того, щоб ШІ використовувався морально і відповідально.

Мета статті полягає у системному аналізі сучасного застосування інформаційного права в контексті штучного інтелекту і формування рекомендацій нормативно-правових положень, які регулюють захист потоків інформації ШІ.

Аналіз останніх досліджень і публікацій. У рамках дискусії навколо ШІ ця публікація висвітлює погляди відомих фахівців та науковців, які присвятили значну частину своєї академічної кар’єри цій галузі досліджень. У своїй науковій книзі «Регулювання технологій: ризик-орієнтовані підходи до управління штучним інтелектом» [1] один з відомих експертів досліджує проблеми регулювання ШІ та безпеки використання цієї передової технології. Основний аргумент автора полягає в тому, що штуч-

ний інтелект необхідно регулювати, звертаючи особливу увагу на ризики, які можуть виникнути. Покращення міжнародної співпраці між країнами та зацікавленими сторонами, а також створення методів регулювання ШІ на основі оцінки ризиків можуть бути використані для вирішення цього питання і гарантувати ефективне та дієве регулювання ШІ.

Ризики та труднощі використання ШІ в державному секторі висвітлює Ібрагім Хасан у своїй статті «GDPR та ШІ: повстання машин» [2]. Він звертає увагу на проблеми, які пов'язані зі зловживанням ШІ, ризиками при працевлаштуванні, етичні питання та небезпеку необережного використання ШІ. Загалом, результати дослідження свідчать про те, що хоч штучний інтелект має багато переваг, все рівно необхідне суворе регулювання та нагляд, щоб запобігти негативному впливу на права і свободи користувачів.

Важливо звернути увагу також на погляди українських фахівців і дослідників щодо ШІ і як ця технологія впливає на інформаційне право.

Оскільки інформаційні технології стали невід'ємною частиною нашого повсякденного життя, автор К.Е. Ляпін [3] розглядає важливість захисту інформації в сучасному цифровому середовищі. На його переконання, традиційні методи захисту інформації стають недостатніми у зв'язку зі збільшенням кількості підключених пристроїв та зростанням кіберзагроз. Через це автор наголошує на необхідності пошуку нових, комплексних та ефективних методів захисту інформації в цифрову епоху. К. Е. Ляпін розглядає два основні способи створення стратегій інформаційної безпеки в організаціях для вирішення цих проблем: перший зосереджений на дотриманні законодавчих вимог і норм, тоді як другий використовує методи і моделі для комплексної оптимізації системи. Кожна з цих стратегій має свої переваги й недоліки, і унікальні якості організації визначатимуть, яка стратегія буде більш вдала.

Невід'ємною складовою дослідження є думка видатного вченого О. А. Баранова. Він розглядає стратегії, що передбачають максимальне використання правових механізмів, наявних у традиційній правовій системі, з одночасним внесенням необхідних удосконалень або розробкою нових правових положень, щоб мінімізувати невизначеність і пов'язані з нею витрати на впровадження правового регулювання, орієнтованого на використання штучного інтелекту і роботів. [4]

Спираючись на думку як зарубіжних, так і вітчизняних вчених, можемо зробити висновок, що існує загальновизнана про-

блема в сфері розвитку та регулювання штучного інтелекту й інформаційного права. Така проблема полягає у потребі створення ефективних механізмів регулювання, які б забезпечували баланс між розвитком цієї технології та захистом прав і свобод користувачів.

Виклад основного матеріалу дослідження. Наступна частина цієї статті присвячена інтеграції штучного інтелекту та інформаційного права.

Коли інформація про продукти штучного інтелекту не є загальнодоступною, це може призвести до непередбачуваних наслідків і створити проблеми для контролю цієї технології. Щоб повністю оцінити ризики та вплив штучного інтелекту, органи влади та громадськість повинні мати доступ до цієї інформації. Необмежений доступ до цих даних сприяє відкритості, раціональному управлінню та участі громадськості в законодавстві у сфері ШІ [5].

Технологічний прогрес у сфері ШІ вносить значні зміни в традиційну інформаційну екосистему й інформаційне право. Одним з аспектів впливу штучного інтелекту на інформаційне право є зростання кількості випадків несанкціонованого використання технологій клонування голосу. Нещодавно компанія ElevenLabs, що спеціалізується на генерації голосу за допомогою ШІ [6], повідомила про зростання випадків зловживання їхнім програмним забезпеченням. Згідно з повідомленнями, зловмисники використовували програмне забезпечення ElevenLabs для створення підроблених записів голосів відомих людей, зокрема Емми Вотсон і Джо Рогана, з метою поширення расистських, трансфобних і насильницьких коментарів. Це має значний вплив на інформаційне право, оскільки порушує приватне життя та репутацію людей і тягне за собою юридичні наслідки.

