НОВЕЛІЗАЦІЯ ПРАВОВОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ: МІЖНАРОДНИЙ І НАДНАЦІОНАЛЬНИЙ ВИМІРИ

КАМІНСЬКА Наталія - доктор юридичних наук, професор, провідний науковий співробітник відділу міжнародного права та права Європейського Союзу Інституту держави і права імені В.М. Корецького НАН України
https://orcid.org/ 0000-0002-7239-8893
КАМІНСЬКА Анастасія - Навчально-науковий інститут міжнародних відносин Київського національного університету імені Тараса Шевченка
https://orcid.org/0000-0002-5529-3045
УДК 341.9; 347.73
DOI: https://doi.org/10.71404/NP.2025.2.35

Мета статті полягає в здійсненні аналізу, виокремленні основних новітніх напрямів і пріоритетів міжнародно-правового і наднаціонального регулювання штучного інтелекту, виходячи з існуючих доктринальних і нормативних джерел у цьому контексті. Не зважаючи на активну появу нових наукових розвідок у цьому напрямі, усе ж таки предметом вивчення сучасних дослідників залишаються переважно загальнотеоретичні або галузеві аспекти застосування ШІ. Поза їх увагою питання концептуалізації моделей правової регламентації ШІ, його потенційних ризиків, відповідальності, гарантій безпеки та рівності, новелізація міжнародно-правового регулювання універсального, регіонального, наднаціонального рівнів.

У результаті дослідження відзначено, що очевидна динаміка системи загальноцивілізаційних і європейських цінностей, стандартів і принципів у зв'язку з поширенням ШІ, цифровізацією. Звернуто увагу на роль і значення таких міжнародних організацій як ОЕСР, ООН, Рада Європи, а також Європейський Союз у процесі розробки і прийняття міжнародних стандартів, що стосуються правової регламентації штучного інтелекту, його створення і впровадження, засади використанння у різних сферах життєдіяльності. Так, проаналізовано Міжнародні керівні принципи для організацій з розробки передових систем ШІ і Кодекс поведінки для організацій з розробки передових систем ШІ, Рекомендації ОЕСР з питань штучного інтелекту, Рамкову конвенцію про штучний інтелект і права людини, демократію і верховенство права, особлива увага звернута на Регламент ЄС про штучний інтелект (Закон про AI). Реалізація Цифрового порядку денного для Європи, становлення Цифрового союзу, заснованого на Єдиному цифровому ринку супроводжується численними законодавчими ініціативами, створенням майже півсотні нових прав і свобод у цифровому просторі, де традиційні свободи руху осіб, капіталу і послуг реалізуються онлайн, виокремлюються гарантії їх безпеки і захисту, заборони онлайн дискримінації і т.д. Забезпечення їх належної реалізації сприятиме не лише упорядкуванню сфери ШІ, а й гарантуванню безпеки, дотриманню прав і свобод людини при застосуванні ШІ, відповідальності за порушення встаноленого порядку його створення і використання.

Звісно, ШІ зумовлює трансформацію міжнародного права, наднаціонального і національного права. Проте його належне використання потребує ефективного правового регулювання, яке має бути доступним, прозорим, гарантуватиме права і свободи людини, підзвітність і ефективний нагляд. Статус України як кандидата у члени ЄС зумовлює долучення до згаданих ініціатив, активну участь у міжнародних правотворчих і правозастосовних процесах цифрової епохи.

Ключові слова: штучний інтелект, міжнародне право, правове регулювання, стандарти, ОЕСР, acquis ЄС, Рада Європи, ООН, законодавство, права людини, електронна демократія, цифрові технології, парламент, судочинство, інтелектуальна власність, космос, збройний конфлікт

Постановка проблеми

Активний розвиток технологій пронизує всі сфери сучасного життя людини, суспільства, держав, міжнародних організацій та інших суб'єктів, різноманітних спільнот. Проте все ж таки в деяких сферах очевидний значний прогрес на шляху впровадження і використання інформаційно-комунікаційних технологій (ІКТ), штучного інтелекту (ШІ, Artificial intelligence – AI), а інші значно відстають. Україна ввійшла до рейтингу найбільш готових держав до запровадження ШІ у 2019 р. і стартувала з 63-ї позиції, згодом повільно рухається вище, хоча ще значно відстає від таких країн як США, Сінгапур, Великобританія, Канада, Фінляндія, Естонія, Чехія, Польща, Литва й інші. Його авторами визначено 39 індикаторів, що встановлюють готовність у таких основних сферах: уряд, технологічний сектор і дані й інфраструктура. Так, уряд кожної держави повинен мати стратегічне бачення того, як він розвиває та управляє ШІ, базуючись на правовому регулюванні; увазі до етичних проблем (управління та етика); потужний внутрішній цифровий потенціал, включно з навичками і практиками, що підтримують його адаптивність до нових технологій. [1-2]

