

[https://doi.org/10.32689/2617-2224-2020-3\(23\)-151-163](https://doi.org/10.32689/2617-2224-2020-3(23)-151-163)

Лисенко Сергій Олексійович,
доктор юридичних наук, професор, ПрАТ
“Вищий навчальний заклад “Міжрегіо-
нальна Академія управління персона-
лом”, завідувач кафедри правознавства
Северодонецького інституту, м. Київ,
Україна, +380675740981, sl-bezpeka@iapm.edu.ua,
<https://orcid.org/0000-0002-7050-5536>

Лысенко Сергей Алексеевич,
доктор юридических наук, профессор,
ЧАО “Высшее учебное заведение “Межре-
гиональная Академия управления персо-
налом”, заведующий кафедрой правоведе-
ния Северодонецкого института, г. Киев,
Украина, +380675740981, sl-bezpeka@iapm.edu.ua,
<https://orcid.org/0000-0002-7050-5536>



Lysenko Serhii Alexevich,
Doctor of Law, Professor, PJSC “Higher Education Institution “Interregional Academy of
Personnel Management”, Head of the department of Jurisprudence of Severodonetsk Insti-
tute, Kyiv, Ukraine, +380675740981, sl-bezpeka@iapm.edu.ua,
<https://orcid.org/0000-0002-7050-5536>

МАЙБУТНІ ТЕНДЕНЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІДПОВІДНО ДО ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

Анотація. Статтю присвячено проблематиці зростання ролі технологій штучного інтелекту та необхідності правового регулювання процесів взаємодії штучного інтелекту і людини в контексті інформаційної безпеки.

На переконання автора, без повноцінного і своєчасного нормативного регулювання розробок технологічних новацій, які зможуть приймати самостійні рішення, суспільство ризикує зазнати серйозних втрат. Тому вкрай важливо вже зараз розробити та впроваджувати для інформаційних технологій таке адміністративно-правове регулювання, в якому розвиток технологій не призведе до ризиків для суспільства і збереже за людиною контроль над тим, що відбувається.

Автор припускає, що штучний інтелект колись буде позбавлений статусу комп'ютерної програми або технології, і стане самостійним суб'єктом пра-

ва, наводячи в якості прикладу набуття правоздатності іншим штучним, абстрактним утворенням — державою.

У публікації розглянуто наявні спроби формування правових рамок для взаємодії людини та штучного інтелекту, що мали місце в Європейському Союзі, Японії та КНР. У тому числі — прецедент визнання штучного інтелекту самостійною творчою одиницею, який вже мав місце у китайському місті Шеньчжень, де суд постановив, що певні статті, написані з використанням штучного інтелекту, захищені авторським правом.

Окрему увагу присвячено аналізу сучасних досліджень перспектив застосування штучного інтелекту та його взаємодії з людиною. Автором пропонується підхід до регулювання правовідносин, пов'язаних зі штучним інтелектом.

Ключові слова: інформаційна безпека; інформаційні технології; штучний інтелект; правове регулювання; електронний уряд; дистанційне навчання; права людини.

БУДУЩИЕ ТЕНДЕНЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СООТВЕТСТВИИ С ТЕХНОЛОГИЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. Статья посвящена проблематике возрастания роли технологий искусственного интеллекта и необходимости правового регулирования процессов взаимодействия искусственного интеллекта и человека в контексте информационной безопасности.

По мнению автора, без полноценного и своевременного нормативного регулирования разработок технологических новаций, которые смогут принимать самостоятельные решения, общество рискует понести серьезные потери. Поэтому крайне важно уже сейчас разработать и внедрять для информационных технологий такое административно-правовое регулирование, при котором развитие технологий не приведет к рискам для общества и сохранит за человеком контроль над происходящим.

Автор предполагает, что со временем искусственный интеллект, лишившись статуса компьютерной программы или технологии, станет самостоятельным субъектом права, приводя в качестве примера приобретения правоспособности другим искусственным, абстрактным образованием — государством.

В публикации рассмотрены имеющиеся попытки формирования правовых рамок для взаимодействия человека и искусственного интеллекта, имевшие место в Европейском Союзе, Японии и КНР. В том числе — прецедент признания искусственного интеллекта самостоятельной творческой единицей, который уже имел место в китайском городе Шэньчжэнь, где суд постановил, что некоторые статьи, написанные с использованием искусственного интеллекта, защищены авторским правом.

Отдельное внимание посвящено анализу отечественных исследований перспектив применения искусственного интеллекта и его взаимодействия с человеком. Автором предлагается подход к регулированию правоотноше-

ний, связанных с искусственным интеллектом, построенный вокруг принципа — технологии на благо человека, для соблюдения его прав и свобод.