Ще одним ключовим моментом, що впливає на інформаційне право є ризики для приватності та захисту даних. Вони можуть виникати через широке використання штучного інтелекту, особливо коли створюються бази даних, які містять фотографії та персональні дані про конкретних людей. Наприклад, у травні 2022 року британський Офіс комісара з питань інформації оштрафував компанію [7] Clearview AI Inc. за порушення Загального регламенту про захист даних (GDPR), щодо збору та використання даних про обличчя. Ще одним прикладом порушення конфіденційності є використання та обробка персональних даних державними організаціями та комерційними компаніями, що використовують системи штучного інтелекту. За словами професорів Даніель Ци-

трон та Даніеля Солове, «порушення автономії» [8] відбувається тоді, коли державна установа використовує ваші персональні дані без вашої згоди, тим самим обмежуючи ваш контроль над власними даними. Це призводить до того, що ви втрачаєте можливість вирішувати, як використовувати ваші дані, а приватні підприємники не можуть отримати доступ до ваших даних або використовувати інформацію з комерційних баз даних, щоб сформувати неправильне враження про вас, тим самим порушуючи ваші права на приватність. Регулювання ШІ в цій сфері є вкрай важливим, оскільки ця проблема пов'язана із захистом персональних даних.

Це підводить нас до повчального прикладу кампанії «ShareWithCare» [9], яка досить наочно демонструє, як штучний інтелект може бути використаний для модифікації приватних даних. Ключовим елементом проекту є підроблене відео під назвою «Послання від Елли». Цей матеріал слугує попередженням про наслідки необережного розміщення дитячих даних в Інтернеті за допомогою штучного інтелекту і ще раз підтверджує той факт, що з розвитком технологій зростає і моральна потреба захищати цифрову приватність, відповідаючи таким чином вимогам інформаційного права.

Безперечно, інший аспект впливу ШІ на інформаційне право є питання про те, наскільки достовірними і точними можуть бути судження систем ШІ. Оскільки системи штучного інтелекту базуються на вивченні великих обсягів даних, вони можуть прогнозувати та робити узагальнення щодо людської поведінки. Однак, ці узагальнення є лише середньостатистичними і не завжди враховують індивідуальні особливості кожної людини. [10]

Коли ШІ застосовують для прийняття рішень щодо окремих осіб, які можуть виходити за рамки стандартних статистичних показників, існує ризик прийняття неправильних рішень і потенційного порушення прав цих осіб, особливо коли системи ШІ покладаються на дані зі значними історичними упередженнями та дискримінацією.

Загалом, вплив штучного інтелекту на інформаційне право вимагає створення законів та обмежень для захисту прав громадян та особистої інформації в цифровій сфері. Для справедливого та етичного використання цієї технології необхідно встановити баланс між можливостями штучного інтелекту та правами і свободами людей.

Для вирішення проблем, які виникають у зв'язку з використанням штучного інтелекту, поточна концепція інформаційного

права в Європейському Союзі та інших юрисдикціях потребує ретельного дослідження і оновлення законодавства у разі потреби.

Так, для захисту прав споживачів і конфіденційності у віртуальному світі велике значення має Загальний регламент захисту даних (GDPR) [11], який містить положення про використання штучного інтелекту. Одним із основоположних принципів GDPR є обов'язковість отримання індивідуальної згоди на обробку персональних даних. Це означає, що перш ніж збирати та використовувати дані користувачів, розробники ШІ повинні отримати їх дозвіл. GDPR також встановлює правила щодо обмежень, прозорості та законності обробки даних. Звідси виникає запит, що для збору та обробки даних розробники штучного інтелекту повинні мати законну правову підставу інформувати користувачів про причини обробки та збирати й аналізувати дані лише для таких цілей [2]. Італія обмежила доступ до широко відомого чату GPT [12] через порушення в сфері обробки персональних даних. Зокрема, італійський регулятор зазначає, що не існує жодних правових підстав, які б виправдовували масовий збір та зберігання персональних даних з метою «навчання» алгоритмів, що складають основу платформи.

Друге питання яке розглядається у цій статті це визнання авторства, коли системи штучного інтелекту роблять творчий внесок. Чи доречно, щоб системи штучного інтелекту володіли авторськими правами, і який вплив це матиме на чинне законодавство про авторське право?

Розглянемо Рішення Управління з авторських прав США, щодо штучного інтелекту [13]. Воно однозначно має важливі наслідки для інформаційного права та управління інтелектуальною власністю. У березні 2023 року Бюро опублікувало нові рекомендації, в яких зазначено, що авторське право застосовується лише до творів, які є результатом людської винахідливості. Згідно цього рішення, авторське право застосовується лише до творів, що мають суттєвий внесок людини, і не розповсюджується на твори, створені виключно ШІ, без активної її участі.