Водночас залишаються дискусії про доцільність впровадження технологій штучного інтелекту в усі без виключень напрями і сфери життєдіяльності, попри його унікальні можливості й потенціал, значення для інноваційного розвитку науки і техніки, економічні й фінансові переваги. Йдеться про потенційно негативні етичні та правові наслідки, загрози національній безпеці, певний дискримінаційний вплив на основоположні права і свободи людини, зокрема, стосовно конфіденційності, захисту персональних даних, прав інтелектуальної власності, інформаційної безпеки, кібербезпеки, сталого розвитку, ринку праці і безробіття. За прогнозами вченого Н. Бострома у виданні Technology Review, за 60 років ШІ може стати суттєвою загрозою для всього людства: якщо до 2022 р. він мислитиме орієнтовно на 10 % як людина, до 2040 р. – на 50 %, до 2075 р. – мислення ШІ і людини практично неможливо буде відрізнити, тому ШІ може стати занадто загрозливим для людства. [3]

На наш погляд, не вистачає наразі ґрунтовних наукових праць комплексного характеру, де було б проаналізовано теоретичну основу, концептуальні засади запровадження ШІ, його потенціал, ризики й рамки міжнародно-правової й національної регламентації.

Як українські, так і зарубіжні вчені підкреслюють «сильні» та «слабкі» сторони ШІ, деякі із зазначених аспектів. Наприклад, О. Стойко вивчає політико-правові наслідки використання штучного інтелекту (2023) [2]; О. Радутний – специфіку кримінальної відповідальності штучного інтелекту (2017) [3]; І. Берназюк – штучний інтелект як нову реальність, його потенційний вплив на конституційно-правове регулювання в Україні (2025) [4]; Д. Бєлов і Н. Шишка – штучний інтелект в судочинстві та судових рішеннях, в українському правосудді (2023; 2021) [5-6]; І. Скляренко – перспективи заміни суддів у цивільному судочинстві на технологію ШІ (2024) [7]; Г. Авдєєва – проблеми використання систем штучного інтеолекту у правозастосовній діяльності. (2023) [8]; Г. Андрощук і Є. Тимошенко – проблеми патентування винаходів, створених з використанням ШІ (2022; 2020) [9-10]; Т. Тарасевич – правове регулювання ШІ у сфері репродуктивних функцій людини (2023) [11] тощо. Зрештою, небагато дослідників звертають увагу на особливості міжнародно-правового регулювання ШІ (Г. Прохазка, М. Харіна, Г. Татаренко і М. Карпенко, А. Пазюк, Н. Попова та ін.) [12-16]; його регламентацію в Європейському Союзі (І. Городиський, О. Кожухар, А. Пазюк) [17-18].

Враховуючи вищевикладене, за *мету нашого дослідження* слід визначити здійснення аналізу та виокремлення основних новітніх напрямів і пріоритетів міжнародно-правового і наднаціонального регулювання штучного інтелекту, виходячи з існуючих доктринальних і нормативних джерел у цьому контексті.

Виклад основного матеріалу

Безумовно, що існують потенційні й реальні переваги ШІ для людини і громадянина, економіки й політики, дипломатії, медицини тощо. Погоджуємось з висновками, що

активний розвиток його можливостей зумовлює численні виклики, потік яких лише зростатиме. Тому держави в різних куточках світу працюють над розробкою правил і стандартів, що визначатимуть обґрунтовані межі правового регулювання процесів розробки й впроваджєння, використання ШІ в усі сфери життя, а також відповідальності за порушення встановленого правового порядку, захисту персональних данних, кібербезпеки тощо. Властиво, насамперед, є важливою розробка і прийняття міжнародно-правових стандартів, правил і принципів у цій сфері, враховуючи транскордонний, до певної міри масштабний характер поширення. Тому загальні стратегії та концепції, погоджені на міжнародному універсальному та/або загальноєвропейському чи інших регіональних рівнях надалі повинні стати основою для розробки нормативно-правових актів і правозастосування у сфері ШІ на національному рівні. Це стосується методик і способів протидії, дієвого реагування на явні порушення й виклики, пов'язані з ШІ.