Автор прогнозирует смещение приоритетов в сфере информационной безопасности от защиты персональных данных и безопасности их использования к недопущению бесконтрольного использования искусственного интеллекта в сферах, связанных с реализацией прав и свобод человека.

Ключевые слова: информационная безопасность; информационные технологии; искусственный интеллект; правовое регулирование; электронное правительство; дистанционное обучение; права человека.

FUTURE TRENDS IN INFORMATION SECURITY ACCORDING TO ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Abstract. The article is devoted to the problems of the growing role of artificial intelligence technologies and the need for legal regulation of the processes of interaction between artificial intelligence and humans, in the context of information security.

According to the author, without a full and timely regulatory regulation of the development of technological innovations that can make independent decisions, society runs the risk of suffering serious losses. Therefore, it is extremely important already now, to develop and implement for information technologies such administrative and legal regulation in which the development of technologies will not lead to risks for the society and will retain control over what is happening to the person.

The author suggests that in the future artificial intelligence is deprived of the status of a computer program or technology, and it will become an independent subject of law, citing as an example of acquiring legal capacity by another artificial, abstract entity — the state.

The publication examines the existing attempts to form a legal framework for interaction between humans and artificial intelligence, which took place in the European Union, Japan and the PRC. This includes the precedent for recognizing artificial intelligence as an independent creative unit, which has already taken place in the Chinese city of Shenzhen, where the court ruled that some articles written using artificial intelligence are protected by copyright.

Special attention is devoted to the analysis of domestic studies of the prospects for the use of artificial intelligence and its interaction with humans. The author proposes an approach to the regulation of legal relations associated with artificial intelligence, built around the principle — technology for the benefit of a person, to respect his rights and freedoms.

The author predicts a shift in priorities in the field of information security from the protection of personal data and the security of their use, to the prevention of uncontrolled use of artificial intelligence, in the areas related to the implementation of human rights and freedoms.

Keywords: information security; Information Technology; Artificial Intelligence; legal regulation; electronic government; distance learning; human rights.

Постановка проблеми. Тотальна інформатизація сучасного суспільства, що супроводжується масовим впровадженням новітніх систем обробки інформації та телекомунікації, несуть в собі, окрім нечуваних раніше можливостей, чимало загроз, зумовлених не лише природою комп'ютерних інтелектуальних систем, а й відсутністю належного нормативно-правового регулювання їх діяльності.

Раніше поняття “штучний інтелект” викликало асоціації з науково-фантастичними романами та кіно, однак, уже сьогодні кожна людина так чи інакше стикається з використанням інтелектуальних систем пошуку контенту та обробки масивів інформації у повсякденному житті. При цьому, досі залишається під сумнівом відповідь на питання — чи може у штучного інтелекту з'явитися власна свідомість? Особливо гостро це питання постає в контексті того, що природа “свідомості” до кінця не досліджена і не є однозначно визначеною. Дослідження проблематики свідомості сягають глибини століть, беручи свій початок в античних філософських дискусіях і більш пізніх спробах зрозуміти, чи можна розум пояснити фізичними законами. У 20-ті роки ХХІ ст. ми сприймаємо штучний інтелект скоріше як алгоритм, який здатний узагальнити і обробити масив інформації, сформулювати прогнози щодо невідомих йому фактів. Однак, у деяких випадках при отриманні корисних висновків ми розуміємо, що програма здатна переналаштуватися на нові алгоритми [1].

Аналіз останніх досліджень та публікацій. Вагомий внесок у до-

слідження особливостей технологій штучного інтелекту в контексті інформаційної безпеки зробили такі вчені, як О. Кривецький, Г. Андрощук, Є. Романенко, І. Жукова, І. Давидова, В. Некрасов та ін.

Мета статті — дослідити проблематику зростання ролі технологій штучного інтелекту та необхідності правового регулювання процесів взаємодії штучного інтелекту і людини в контексті інформаційної безпеки.

Виклад основного матеріалу. Вже давно не є новиною, що інновації у сфері інформаційних технологій та інформаційної безпеки, дедалі більше надають штучному (електронному) інтелекту ознаки правової автономії, свободи вибору і навіть творчості. Тому, на наше переконання, взаємини людини з носіями інформації, базами даних, а в подальшому — і зі штучним інтелектом повинні регулюватися адміністративно-правовим шляхом у рамках інституту інформаційної безпеки. Конкуренція за першість в області інформаційних технологій і штучного інтелекту, прогнозовано буде одним з ключових процесів для всіх високорозвинених країн, щонайменше у наступні десять років. І хоча цей період видається невеликим, навіть за мірками нашого швидкого часу, лідери зазначеного процесу, напевно, визначаться доволі скоро. Проте, невід'ємною характеристикою лідерства будуть не лише новації та досягнення у галузі штучного інтелекту. Його найважливішою складовою залишаться забезпечення інформаційної безпеки людства і можливість легального впровадження новацій в

усіх сферах економіки та суспільного життя.