Європейський Союз активно працює над законодавством щодо штучного інтелекту, розподіляючи системи генерації контенту на різні категорії залежно від рівня ризику та впливу на права людини. Відповідно до ступеня небезпеки, яку вони становлять для прав і здоров'я людини, запропоноване законодавство розділяє генеративні системи — в тому числі ті, що створюють текст, зображення, аудіо- та медіафайли — на різні категорії. За цим за-

коном, чим вищий ризик використання ШІ у конкретній галузі, тим більше обов’язків і вимог накладається на ці системи. Зокрема, застосування ШІ в охороні громадського порядку, життєво важливих об’єктах інфраструктури, освіти та управлінні міграційними процесами є сферами підвищеного ризику (див. табл.1.). Генеративні системи, такі як ChatGPT і DALL-E, повинні інформувати користувачів про те, що матеріал, який вони надали, був створений комп’ютером, а не людиною [14].

Таблиця 1

**БІЛА КНИГА КОМІСІЇ ЩОДО ШТУЧНОГО ІНТЕЛЕКТУ —
ЗАПРОПОНОВАНІ ОBOB’ЯЗКОВІ ВИМОГИ
ДО ШТУЧНОГО ІНТЕЛЕКТУ «ВИСОКОГО РИЗИКУ»**

Ключові функції	Приклади
Навчальні дані	Вимоги, що забезпечують навчання систем ШІ на достатньо широких наборах даних
Ведення даних і записів	Зберігайте «точні записи щодо набору даних, які використовуються для навчання та тестування систем ШІ»
Публічна інформація	«Громадяни повинні бути чітко поінформовані, коли вони взаємодіють із системою ШІ, а не з людиною»
Надійність і точність	«Вимоги, що забезпечують відтворюваність результатів»
Людський нагляд	«Моніторинг системи штучного інтелекту під час роботи та можливість втручання в режимі реального часу та деактивації»
Спеціальні правила для деяких випадків використання ШІ	Наприклад: дистанційна біометрична ідентифікація

Українське законодавство, з іншого боку, змінило підходи до авторських прав на твори ШІ з введенням Закону «Про авторське право і суміжні права» [15] в силу на початок 2023 року. Що стосується регулювання штучного інтелекту (ШІ) в інформаційному праві, то ці зміни мають вирішальне значення. Фундаментальним елементом цього законодавства є стаття 33 Закону України, в якій представлено поняття «неоригінальні об’єкти». Українське законодавство визнає «неоригінальні об’єкти», створені штучним інтелектом, творами, що охороняються авторським правом; тим не менш, авторське право на ці твори належить особі, яка розро-

била комп'ютерну програму або встановила критерії для їх розробки. Це підкреслює цінність людського внеску у творчий процес і надає творам, створеним штучним інтелектом в Україні, правову легітимність [14].

У сучасному світі можливість регулювання ШІ в інформаційному праві стає все більш важливою проблемою. Чотири з десяти респондентів опитування Edelman [16] щодо довіри до технологічної індустрії заявили про необхідність посилення регулювання у сфері ШІ, і більшість з них мають сумніви щодо потенційних переваг цієї технології. Цей показник розриву між технологічним прогресом і довірою до нього зумовлений умовами сьогодення. Зокрема, нормативно-правова база, що регулює технологію ШІ, історично була слабкою і неоднозначною порівняно зі швидкими і широкомасштабними змінами, які ШІ спричиняє в контексті сучасного світу [17]. У відповідь на цю проблему сучасні національні та міжнародні уряди й організації працюють над створенням законодавства щодо ШІ, яке встановлюватиме норми у відповідних сферах. Національні та міжнародні зусилля є одними з основних інструментів, на основі чого вивчається тема регулювання ШІ. Широко поширеною є думка, що фрагментарної правової бази недостатньо для належного контролю над штучним інтелектом (ШІ), зважаючи на глобальне поширення технології та її вплив на корпоративне середовище. Довіра громадськості до ШІ зростатиме з впровадженням міжнародних законів, які контролюватимуть його використання для загального блага, забезпечуючи при цьому баланс між інноваціями та правовим наглядом.

Висновки. Оскільки штучний інтелект (ШІ) дедалі більше охоплює суспільство і повсякденне життя, регулювання ШІ стає все більш важливою і нагальною проблемою. Життєво необхідним є ефективне законодавство, яке б забезпечувало захист прав і свобод людини, знижуючи при цьому ризики, пов'язані з використанням ШІ. Звідси випливає, що закон про ШІ повинен мати кілька ключових компонентів, які ґрунтуються на перерахованих вище критеріях.