Цікавим прикладом правового регулювання глобального виміру деяких питань використання ШІ є ухвалення під час Хіросімського процесу зі штучного інтелекту (The G7 Hiroshima Artificial Intelligence Process) Міжнародних керівних принципів для організацій з розробки передових систем ШІ (The International Guiding Principles for Organizations Developing Advanced AI Systems, Керівні принципи) і Кодексу поведінки для організацій з розробки передових систем ШІ (The International Code of Conduct for Organizations Developing Advanced AI Systems, Кодекс поведінки), що були оприлюднені 30 жовтня 2023 р. Вони базуються на принципах, зафіксованих у Рекомендації щодо штучного інтелекту (The Recommendation on Artificial Intelligence) Ради ОЕСР 22 травня 2019 р. – фактично першому міжурядовому стандарті щодо ШІ. Прийняття додаткових стандартів за результатами Хіросімського процесу зі штучного інтелекту спричинено потребою використання перевагам передових систем ШІ, подолання ймовірних ризиків.

Власне Керівні принципи і Кодекс поведінки встановлюють 11 стандартів або базових принципів та заходів щодо регулювання і використанні ШІ:

- використання при розробці передових систем ШІ різноманітних заходів внутрішнього та незалежного зовнішнього тестування задля виявлення, оцінки та зменшення ризиків протягом усього життєвого циклу ШІ;
- виявлення та пом'якшення вразливостей, інцидентів і схем нецільового використання після розгортання, включаючи розміщення на ринку;
- публічне повідомлення про можливості, обмеження та сфери (не)належного використання передових систем ШІ для забезпечення достатньої прозорості;
- обмін інформацією і звітування про інциденти серед організацій, що розробляють передові системи ШІ, включаючи представників промисловості, уряди, громадянське суспільство та наукові кола;
- розробка, впровадження політик управління ШІ, організаційних механізмів для реалізації цих політик відповідно до підходу, що ґрунтується на оцінці ризиків;
- інвестування і впровадження надійних засобів контролю безпеки, включаючи фізичну безпеку, кібербезпеку і засоби захисту від внутрішніх загроз протягом усього життєвого циклу ШІ;
- розробка і впровадження надійних механізмів автентифікації й підтвердження походження контенту, що дозволяють користувачам ідентифікувати контент, створений ШІ;
- пріоритетність досліджень про зменшення ризиків для суспільства, безпеки і захисту, пріоритетність інвестицій в ефективні способи пом'якшення наслідків;
- пріоритетність розробки передових систем ШІ для вирішення глобальних проблем людства;
- розробка міжнародних технічних стандартів;
- впровадження належних процедур введення даних і захисту персональних даних та інтелектуальної власності. [19].

Такі стандарти і заходи є невичерпні, оскільки це «живий документ», тому вони є об'єктом обговорення та еволюції. Не зважаючи на те, що це норми «м'якого права»,

вони відображають спільні наміри країн G7, ЄС про напрямки подальшого правового розвитку регулювання сфери ШІ. Крім цього, як свідчить аналіз Закону про штучний інтелект (Artificial Intelligence Act, Регламент про ШІ) у ЄС, його положення узгоджується з вищезазначеними в Керівних принципах і Кодексі поведінки. При цьому, слід відзначити ризикоорієнтований підхід, використаний в останніх згаданих документах, що зумовлює необхідність постійного вивчення, тестування, попередження і реагування на можливі ризики й виклики.

Хоча ООН і система її органів, спеціалізованих інституцій потребує невідкладного реформування, але слід відзначити, що ця організація не залишається осторонь цифровізації, діджиталізації, використання інноваційних технологій. Так, з 2014 р. в ООН дискутується необхідність заборони або обмеження LAWS – автономних бойових систем, механізмів, здатних самостійно вибирати цілі та здійснювати атаки без прямого контролю людини. Це підтверджує той факт, що в міжнародному праві серед складних сфер застосування ШІ – військова. Запропоновані ініціативи прийняття нового протоколу до Конвенції про заборону звичайної зброї не знайшли одностайної підтримки, у т.ч. США, росії тощо. [20]. Цікавими, але такими, що потребують комплексного вивчення, є також космічна сфера, фінансова та економічна, екологічна та енергетична, соціальна і культурна та ін. сфери.

