

СТИРАНКА М. Б.,

кандидат юридичних наук

ORCID ID: 0009-0007-6523-0586

УДК 342.9+321.7+347.121

DOI <https://doi.org/10.32842/2078-3736/2024.4.111>

СУБ'ЄКТИ ЦИФРОВОГО ПРАВА: КОНЦЕПТУАЛЬНИЙ ЗМІСТ

Стаття концептуалізує суб'єктний вимір цифрового права в умовах трансформації соціальних відносин під впливом науки й технологій. Вихідною рамкою є класична тріада правосуб'єктності – правоздатність, дієздатність, деліктоздатність – яка застосовується до учасників цифрових правовідносин із урахуванням специфіки електронної ідентифікації, простежуваності дій та необхідності ефективного притягнення до відповідальності. Обґрунтовано, що ідентифікація в електронному середовищі (кваліфікований електронний підпис, засоби е-ідентифікації, біометрія) є умовою надання юридичної сили електронним діям і визначення належного кола прав та обов'язків сторін. Розкрито гібридну природу статусу ключових учасників цифрових сервісів (власники інформаційних ресурсів і аудіовізуальних сервісів, провайдери хостингу, оператори зв'язку й пошукових систем), у яких приватно-правові моделі взаємодії обмежуються публічно-правовими вимогами прозорості, недискримінаційності, захисту даних і кіберстійкості з огляду на пріоритет публічного інтересу. Продемонстровано, як інфраструктурність «інтернету речей» зміщує акцент до посилення стандартів безпеки та підзвітності. Проаналізовано ризики автоматизованих рішень для справедливого процесу і зроблено висновок про потребу процесуальних гарантій перевірки та оскарження таких висновків. Узагальнено чотири доктринальні підходи до правосуб'єктності цифрових систем і аргументовано перевагу еволюційної моделі мінімальної або помірної інклюзивності, за якої машина виконує делеговані технічні дії в межах чітко окресленого мандату, тоді як персоніфікована відповідальність зберігається за людськими й організаційними носіями. Запропоновано нормативну архітектуру «відповідального використання»: формалізована прозорість, аудитуваність, страхове покриття шкоди, реєстрація куратора, верифіковані журнали подій, механізми негайного зупинення та відзиву повноважень. Сформульовано висновок про доцільність поетапної кодифікації таких вимог як умови інтеграції інновацій у правопорядок без розмивання базових гарантій суб'єктивних прав.

Ключові слова: *цифрове право, правосуб'єктність, правоздатність, дієздатність, деліктоздатність, ідентифікація в електронному середовищі, персоніфікована відповідальність.*

Styranka M. B. Subjects of digital law: conceptual content

The article conceptualizes the subjective dimension of digital law in the context of the transformation of social relations under the influence of science and technology. The starting point is the classical triad of legal personality – legal capacity, capacity to act, tortious capacity – which is applied to participants in digital legal relations, taking into account the specifics of electronic identification, traceability of actions and the need for effective prosecution. It is substantiated that identification in the electronic environment (qualified electronic signature, e-identification means, biometrics) is a condition for granting legal force to electronic actions and determining the appropriate range of rights and obligations



of the parties. The hybrid nature of the status of key participants in digital services (owners of information resources and audiovisual services, hosting providers, communication and search engine operators) is revealed, in which private-law models of interaction are limited by public-law requirements of transparency, non-discrimination, data protection and cyber resilience given the priority of the public interest. It is demonstrated how the infrastructural nature of the “Internet of Things” shifts the emphasis to enhanced security and accountability standards. The risks of automated decisions for a fair process are analyzed and the conclusion is drawn about the need for procedural guarantees for the verification and appeal of such conclusions. Four doctrinal approaches to the legal personality of digital systems are summarized and the advantage of an evolutionary model of minimal or moderate inclusiveness is argued, in which the machine performs delegated technical actions within a clearly defined mandate, while personalized responsibility remains with human and organizational carriers. The normative architecture of “responsible use” is proposed: formalized transparency, auditability, insurance coverage of damage, curator registration, verified event logs, mechanisms for immediate suspension and revocation of powers. The conclusion is formulated on the feasibility of a phased codification of such requirements as conditions for integrating innovations into the legal order without diluting the basic guarantees of subjective rights.

Key words: *digital law, legal personality, legal capacity, capacity, tortious capacity, identification in the electronic environment, personalized responsibility.*

Постановка проблеми. Стрімкий поступ науки й технологій змінює конфігурацію суспільних взаємодій і примушує по-новому осмислювати сучасне право: його предмет, принципи, межі та коло учасників. У цьому контексті потребує уточнення як перелік потенційних носіїв суб'єктивних прав і обов'язків, так і спектр об'єктів правового впливу у цифровому середовищі.