На наш погляд, слід заборонити використання технологій, які порушують базові права людини, наприклад, біометричний масовий доступ до інформації. По-друге, мають бути встановлені норми, які чітко контролюють публічне розкриття інформації про продукти штучного інтелекту та забезпечують необмежений доступ до цих знань. По-третє, на законодавчому рівні компанії та уряди повинні нести відповідальність за будь-які проблеми, які можуть виникнути в результаті застосування штучного інтелекту.

По-четверте, необхідно створити неупереджені регуляторні органи, які гарантуватимуть дотримання норм.

Нарешті, права і свободи людини повинні бути захищені законами, які контролюють ШІ, так само як і права найбільш незахищених груп населення. Дотримуючись цих принципів, суспільство зможе використовувати ШІ на користь, зберігаючи цінності свободи і справедливості.

Бібліографічні посилання

1. Singh, N. (2021, June 23). Technology Regulation: Risk-based approaches to Artificial Intelligence governance, Part II. The CCG Blog. <https://ccgnludelh.wordpress.com/2021/06/23/technology-regulation-risk-based-approaches-to-artificial-intelligence-governance-part-ii/>

2. GDPR and AI: The Rise of the Machines. (2023, February 3). Local Government Lawyer. <https://www.localgovernmentlawyer.co.uk/information-law/344-information-law-features/52845-gdpr-and-ai-the-rise-of-the-machines>

3. Ляпін, К. Е. (n.d.). ВИКЛИКИ ТА МОЖЛИВОСТІ СУЧАСНОСТІ: КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ. Аналітично-порівняльне Правознавство. <https://doi.org/10.24144/2788-6018.2023.04.43>

4. Баранов О.А. Правові аспекти національних стратегій розвитку штучного інтелекту // Юридична Україна. — № 7. — 2019. — С. 21-38.

5. Galaski, J. (2021, September 8). AI Regulation: Present Situation And Future Possibilities. Liberties.eu. <https://www.liberties.eu/en/stories/ai-regulation/43740>

6. Cox, J. (2023, January 30). AI-Generated Voice Firm Clamps Down After 4chan Makes Celebrity Voices for Abuse. Wwww.vice.com. <https://www.vice.com/en/article/dy7mww/ai-voice-firm-4chan-celebrity-voices-emma-watson-joe-rogan-elevenlabs>

7. ICO Fines «World's Largest Facial Network.» (2022, May 25). Your Front Page for Information Governance News. <https://actnowtraining.blog/2022/05/25/ico-fines-worlds-largest-facial-network/>

8. Fergusson. (2023, September). How AI Companies Have Taken Over Government Decision-Making. In Epic. epic. Retrieved November 7, 2023, from <https://epic.org/wp-content/uploads/2023/09/FINAL-EPIC-Outsourced-Automated-Report-w-Appendix-Updated-9.26.23.pdf>

9. AG, D. T. (2023, September 4). #ShareWithCare: Photos of children require special protection online. Wwww.telekom.com. <https://www.telekom.com/en/media/media-information/archive/sharewithcare-children-s-images-deserve-protection-on-the-net-1048376>

10. Fergusson, G. (2023). How AI Companies Have Taken Over Government Decision-Making. <https://epic.org/wp-content/uploads/2023/09/FINAL-EPIC-Outsourced-Automated-Report-w-Appendix-Updated-9.26.23.pdf>

11. Intersoft Consulting. (2013). General Data Protection Regulation (GDPR) . General Data Protection Regulation (GDPR). <https://gdpr-info.eu>
12. Гаращенко, Р. (2023, March 31). Італія першою в Європі заблокувала ChatGPT: У чому річ. Uworld.news. <https://uworld.news/news/italia-persha-ievropeiska-kraina-iaka-1002011.html>
13. U.S. Copyright Office. (2023, March 16). NewsNet Issue 1004 | U.S. Copyright Office. Wwww.copyright.gov. <https://www.copyright.gov/newsnet/2023/1004.html>
14. European Parliament. (2023, August 6). EU AI Act: First Regulation on Artificial Intelligence | News | European Parliament. Wwww.europarl.europa.eu. <https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>
15. Про авторське право і суміжні права. (n.d.). Офіційний вебпортал парламенту України. <https://zakon.rada.gov.ua/laws/show/2811-20#Text>
16. 2022 Special Report: Trust in Technology. (n.d.). Edelman. <https://www.edelman.com/trust/2022-trust-barometer/special-report-trust-technology>
17. The Future of Artificial Intelligence Regulation. (2022, January 13). Wwww.telusinternational.com. <https://www.telusinternational.com/insights/ai-data/article/the-future-of-ai-regulation>

Статтю подано до редакції: 18.11.2023