На рівні ООН відбувались міжурядові переговори стосовно глобального регулювання використання ШІ і 2024 р. Запропоновано створення спеціального міжнародного органу з нагляду за високоризиковими ШІ-системами, за аналогією з МАГАТЕ у сфері ядерної енергії. Така ініціатива важлива задля забезпечення прозорості, уніфікації стандартів безпеки, підзвітності розробників і користувачів ШІ, тим самим відкриваючи перспективу укладення глобальної міжнародно-правової угоди про регулювання ШІ найближчим часом.

Слід звернути увагу на проблему відповідальності держави в міжнародному праві за здійснення контролю за діяннями, що спричинили порушення. Тобто раціональним вбачається розширення концепції «due diligence» в міжнародному праві, включивши до неї обов'язок держав забезпечити превентивне регулювання і контроль за системами ШІ [21, с. 65].

Передбачено створення міжнародного механізму аудиту моделей ШІ, зокрема через т.зв. «червоні команди», що тестують моделі на вразливості, з огляду на те, що потужні моделі ШІ (foundation models) можуть спричинити екзистенційні загрози, якщо вийдуть з-під контролю. Йдеться про Блетчлійську декларацію 2023 р., прийняту на Саміті з безпеки ШІ у Великобританії, до якої долучились близько 30 країн, включаючи Україну. [22].

Україна, яка є членом Спеціального комітету зі штучного інтелекту при Раді Європи, 2019 р. приєдналася до Рекомендацій ОЕСР з питань штучного інтелекту (Organization for Economic Cooperation and Development, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449) та визначила для себе пріоритетними для впровадження технологій штучного інтелекту такі сфери, як: освіта, економіка, публічне управління, кібербезпека, оборона.

Так само значущим стало прийняття в рамках Ради Європи 2024 р. Рамкової конвенції про штучний інтелект і права людини, демократію і верховенство права (CETS № 225). Її положення є обов'язковими для сторін, також приєднатись можуть як держави-члени РЄ, так і треті країни, на засадах «інклюзивного мультилатералізму» (Японія, Канада, США, Ізраїль, Мексика, Перу, Уругвай, Аргентина, Австралія, Коста-Ріка, Святий Престол, ЄС тощо) [23]. Це відкритий для підписання перший в історії глобальний договір про ШІ, міжнародний юридично обов'язковий договір, спрямований на забезпечення того, щоб використання систем ШІ повністю відповідало правам людини, демократії та верховенству права. Стандарти, що містяться в договорі, охоплюють весь життєвий цикл систем ШІ, є технологічно нейтральниим, сприячи прогресу та інноваціям у цій галузі, одночасно керуючи ризиками, які він може становити для прав людини, демократії та верховенства права. Прикметно, що до його розробки долучи-

лись представники громадянського суспільства, приватного сектору, наукові експерти.

Крім того, очевидний прогрес законодавчого регулювання процесу використання штучного інтелекту державами ЄС пов'язаний з прийняттям 2024 р. Регламенту про штучний інтелект (Регламент ЄС, Закон про AI) [24]. Це фактично перший обов'язковий до виконання горизонтальний нормативно-правовий акт з питань ШІ, встановлює загальні рамки використання і постачання систем ШІ в Євросоюзі. Тут класифіковано системи ШІ з різними вимогами та зобов'язаннями, адаптованими до «ризик-орієнтованого підходу», у т.ч. «високоризикові» системи ШІ з можливим негативним впливом на здоров'я, безпеку людей, їх основні права і свободи, дозволені за умови дотримання ряду вимог і зобов'язань для отримання доступу на ринок ЄС; системи ШІ, що становлять «обмежені» ризики через непрозорість, на які поширюються вимоги про інформацію і прозорість; системи ШІ, що становлять «мінімальний» ризик для людей, на які додаткові зобов'язання не поширюваються. Передбачено нові правила для моделей ШІ загального призначення (GPAI), більш жорсткі вимоги до моделей GPAI з «можливостями високого впливу», що можуть встановити системні ризики, значно впливаючи на внутрішній ринок, а також визначено зобов'язання для провайдерів і користувачів залежно від рівня ризику від впровадження інструментів ШІ. Серед неприйнятних ризиків цим Регламентом ЄС визначено системи, що є загрозою для людей, зокрема, з т.з. безпеки, і мають бути заборонені, а саме: 1) когнітивне поведінкове маніпулювання людьми або окремими вразливими групами; 2) соціальну оцінку (класифікація людей на основі поведінки, соціально-економічного статусу чи особистих характеристик); 3) біометричну ідентифікацію та категоризацію людей. Для правоохоронних цілей можливі деякі винятки, системи дистанційної біометричної «пост»-ідентифікації, можуть бути дозволені для переслідування серйозних злочинів і лише після схвалення суду. Системи штучного інтелекту, які негативно впливають на безпеку або фундаментальні права, вважаються системами з високим ризиком з поділом на дві категорії: 1) системи ШІ, що використовуються у виробах, які підпадають під дію Регламенту ЄС про ШІ щодо безпеки продуктів, їх перелік включає іграшки, авіацію, автомобілі, медичне обладнання та ліфти; 2) системи ШІ, що належать до певних сфер, які повинні бути зареєстровані в базі даних ЄС – управління та експлуатація критичної інфраструктури; освіта і професійна підготовка; працевлаштування, управління працівниками й доступ до самозайнятості; доступ і користування основними приватними та державними послугами й перевагами; правоохоронні органи; управління у сфері міграції, надання притулку та прикордонного контролю; допомога в правовому тлумаченні та застосуванні законодавства. [24-25].