Правосуб'єктність посідає центральне місце у загальній теорії права. Традиційно вона включає три взаємопов'язані складові: по-перше, правоздатність – потенційну можливість мати суб'єктивні права й юридичні обов'язки; по-друге, дієздатність – спроможність особи самостійно здійснювати належні їй права та виконувати обов'язки; по-третє, деліктоздатність – здатність нести юридичну відповідальність за наслідки власної поведінки. Саме ця тріада забезпечує реальну участь носіїв прав у конкретних правовідносинах. Соціальною передумовою правосуб'єктності визнається свобода волі як атрибутивна властивість людини, що дає підстави для самостійного та усвідомленого вибору правомірної поведінки [1].

У науковому дискурсі нерідко ототожнюють поняття «суб'єкт права» та «суб'єкт правовідносин». Проте коректність такого ототожнення залежить від фактичної включеності особи у сталі правові зв'язки: статус суб'єкта правовідносин набувається щодо конкретної норми, яка регулює певний тип соціальних відносин і «вмикає» відповідні права та обов'язки.

Перенесення цього підходу у цифровий простір висуває на перший план проблему ідентифікації. Саме встановлення цифрової ідентичності дозволяє визначити учасників правовідносин і віднести їх до відповідної «цифрово-правової» сфери. Водночас особливості мережових технологій уможливають приховування персональних даних, використання псевдонімів і багатошарових цифрових профілів. Через це в науковій літературі обґрунтовується теза про знеособлення значної частини цифрових правовідносин, що ускладнює реєстрацію, доказування, притягнення до відповідальності та, зрештою, вимагає переосмислення традиційних конструкцій правосуб'єктності у світлі нових техніко-правових реалій.

Стан наукової розробки проблеми. В українській правовій науці окремі загально-теоретичні аспекти цієї проблематики відображені у працях О.М. Бандурки, В.В. Головченка, М.І. Козюбри, А.М. Колодія, Н.М. Крестовської, Т.Є. Мураховської, О.Г. Мурашина,



Ю.М. Оборотова, Н.М. Оніщенко, О.В. Петришина, В.Ф. Погорілка, С.П. Погребняка, І.М. Погрібного, П.М. Рабіновича, О.Д. Тихомирова, Ю.С. Шемшученка та інших дослідників.

Метою наукової статті є визначення концептуального змісту суб'єктів цифрового права.

Виклад основного матеріалу. В українському контексті питання встановлення особи користувача у мережевому просторі розглядається як складова цифрового права. Розбудова такого простору потребує глибокого оновлення нормативної бази щодо ідентифікації учасників правовідносин, адже ключова мета цих змін – наділення юридичною силою дій, що вчиняються в електронній формі. Ідентифікаційні процедури, з одного боку, забезпечують достовірне визначення особи учасника цифрових правовідносин або його уповноваженого представника (цифрового посередника), а також контрагента у правочинах [2].

З іншого боку, цифрове середовище становить фундамент інфраструктури електронних публічних послуг в Україні. Серед технологічних інструментів встановлення особи ключове місце посідають кваліфікований електронний підпис, засоби електронної ідентифікації та біометричні параметри. Додатковою функцією ідентифікації є фіксація місця перебування користувача, від чого нерідко залежить вибір права, що регулює діяльність відповідного суб'єкта. Водночас фізична локалізація серверів, платформ і дата-сховищ не завжди піддається однозначному визначенню у межах державних кордонів, що ускладнює прив'язку до конкретної юрисдикції.

Носії цифрових прав, реалізуючи можливості віртуального простору, набувають і спеціальних правомочностей – зокрема права на доступ до мережі Інтернет, «права бути забутим», права на цифрове припинення персоніфікованої присутності («цифрову смерть») тощо. Саме під впливом цифровізації традиційні права та свободи людини зазнають змістовної трансформації. Оцифрування дій і процедур відкриває можливість здійснювати публічні функції в електронному форматі: надавати адміністративні послуги, організовувати електронне соціальне обслуговування, забезпечувати дистанційну участь громадян у виборчих процесах і в інших формах залучення до управління суспільними та державними справами.

У сучасній архітектоніці цифрового права ключовими носіями прав та обов'язків постають юридичні та фізичні особи, що проєктують, впроваджують і надають цифрові послуги (зокрема суб'єкти підприємницької діяльності). Експансія цифрових сервісів зумовила формування спеціалізованого понятійного апарату, який фіксує нові ролі у правопорядку: «власник інформаційного ресурсу», «власник аудіовізуального сервісу», «провайдер хостингу», «оператор зв'язку», «оператор пошукової системи», «посередник чи організатор поширення інформації у мережі Інтернет», «правовласник цифрової інформації» тощо [3]. Кожна з цих ролей маркує не лише технологічну функцію, а й специфічну конфігурацію відповідальності, управлінських обов'язків і меж особистої недоторканості в умовах мережевої взаємодії.