Без повноцінного і своєчасного нормативного регулювання розробок технологічних новацій, які зможуть приймати самостійні рішення, суспільство ризикує отримати удар у спину від результатів роботи своїх же рук. Тому вкрай важливо вже зараз задуматися і забезпечити для інформаційних технологій таке адміністративно-правове регулювання, в якому розвиток технологій не призведе до ризиків для суспільства і збереже за людиною контроль над тим, що відбувається.

Штучний інтелект наразі сприймається як безпрецедентний технологічний прорив, як технологія, здатна кардинально змінити наше життя. Однак варто пам'ятати, що подібні технології вже зустрічалися в історії людства. Електрика, радіо, телефон, автомобіль, літак здійснювали революційні прориви у світовому масштабі, і кожна таку технологію супроводжували громадські страхи, пов'язані з поширенням невідомого і погано зрозумілого.

Першим яскравим прикладом зміни суспільного ставлення до наслідків наукового прогресу може служити "The Locomotive Act", прийнятий британським парламентом у 1865 р. Цей закон, серед іншого, наказував, щоб перед кожним самохідним безрейковим транспортом, який ми зараз називаємо автомобілем, на відстані 55 метрів йшов чоловік із червоним прапором або ліхтарем, для попередження про небезпеку, а в самому екіпажі мало бути щонайменше два водія [2]. Уявити таку процедуру руху автомобільного

транспорту в сучасному світі доволі складно, адже сучасні люди сприймають автомобілі як буденність, не помічаючи їх та не виокремлюючи з-поміж звичного оточуючого світу. Отож, нескладно спрогнозувати, що зміна сприйняття аналогічна відмінності сьогоденного ставлення до автомобілів від того, яке мало місце в ХІХ ст., нас чекає і в контексті інформаційних технологій та штучного інтелекту. Хоча ми впевнені, що всі зміни будуть відбуватися доволі комфортно, якщо процес впровадження технологій штучного інтелекту буде супроводжувати певне адміністративно-правове регулювання стандартів і правил поведінки, що має перетворити його в буденність, яку ми теж не будемо помічати.

У законодавстві окремих держав та наддержавних утворень уже з'являються перші норми, що регулюють відносини інформаційних технологій і штучного інтелекту. Так, нещодавно, у 2017 р., Європейський Союз ухвалив Резолюцію "Норми цивільного права для робототехніки". У цьому документі, що містить понад сотню пунктів, адмініструються аспекти робототехніки і штучного інтелекту. Конкретно, пропонується закріпити правові основи використання штучного інтелекту і впровадження загальноєвропейської системи реєстрації розумних машин, за прикладом з автомобільним транспортом. Крім цього, планується регулювати правовим шляхом процеси роботизації людського організму [3; 4]. Таким чином, можна вести мову про закладення підвалин правового базису не лише для штучного інтелекту, а й кіборгізації.

Не відстають у досліджуваній сфері Японія та КНР. Зокрема, в Японії, ще у 2016 р., на засіданні Державної комісії з інтелектуального права було прийнято рішення почати розробку нормативних документів щодо захисту авторських прав на продукти творчої діяльності, створені штучним інтелектом [3]. Не менш яскравий випадок трапився у китайському місті Шеньчжень, де штучний інтелект визнали самостійною творчою одиницею. Там суд постановив, що певні статті, написані з використанням штучного інтелекту, захищені авторським правом. Звісно ж, рішення суду стосувалося конкретних текстів компанії Tencent, яка публікує контент програмного забезпечення у сфері бізнесу і фінансів. Компанія звернулася до суду після того, як одна з онлайн-платформ розмістила на своєму сайті текст Tencent, згенерований за допомогою штучного інтелекту. Суд постановив, що формулювання матеріалу і використувані вирази були оригінальними, і класифікував його як письмовий твір, який захищається авторським правом [5]. Цілком можливо, що цей випадок стане прецедентом для світової юридичної спільноти.