Важливо, що передбачено необхідність оцінення всіх систем ШІ з високим рівнем ризику перед виведенням на ринок, так само і протягом усього життєвого циклу. При цьому Генеративний ШІ та ChatGPT не буде віднесений до категорії високого ризику, але вони повинні відповідати вимогам прозорості і Регламенту ЄС про авторське право, щоб сприяти довірі від людей, забезпечуючи їх інформування. Запроваджено зобов'язання щодо прозорості, надання інформації при використанні систем ШІ (чатботи, у т.ч. при створенні фейкового аудіо та відеоконтенту), щоб людина знала і мала можливість визначитись чи продовжити їх використання. На постачальників також покладено обовязок забезпечити ідентифікацію створеного ШІ контенту. Регламент про ШІ дозволяє безкоштовно застосовувати ШІ з мінімальним ризиком (відеоігри з підтримкою ШІ, фільтри спаму).

Також значущою гарантією вбачаємо право подавати скарги на системи ШІ до визначених національних органів. А задля переходу до нової нормативної бази, Європейська Комісія прийняла Пакт про штучний інтелект – своєрідну добровільну ініціативу, спрямовану на підтримку запровадження нових стандартів, залучення розробників ШІ з Європи і поза її межами завчасно виконати основні зобов'язання Регламенту про ШІ. Встановлено, що держави-члени ЄС по-

винні до 2 серпня 2025 р. визначити національні компетентні органи для моніторингу застосування правил для систем на основі ШІ, здійснення нагляду за ринком [26-28]. Тут необхідна координація дій парламентів та урядів, інших владних інститутцій держав-членів ЄС, залучення громадянського суспільства та експертного середовища до консультацій, обговрення наступних невідкладних законотворчих ініціатив щодо використання ШІ в різних сферах і напрямах.

Ще 2023 р. ратифіковано Угоду між Україною та ЄС про участь України в програмі Європейського Союзу «Цифрова Європа» (2021–2027) [29], що покликана сприяти інтеграції у Єдиний європейський цифровий простір, забезпеченню конкурентноздатності в європейському дослідницькому та інноваційному просторі. Так, війна і значні збитки значно впливають на пріоритети і темпи розвитку цієї галузі, але зумовлюють визначення першочергових дій, процесів, явищ, необхідних для припинення війни, притягнення винних до відповідальності й відшкодування заподіяних збитків. Звісно, для таких цілей необхідним є використання можливостей ШІ, цифровізації, різноманітних форм і методів співпраці на європейському і глобальному рівнях. Йдеться, насамперед, про цифрову трансформацію національної економіки, сектору безпеки і оборони, системи національного і міжнародного правосуддя та ін.

Неодноразово дослідники акцентували на тому, що з активізацією цифровізації, поширення ШІ розвиваються нетипові або специфічні форми та інститути демократії, наприклад, електронна демократія, у межах механізмів якої вже функціонує моніторингова демократія, технологія блокчейн, еволюціонує статус електронної особи тощо. [31-33]. Це сприяє суттєвим змінам форм і способів участі людини та громадянина в публічно-владних відносинах, їх модернізації. Поряд з цим, слід підкреслити розвиток теорії й практики войовничої демократії, обороноздатної демократії або демократії, здатної себе захистити. Усе це демонструє врахування викликів, загроз і здобутків сьогодення, актуалізує необхідність використання результатів технологічного, інноваційного прогресу разом з людським потенціалом задля припинення війн та інших збройних конфліктів, катастроф природного і техногенного характеру, захисту прав людини і соціальної справедливості, стимулювання сталого безпечного розвитку людини, територіальної громади, держави і суспільства, цивілізованого світу.

Висновки

Не зважаючи на активну появу нових наукових розвідок у зазначеному напрямі, усе ж таки предметом вивчення сучасних учених залишаються переважно загальнотеоретичні або галузеві аспекти застосування ШІ. Поза їх увагою питання концептуалізації моделей правової регламентації ШІ, його потенційних ризиків, відповідальності, гарантій безпеки та рівності, новелізація міжнародно-правового регулювання універсального, регіонального, наднаціонального рівнів.

Тому в результаті дослідження відзначено, що очевидна динаміка системи загальноцивілізаційних і європейських цінностей, стандартів і принципів у зв'язку з поширенням ШІ, цифровізацією. Звернуто увагу на роль і значення таких міжнародних організацій як ОЕСР, ООН, Рада Європи, а також Європейський Союз у процесі розробки і прийняття міжнародних стандартів, що стосуються правової регламентації штучного інтелекту, його створення і впровадження, засади використанння у різних сферах життєдіяльності. Так, проаналізовано Міжнародні керівні принципи для організацій з розробки передових систем ШІ і Кодекс поведінки для організацій з розробки передових систем ШІ, Рекомендації ОЕСР з питань штучного інтелекту, Рамкову конвенцію про штучний інтелект і права людини, демократію і верховенство права, особлива увага звернута на Регламент ЄС про штучний інтелект (Закон про AI). Останній з них, поряд із Загальним регламентом ЄС про захист даних, значно вплинув і надалі впливатиме на регіональний, наднаціональний та національні правопорядки. Реалізація Цифрового порядку денного для Європи, становлення Цифрового союзу, заснованого на Єдиному цифровому ринку, супроводжуєть-

ся численними законодавчими ініціативами, створенням майже півсотні нових прав і свобод у цифровому просторі, де традиційні свободи руху осіб, капіталу і послуг реалізуються он-лайн, виокремлюються гарантії їх безпеки і захисту, заборони онлайн дискримінації і т.д. Забезпечення їх належної реалізації сприятиме не лише упорядкуванню сфери ШІ, а й гарантуванню безпеки, дотриманню прав і свобод людини при застосуванні ШІ, відповідальності за порушення встаноленого порядку його створення і використання.

Звісно, ШІ зумовлює трансформацію міжнародного права, наднаціонального і національного права. Проте його належне використання потребує ефективного правового регулювання, яке має бути доступним, прозорим, гарантуватиме права і свободи людини, підзвітність і ефективний нагляд. Статус України як кандидата в члени ЄС зумовлює долучення до згаданих ініціатив, активну участь у міжнародних правотворчих і правозастосвних процесах цифрової епохи.

Література

1. Oxford Insights Government AI Readiness Index 2022. URL: https://www. oxfordinsights.com/government-ai-readiness-index-2022

2. Стойко О. М. Політико-правові наслідки використання штучного інтелекту. Правова держава. 2023. Вип. 34. С. 684-693. URL: http://jnas.nbuv.gov.ua/article/UJRN-0001449266

3. Радутний О. Е. Кримінальна відповідальність штучного інтелекту. Інформація і право. 2017. № 2 (21). С. 124–132. 2

4. Берназюк І.М. Штучний інтелект як нова реальність та його потенційний вплив на конституційно-правове регулювання в Україні. Електронне наукове видання «Аналітично-порівняльне правознавство» С. 76-82. DOI https://doi.org/10.24144/2788-6018.2025.01.11

5. Бєлов Д. М. Штучний інтелект в судочинстві та судових рішеннях, потенціал та ризики: Науковий вісник Ужгородського національного університету. Серія: Право. 2023. Т.2 № 78.