У східноєвропейському суспільстві, на жаль, поки що не прийшли до необхідності регулювання цієї сфери діяльності. Твори, створені штучним інтелектом, наприклад в Україні, поки що буквально не визнаються створеними, оскільки, відповідно до чинного законодавства, авторське право може поширюватися тільки на живу людину. Водночас, чимало досліджень уже присвячується можливостям і ризикам імплементації штучно-

го інтелекту в існуючі галузі права, такі як законодавство про персональні дані, захист інтелектуальної власності або антимонопольне. Окрім того, вітчизняна наукова спільнота дедалі більше уваги приділяє проблематиці впровадження електронного урядування, яке з часом, так чи інакше, переплітатиметься з технологією штучного інтелекту. Ще у 2016 р. під “електронним урядуванням” (е-урядуванням) пропонувалось розуміти спосіб організації державної влади за допомогою систем локальних інформаційних мереж та сегментів глобальної інформаційної мережі, що забезпечує функціонування певних служб у режимі реального часу та робить максимально простим і доступним щоденне спілкування громадян з офіційними установами [6]. Поступово переходячи від теорії до практики правотворення та правозастосування, чимало українських фахівців працює над проблематикою формування правовідносин у сфері застосування штучного інтелекту. Деякі напрацювання вже впроваджені в життя, зокрема, такі як електронний цифровий підпис, ідентифікація за профілем або верифікація особи. Ведуться дискусії щодо створення систем електронного голосування та цифрової економіки. Відповідно до призначення штучний інтелект буде легалізуватися в різних галузях економіки і соціальної сфери, а прийняті адміністративно-правові засади повинні застрахувати суспільство від безлічі прогнозованих ризиків [7–9].

Вкрай важливою сферою, де, на наше переконання, рано чи пізно знайдуть своє застосування технології штучного інтелекту, є дистанційне

навчання, у тому числі із застосуванням технологій віртуальної реальності. Віднедавна, внаслідок введення у десятках країн карантинних обмежень, спрямованих на протидію поширенню коронавірусної хвороби COVID-19, спостерігається висока активність не лише застосування дистанційного навчання паралельно зі стаціонарним, але й повного, хай навіть тимчасово, переходу до ведення лекційних, семінарських, контрольних занять, здачі іспитів, у тому числі державних, дистанційно, за допомогою комп'ютерних засобів [10].

Відповідно, дедалі більше уваги науковців присвячується особливостям адаптації технологій доповненої реальності у навчальних дисциплінах для студентів різних навчальних закладів. Ведеться мова про доцільність застосовування інтегрованого підходу у процесі підготовки майбутніх фахівців нової технологічної ери. При цьому, на думку дослідників, застосування технологій доповненої реальності підвищує мотивацію до навчання, підвищує рівень засвоєння інформації завдяки різноманітності та інтерактивності її візуального подання [11].

Чимало дослідників наразі дискутують про корисність технології блокчейн, що використовується в обороті криптовалют, у різних сферах управління. З точки зору інформаційної безпеки, ця технологія — просто скарб. Найпростішим способом використання її в найближчому майбутньому нам бачиться застосування в електронних виборчих технологіях. Завдяки цій технології повинен буде кодуватися кожен крок

виборчого процесу і голосування. При цьому інформаційна безпека буде забезпечена кодуванням незмінного порядку кожної операції і кожного елемента в ланцюзі подій. У результаті чого, спроба змінити одну з ланок цього ланцюга обов'язково змінить код елемента, а це викличе збій всієї програми, що дасть змогу відразу виявити умисне втручання.

Іншою унікальною якістю для інформаційної безпеки технологія блокчейн володіє в тому сенсі, що всім учасникам процесу, у нашому випадку — голосування, розсилається повна копія всього ланцюга подій із вказаним кодуванням. Тому кожен зможе перевірити відповідність результатів із самим процесом та результатами. Таким чином, завдяки подвійному контролю технології можна досягти ідеалу інформаційної безпеки, тобто такого процесу, який неможливо підробити або штучно змінити. Однак застосування таких технологій вимагає деякої зміни адміністративно-правового регулювання інформаційної безпеки на зазначених напрямках правового поля [12].

Додатково хочеться зазначити, що влада Пекіна заявила про впровадження у 140 державних сервісах технологію блокчейн. За їх словами, використання технології розподіленого реєстру допомогло знизити витрати на 40 % і є проривом, якого не можна було досягти при застосуванні традиційних систем передачі інформації.

“Блокчейн — це прорив в обмінні даними, який важко реалізувати традиційним способом. Зберігання електронних сертифікатів на блок-

чейні підвищує надійність, ефективність і спрощує процес перевірки даних”, — зазначили представники китайської влади. Також в уряді Китаю зазначили, що сервіси, які використовують блокчейн, поділені на 3 категорії. По-перше, обмін і передача даних; по-друге, їх спільна обробка і, по-третє, — зберігання електронних ліцензій і сертифікатів [12].