6. Шишка Н. В. Штучний інтелект в українському правосудді: правові передумови запровадження. Юридичний науковий електронний журнал. 2021. № 3. С. 143-145. URL: http://lsej.org.ua/3_2021/37.pdf

7. Скляренко І. В. Сучасні перспективи заміни суддів у цивільному судочинстві на технологію штучного інтелекту. Юридичний науковий електронний журнал. 2024. № 2. С. 153-156. URL: http://lsej.org.ua/2_2024/38.pdf

8. Авдєєва Г. К. Проблеми використання систем штучного інтеолекту у правозастосовній діяльності. Вісник ЛДУВС ім. Е.О. Дідоренка. 2023. Вип. 2 (102). С. 63-79. URL: https://luhbulletin.dnuvs.ukr.education/index.php/main/article/view/105/98

9. Андрощук Г. О. Проблеми патентування винаходів, створених з використанням штучного інтелекту: доктрина і практика (Ч. 1). Теорія і практика інтелектуальної власності. 2022. № 2. С. 54-67. URL: https://doi.org/10.33731/22022.259744

10. Тимошенко Є.А. Штучний інтелект як суб'єкт права інтелектуальної власності. Часопис Київського університету права, (4), 328-332. URL: https://doi.org/10.36695/2219-5521.4.2020.58

11. Тарасевич Т.Ю. Правове регулювання штучного інтелекту у сфері репродуктивних функцій людини: сучасні виклики та перспективи реалізації. Науковий вісник Ужгородського Національного Університету, 2023. Серія ПРАВО. Вип.75: част. 1. URL: https://doi.org/10.24144/2307-3322.2022.75.1.20

12. Прохазка Г.А. Штучний інтелект в міжнародному праві. Юридичний науковий електронний журнал. 2022. № 2. URL: http://www.lsej. org.ua/2_2022/33.pdf

13. Харіна М. До питання регулювання правового статусу штучного інтелекту в міжнародному праві та українському законодавстві. Молодий вчений. 2019. 5 (69). URL: https://doi.org/10.32839/2304-5809/2019-5-69-108

14. Татаренко Г. В., Карпенко М. В. Міжнародно-правове регулювання технологій штучного інтелекту в бойових діях Актуальні проблеми права: теорія і

практика № 2(46), 2023. URL: https://doi.org/10.33216/2218-5461/2023-46-2-135-145

15. Попова Н.О. Міжнародно-правове регулювання штучного інтелекту: сучасний стан та перспективи. Юридичний науковий електронний журнал. 2024. №4. С. 443-447. http://www.lsej.org.ua/4_2024/107.pdf DOI https://doi.org/10.32782/2524-0374/2024-4/105

16. Товкун Л.В., Леонович М.Ю. Правове регулювання штучного інтелекту: міжнародний досвід та перспективи впровадження для України. Юридичний науковий електронний журнал. № 12. 2024. С. 278-282. http://lsej.org.ua/12_2024/64.pdf DOI https://doi.org/10.32782/2524-0374/2024-12/62

17. Городиський І.М. Тенденції розвитку правового регулювання штучного інтелекту в Європейському Союзі. URL: http://aphd.ua/publication-388

18. Кожухар О. Г. Правове регулювання систем штучного інтелекту в ЄС: передумови, сучасний стан та перспективи. Наукові записки НаУКМА. Юридичні науки. 2024. Том 13. С.65-73. DOI: 10.18523/2617-2607.2024.13.65-73

19. Ракитянська К. Міжнародні стандарти регулювання штучного інтелекту: аналіз актів, розроблених за результатами Хіросімського процесу з ШІ. https://jurliga.ligazakon.net/news/225406_mzhnarodn-standarti-regulyuvannya-shtuchnogo-ntelektu-analz-aktv-rozroblenikh-za-rezultatami-khrosmskogo-protsesu-z-sh

20. Stopping Killer Robots: Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control. 2021. URL: https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and

21. Besson S. Due Diligence and International Responsibility in AI Contexts. International Law Journal. 2022. Vol. 33. P. 59–78.

22. UK Government. Bletchley Declaration on AI Safety. 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

23. Council of Europe. Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (Vilnius, 2024). URL: https://edoc.coe.int/en/artificial-intelligence/11926-council-of-europe-framework-convention-on-artificial-intelligence-and-human-rights-democracy-and-the-rule-of-law.html; https://rm.coe.int/1680afae3c

24. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689

25. Парламентське дослідження щодо законодавчих тенденцій впровадження інструментів штучного інтелекту у сфері правосуддя в Європейському Союзі. https://research.rada.gov.ua/uploads/documents/33379.pdf

26. AI Pact. URL: https://digital-strategy.ec.europa.eu/en/policies/ai-pact

27. Artificial Intelligence and Life in 2030. URL: https://ai100.stanford.edu/sites/g/files/sbiybj18871/files/media/file/ ai100report-10032016fnl_singles.pdf

28. Формування цифрового майбутнього Європи. URL: https://digital-strategy.ec.europa.eu/en/policies/regulatoryframework-ai

29. Про ратифікацію Угоди між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» (2021–2027) : Закон України від 23.02.2023 № 2926-IX. URL: https://zakon.rada.gov.ua/laws/ show/2926-20#Text

30. Artificial Intelligence Act: MEPs adopt landmark law. European Parliament. European Parliament (2024). https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

31. Демиденко В.О. Електронне голосування на місцевих виборах в Україні: вимога сьогодення чи далеке майбутнє?: *Муніципальна реформа в контексті євроінтеграції України: позиція влади, науковців, профспілок та громадськості* матеріали IV Всеукраїн-

ської конф.(Київ, 10 грудня 2020 р.): Київ: АПСВТ, 2020. С. 138-140

32. Михайлов М.Б. Нетипові (допоміжні) форми безпосередньої демократії: теорія та конституційно-правове регулювання: автореф. дис. … канд. юрид. наук за спеціальністю 12.00.02 – конституційне право; муніципальне право. Харків, 2019. 20 с.

33. Камінська Н.В. Правовий статус електронної особи у світлі законодавчих ініціатив ЄС та України *Стан дотримання прав людини в умовах сучасності: теоретичні та практичні аспекти:* матеріали всеукраїн. конференції від 22 березня 2018. Київ, 2018.

34. Камінська Н. «Цифрова Україна»: конституційно-правова модель / за заг. ред. Р.О.Стефанчука, О.Л.Копиленка, Є.Р.Бершеди, О.М.Клименко. К.: Інститут законодавства Верховної Ради України, 2021. С.100-128, 648-671.

NOVELIZATION OF LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE: INTERNATIONAL AND SUPRANATIONAL DIMENSIONS

The purpose of the article is to analyze, identify the main new directions and priorities of international legal and supranational regulation of artificial intelligence, based on existing doctrinal and normative sources in this context. Despite the active emergence of new scientific research in this area, the subject of study of modern researchers remains mainly general theoretical or industry aspects of the application of AI. Beyond their attention are the issues of conceptualizing models of legal regulation of AI, its potential risks, liability, guarantees of security and equality, and the novelization of international legal regulation at the universal, regional, and supranational levels.

As a result of the study, it was noted that the dynamics of the system of general civilizational and European values, standards and principles in connection with the spread of AI, digitalization are obvious. Attention is drawn to the role and importance of such international organizations as the OECD, the UN, the Council of Europe, as well as the European Union in the process of developing and adopting international standards related to the legal regulation of artificial intelligence, its creation and implementation, and the principles of use in various spheres of life. Thus, the International Guidelines for Organizations Developing Advanced AI Systems and the Code of Conduct for Organizations Developing Advanced AI Systems, the OECD Recommendations on Artificial Intelligence, the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law were analyzed, with special attention paid to the EU Regulation on Artificial Intelligence (AI Law). The implementation of the Digital Agenda for Europe, the formation of the Digital Union based on the Single Digital Market is accompanied by numerous legislative initiatives, the creation of almost fifty new rights and freedoms in the digital space, where the traditional freedoms of movement of persons, capital and services are implemented online, guarantees of their safety and protection are highlighted, prohibitions of online discrimination, etc. Ensuring their proper implementation will contribute not only to the regulation of the AI sphere, but also to guaranteeing security, compliance with human rights and freedoms when applying AI, and liability for violation of the established procedure for its creation and use.

Of course, AI entails the transformation of international law, supranational and national law. However, its proper use requires effective legal regulation, which must be accessible, transparent, guarantee human rights and freedoms, accountability and effective supervision. Ukraine's status as a candidate for EU membership presupposes its participation in the aforementioned initiatives, active participation in international law-making and law-enforcement processes of the digital age.

Keywords: artificial intelligence, international law, legal regulation, standards, OECD, EU acquis, Council of Europe, UN, legislation, human rights, e-democracy, digital technologies, parliament, judiciary, intellectual property, space, armed conflict