В якості прикладу китайський чиновник назвав базу для реєстрації нерухомості. Вона містить 11 секторів, куди входить комісія з муніципального планування, комісія по житловому будівництву і розвитку сільських районів, податкове бюро, бюро громадської безпеки та ін.

Додатковим свідченням значущості проблематики штучного інтелекту можна вважати експертні прогнози щодо обсягів інвестицій у цю сферу. Наразі експерти відзначають, що обороти інвестицій в технологію штучного інтелекту ростуть щорічно і до 2024 р. можуть досягти майже 140 млрд дол. Лише у Китаї бюджет на впровадження стратегії розвитку технологій штучного інтелекту до 2030 р. становить 150 млрд дол. [13].

Наприкінці червня 2020 р. Італійська банківська асоціація (ABI), яка складається з більше ніж 700 банків, повідомила, що її члени готові протестувати цифровий євро, про що написала на своєму офіційному сайті. Участь у суміжних проектах і експериментальних програмах допоможе прискорити впровадження цифрової валюти, підтримуваної Європейським центральним банком [17].

Під час інвестиційного буму на перший план виходять питання захисту прав і свобод людини, а також ін-

формаційної безпеки. Йдеться, перш за все, про неприпустимість використання розробок в цілях навмисного заподіяння шкоди громадянам і юридичним особам. Тому автором пропонується стимулюючий підхід до регулювання даних відносин, побудований навколо принципу — технології на благо людини для дотримання зазначених прав і свобод. Якщо в даний час у сфері інформаційної безпеки пріоритетом є захист персональних даних і безпека їх використання, то у майбутньому акцент зміститься на недопущення безконтрольного використання штучного інтелекту, пов'язаного з реалізацією прав і свобод людини.

Водночас, як ми вже зазначали, окрім вражаючих перспектив технології штучного інтелекту несуть в собі ряд потенційних загроз. Відповідно до проведеного в 2019 р. звіту Натана Бенайча і Яна Хогарта, під назвою “Шкідливе використання штучного інтелекту”, інтелектуальні системи цілком можуть служити злочинцям і терористам. І науковці, і розробники повинні це врахувати і попереджати можливе використання їх напрацювань на шкоду суспільству. В якості первинного превентивного заходу слід закріпити відповідні обмеження на законодавчому рівні [14].

Наразі спроби адміністративного регулювання відносин людини і штучного інтелекту існують тільки на рівні поверхневого обговорення їх подальшої реалізації. Але скоро доведеться взаємодіяти значно більше, особливо — якщо штучний інтелект набуде всіх ознак суб'єкта, зокрема свободи вибору і творчості. Переві-

рений спосіб — це вписати пов'язані зі штучним інтелектом відносини у правове поле. При цьому насправді не надто важливо, як він буде розвиватися у цьому полі. Головне — наявність гнучкості і своєчасної зміни запропонованих норм. Але коригувати адміністративно-правове поле необхідно вже зараз, і кейси застосування штучного інтелекту підказують напрями подальшого його вдосконалення.

Досі взаємовідносини суспільства і штучного інтелекту співіснують за правилами рівноваги Неша. Коли кожна зі сторін не в змозі дізнатися про наміри опонента і домовитися один з одним, обидві вибирають не найвигодніший для себе варіант розвитку подій, чи прямо кажучи, менш руйнівний. Це положення відкрив і описав через математичні закони американський математик Джон Неш, за що отримав Нобелівську премію з економіки у 1994 р. [15].

Цілком можливо, що штучний інтелект колись буде позбавлений статусу комп'ютерної програми або технології, і стане самостійним суб'єктом права. Правова наука вже стикалася зі схожими питаннями, коли неживе явище заради загальної зручності визнавали правоздатним. Найвідоміший приклад — це визнання держави як юридичної особи. Таке визначення в майже незмінному вигляді прийнято в усьому світі, воно стало звичним, і ні у кого не викликає подиву, що таке абстрактне явище, як держава, що не має ні власної волі, ні природи — має правоздатність.

Також у майбутньому обов'язково виникне питання необхідності

регламентації взаємодії людини зі штучним інтелектом. Такий процес вже розпочато на міждержавному рівні. В уже згадуваному нами проекті зводу етичних правил для штучного інтелекту, підготовленого в Європейському Союзі ще у 2017 р., зазначається, що штучний інтелект повинен служити справедливому суспільству, підтримувати фундаментальні права людини, ніяк не обмежувати автономність людей і, взагалі, працювати на благо позитивних змін у суспільстві. При цьому повинен зберігатися цивільний контроль над відповідними даними. Юристам слід створити адміністративно-правові механізми, які гарантуватимуть відповідальність і підзвітність всіх систем штучного інтелекту і їх діяльності. І це тільки перші вимоги до нормативної бази для регуляції зазначених відносин. Коли і як ці етичні норми будуть реалізовуватися в життя, ми ще будемо бачити [4; 16]. Однак уже сьогодні цілком актуальною є тема інформаційної безпеки і відповідальності за дії систем зі штучним інтелектом. Відповідальність представляється складовою інституту інформаційної безпеки, що відповідає за правосуб'єктність.

Уже зараз нанесення шкоди фізичній чи юридичній особі в процесі експлуатації систем зі штучним інтелектом не є чимось нереальним. Перший простий приклад можна легко уявити. Безпілотний автомобіль збиває людину, яка переходила вулицю по пішохідному переходу. Хто у даному випадку є відповідальним за заподіяння шкоди? Адже таким може бути визнано як господаря безпілотника, так і його виробника. В ін-

ших випадках, після проведення розслідування, звинуватять розробника програмного забезпечення для нього, ліцензіата або інженера служб технічної чи програмної підтримки, що відповідають за налаштування програми і запуск. Далі виникає питання — за яких умов відповідальність може бути покладена на кожного із зазначених суб'єктів? Хто буде відповідати за випадки порушення інформаційної безпеки або за наслідки простих хакерських атак? Можливо в таких випадках буде застосовуватися практика притягнення до відповідальності власників засобів підвищеної небезпеки? Зараз відповіді на ці питання ще зовсім не очевидні і породжують нові питання, які потребують врегулювання, у тому числі — у нормах права і судовій практиці.

Отже, проблем, які спричинить за собою поширення технологій штучного інтелекту, виникне багато. Тому як ніколи слід виходити за межі класичних наукових течій та створювати міждисциплінарні напрями досліджень. Важливо не боятися шукати для них рішення, об'єднуючи зусилля вчених-правознавців і експертів з різних галузей знань.

Висновки. Зростання ролі технологій штучного інтелекту та усвідомлення цього процесу обумовлює всезростаючу конкуренцію за першість у цій галузі серед найбільш розвинених країн. Невід'ємною характеристикою лідерства будуть не тільки новації та досягнення в галузі штучного інтелекту. Його найважливішою складовою залишаться забезпечення інформаційної безпеки людства і можливість легального впровадження новацій у всіх сферах

економіки та суспільного життя. Без повноцінного і своєчасного адміністративно-правового регулювання розробок технологічних новацій, які зможуть приймати самостійні рішення, суспільство ризикує зазнати серйозних втрат. Тому вкрай важливо вже зараз розробити та впроваджувати для інформаційних технологій таке адміністративно-правове регулювання, в якому розвиток технологій не призведе до ризиків для суспільства і збереже за людиною контроль над тим, що відбувається.

Цілком ймовірно, що штучний інтелект колись буде позбавлений статусу комп'ютерної програми або технології, і стане самостійним суб'єктом права. Мають місце спроби формування правових рамок для взаємодії людини та штучного інтелекту. Європейський Союз ще у 2017 р. підготував проект зводу етичних правил для штучного інтелекту, відповідно до норм якого ключовими цілями штучного інтелекту зазначено: служіння справедливому суспільству, підтримка фундаментальних прав людини, заборона на обмеження автономності людей тощо.

Автором пропонується стимулюючий підхід до регулювання правовідносин, пов'язаних зі штучним інтелектом, побудований навколо принципу — технології на благо людини, для дотримання її прав і свобод. Якщо наразі у сфері інформаційної безпеки пріоритетом є захист персональних даних і безпека їх використання, то у майбутньому ми прогнозуємо зміщення акценту на недопущення безконтрольного використання штучного інтелекту у сфе-

рах, пов'язаних з реалізацією прав і свобод людини.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Нік Бостром*. Штучний інтелект. Етапи. Загрози. Стратегії. 2016. 496 с.
2. Юрист. Випуск нової серії XI. Ч. II. 32-3 доповнення Статуту, прийняті на сесії 1865-28 та 29 Вікторія. Н. Sweet, Лондон. Stevens & Sons, Лондон. Hodges, Smith, & Co., Дублін. 1866. [Електронний ресурс] URL: <http://www.archive.org/details/jurist09britgoog>
3. *Кривецький О.* До проблеми правового регулювання штучного інтелекту. Центр досліджень соціальних комунікацій НБУВ [Електронний ресурс]. URL: http://nbuviar.gov.ua/index.php?option=com_content&view=article&id=3728:do-problemi-pravovogo-regulyuvannya-shtuchnogo-intelektu&catid=8&Itemid=350
4. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). [Електронний ресурс]. URL: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//EN>
5. *Геннадій Андросчук*. Твори, створені AI, мають право на захист авторських прав? // Юридична газета online [Електронний ресурс] URL: <https://yur-gazeta.com/golovna/tvori-stvoreni-ai-mayut-pravo-na-zahist-avtorskih-prav.html>
6. *Romanenko Y. O. & Chaplay I. V.* (2016). Marketing communication system within public administration mechanisms // Actual Problems of Economics. 178(4). 69–78.
7. Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI [Електронний ресурс] URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
8. Про авторське право та суміжні права: Закон України від 23 грудня 2012 р. № 3792-XII [Електронний ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/3792-12#Text>
9. Про захист економічної конкуренції: Закон України від 11 січня 2001 р. № 2210-III [Електронний ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/2210-14#Text>.
10. МОН пропонує для громадського обговорення проект положення про дистанційну форму здобуття загальної середньої освіти 22 червня 2020 року. Офіційний веб-портал Міністерства освіти і науки України. [Електронний ресурс]. URL: <https://mon.gov.ua/ua/news/mon-proponuye-dlya-gromadskogo-obgovorennya-proyekt-polozhennya-pro-distancijnu-formu-zdobuttya-zagalnoyi-serednoyi-osviti>
11. *Iatsyshyn A. V., Kovach V. O., Romanenko Y. O. and other* (2020). Application of augmented reality technologies for preparation of specialists of new technological era Augmented Reality in Education : Proceedings of the 2nd International Workshop (AREdu 2019), Kryvyi Rih, Ukraine, March 22, 2019 (2547). p. 181–200. ISSN 1613-0073.
12. *Давидова І. В.* Технологія блокчейн: перспективи розвитку в Україні // Часопис цивілістики Нац. ун-ту “Одеська юридична академія”. 2017. Вип. 26. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_

- name=PDF/Chac_2017_26_10.pdf
13. Катерина Койдан. Штучний інтелект: заявки на лідерство. Український тиждень: матеріал друкованого видання № 23 (603) від 6 червня, 2019. URL: <https://tyzhden.ua/Science/231039>
 14. Некрасов В. Як прогресує штучний інтелект: звіт про останні досягнення, 15.07.2019 // Економічна правда. [Електронний ресурс] URL: <https://www.epravda.com.ua/publications/2019/07/15/649648/>
 15. Ігнатенко О. Теорія ігор: що це таке, та як вона змінює повсякденне життя // Українська правда, 2018. [Електронний ресурс] URL: <https://life.pravda.com.ua/columns/2018/02/3/228782/>.
 16. Єврокомісія започатковує пілотний проект з визначення на практиці етичних принципів, за якими у Європі розвиватиметься штучний інтелект. Укрінформ 01.07.2020. URL: <https://www.ukrinform.ua/rubric-technology/2676698-v-evrosouzi-rozrobili-etiket-dla-stuchnogointelektu.html>.
 17. За посиланням, <https://www.aifi.it/en/soci/aderenti/7131-abi-italian-banking-association/>
3. Kryvetskyi O. (n.d.). Do problemy pravovoho rehuliuвання shtuchnoho intelektu [To the problem of legal regulation of artificial intelligence]. *nbuviar.gov.ua*. Retrieved from http://nbuviar.gov.ua/index.php?option=com_content&view=article&id=3728:problem-i-pravovogo-regulyuvannya-shtuchnogointelektu&catid=8&Itemid=350 [in Ukrainian].
 4. European Parliament resolution of 16 February 2017 with recommendations do the Commission on Civil Law Rules on Robotics (2015/2103(INL)). (n.d.). *www.europarl.europa.eu*. Retrieved from https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html?redirect [in English].
 5. Androshchuk H. (2020). Tvory, stvoreni AI, maiut pravo na zakhyst avtorskykh prav?! [Works created by AI have the right to copyright protection?!]. *yur-gazeta.com*. Retrieved from <https://yur-gazeta.com/golovna/tvori-stvoreni-ai-mayut-pravona-zahist-avtorskih-prav.html> [in Ukrainian].
 6. Romanenko Y. O. & Chaplay I. V. (2016). Marketing communication system within public administration mechanisms. *Actual Problems of Economics*, 178(4), 69–78 [in English].
 7. Zakon Ukrainy “Pro zakhyst personalnykh danykh” : vid 01 chervnia 2010, № 2297-VI [Law of Ukraine “On personal data protection” from June 1 2010, № 2297-VI]. *zakon.rada.gov.ua*. Retrieved from <https://zakon.rada.gov.ua/laws/show/2297-17#Text> [in Ukrainian].

REFERENCES

1. Bostrom N. (2016). *Iskusstvennyy intellekt. Etapy. Ugrozy. Strategii*. [Superintelligence: Paths, Dangers, Strategies]. Moscow: “Mann, Ivanov i Ferber” [in Russian].
2. *The Jurist. New Series. Vol. XL-Part II. Containing original articles on legal subjects, all important statutes, the rules and orders of the various courts, cause lists, and miscellaneous legal information, for the year 1865: with an index of principal matters.* (1866). London: H. Sweet, 3, Chancery Lane; Ste-

8. Zakon Ukrainy “Pro avtorske pravo ta sumizhni prava” : vid 23 hrudnia 2012, № 3792-XII [Law of Ukraine “On copyright and related rights” from December 23 2012, № 3792-XII]. *zakon.rada.gov.ua*. Retrieved from <https://zakon.rada.gov.ua/laws/show/3792-12#Text> [in Ukrainian].
9. Zakon Ukrainy “Pro zakhyst ekonomichnoi konkurentsii” : vid 11 sichnia 2001, № 2210-III [Law of Ukraine “On protection of economic competition” from January 11 2001, № 2210-III]. *zakon.rada.gov.ua*. Retrieved from <https://zakon.rada.gov.ua/laws/show/2210-14#Text> [in Ukrainian].
10. MON proponuie dlia hromadskoho obhovorennia proekt polozhennia pro dystantsiinu formu zdobuttia zahalnoi serednoi osvity 22 chervnia 2020 roku [The Ministry of Education and Science proposes for public discussion a draft regulation on the distance form of general secondary education on June 22, 2020]. (2020). *mon.gov.ua*. Retrieved from <https://mon.gov.ua/ua/news/mon-proponuye-dlya-gromadskogo-obgovorennia-proyekt-polozhennia-pro-distancijnu-formu-zdobuttia-zagalnoi-serednoi-osvity> [in Ukrainian].
11. Iatsyshyn A. V., Kovach V. O., Romanenko Ye. O., Deinega I. I., Iatsyshyn A. V., Popov O. O., et al. (2020). Application of augmented reality technologies for preparation of specialists of new technological era. *Augmented Reality in Education* : Proceedings of the 2nd International Workshop (AREdu 2019). (p. 181–200). Kryvyi Rih [in English].
12. Davydova I. V. (2017). Tekhnolohiia blokchein: perspektyvy rozvytku v Ukraini [Blockchain technology: prospects for development in Ukraine]. *Chasopys tsyvilistyky Natsionalnoho universytetu “Odeska yurydychna akademiia” – Journal of Civil Studies of the National University “Odessa Law Academy”*, 26. Retrieved from http://www.irbis-nbu.gov.ua/cgi-bin/irbis_nbu/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Chac_2017_26_10.pdf [in Ukrainian].
13. Koidan K. (2019). Shtuchnyi intelekt: zaiavky na liderstvo [Artificial intelligence: applications for leadership]. *tyzhden.ua*. Retrieved from <https://tyzhden.ua/Science/231039> [in Ukrainian].
14. Nekrasov V. (2019). Yak prohresuie shtuchnyi intelekt: zvit pro ostanni dosiahnennia [How artificial intelligence progresses: a report on recent achievements]. *pravda.com.ua*. Retrieved from <https://www.epravda.com.ua/publications/2019/07/15/649648/> [in Ukrainian].
15. Ihnatenko O. (2018). Teoriia ihor: shcho tse take, ta yak vona zmieniue povsiakdenne zhyttia [Game Theory: what it is and how it changes everyday life]. *life.ppravda.com.ua*. Retrieved from <https://life.ppravda.com.ua/columns/2018/02/3/228782/> [in Ukrainian].
16. V Yevrosoiuzi rozrobyly “etyket” dlia shtuchnoho intelektu [The European Union has developed an “etiquette” for artificial intelligence]. (2020). *www.ukrinform.ua*. Retrieved from <https://www.ukrinform.ua/rubric-technology/2676698-v-evrosouzi-rozrobili-etiket-dla-stucnogo-intelektu.html> [in Ukrainian].
17. ABI – Italian Banking Association. (n.d.). *www.aifi.it*. Retrieved from <https://www.aifi.it/en/soci/aderenti/7131-abi-italian-banking-association/> [in Ukrainian].