Правовий статус означених суб'єктів має гібридну природу, поєднуючи публічно-правові та приватно-правові елементи [4, с. 6]. Навіть діючи як фізичні особи – підприємці, вони здійснюють надання послуг, що за своєю функцією спрямовані на задоволення суспільного інтересу (доступ до інформації, безпеку та безперервність комунікацій, цілісність даних, захист користувачів). Звідси випливає пріоритет публічного інтересу над приватним у регулюванні цифрових сервісів: договірні моделі, характерні для цивільно-правових відносин, обмежуються імперативними приписами щодо прозорості, недискримінаційності, захисту персональних даних і кіберстійкості. Отже, навіть у суто комерційних взаємодіях між «власником інформаційного ресурсу» та користувачем діє посилений режим публічно-правових гарантій.

Ілюстративним є феномен «інтернету речей»: провайдери платформних рішень на основі штучного інтелекту інтегрують об'єкти виробничої та бізнес-інфраструктури у єдині екосистеми з віддаленим керуванням, аналітикою та автономним прийняттям рішень. Така інтеграція перетворює приватні технологічні сервіси на елементи критичної інформаційної



інфраструктури, що, у свою чергу, легітиміє посилені вимоги публічного права до безпеки, надійності, підзвітності та захисту прав користувачів [5; 6, с. 6].

Діяльність учасників цифрового середовища неминуче пов'язана з підвищеними ризиками, зокрема з ризиком помилкового встановлення обставин правопорушення унаслідок збоїв мережевої інфраструктури. У таких ситуаціях особа може бути притягнена до юридичної відповідальності за діяння, яких фактично не вчиняла. Цю проблему виразно ілюструє справа «Держава проти Лумаса», у якій вирок було обтяжено на підставі висновків автоматизованої системи оцінювання ймовірності повторного правопорушення [7]. Особа, що погодилася на угоду зі слідством і розраховувала на умовний строк, отримала шість років позбавлення волі та п'ять років посиленого нагляду саме через такий автоматизований висновок [7].

У матеріалах цієї справи наголошено на трьох ключових вадах використаної системи. По-перше, її призначення не відповідає меті ухвалення процесуальних рішень у кримінальному судочинстві: вона розроблена для потреб виконавчої системи (зокрема, оцінки доцільності дострокового звільнення) і здатна лише виокремлювати групи підвищеного ризику, а не давати індивідуалізовану оцінку конкретної особи. По-друге, достовірність висновків поставлена під сумнів: збіг автоматизованих прогнозів із фактичним рецидивом зафіксовано лише приблизно у п'ятій частині випадків. По-третє, система є приватною розробкою, власник якої відмовився розкривати спосіб формування висновку, що унеможливило перевірку підстав та логіки отриманого результату. Спроба оскарження вироку була доведена до Верховного Суду Сполучених Штатів Америки, який відмовив у задоволенні скарги, водночас зауваживши, що автоматизовані інструменти не можуть бути єдиною підставою судового рішення [7].

Наведений приклад демонструє суспільно значущий ризик – схильність до надмірної довіри до машинно згенерованих висновків. Навіть за формального врахування інших доказів ознайомлення судді з «оцінкою ризику» здатне упередити сприйняття справи. За таких умов будь-яке відхилення від вимог про ухвалення рішення на підставі перевіреної та оспорюваної інформації має автоматично активувати механізми контролю і перегляду для захисту процесуальних гарантій сторін [7].

Становлення глобального інформаційного простору породжує нові виклики суб'єктного виміру права. Цифровізація суспільних відносин змінює антропологічний профіль учасника правового обігу: формується тип особи, чия повсякденна діяльність невідривна від цифрових та інформаційно-аналітичних технологій. Ефективність і безпека життєдіяльності такої особи прямо залежать від здатності оволодівати цифровими інструментами, генерувати та критично опрацьовувати дані, а також будувати на їх основі моделі поведінки й оцінювати дії інших учасників правовідносин.

Поява і швидке поширення нових технологій виходять за межі традиційних конструкцій правової системи, що актуалізує потребу в правовій об'єктивації нового кола відносин – між людиною та робототехнічними системами. Інтенсивний розвиток штучного інтелекту підвищує роль автономних технічних засобів не лише у виробничих процесах, а й у сферах, що вважалися простором інтелектуальної праці людини. Це, у свою чергу, ставить питання про належне визначення правового статусу таких систем і меж їх залучення до юридично значущих процесів.

У науці та практиці точиться дискусія щодо можливості визнання робототехнічних систем суб'єктами права. Підставово вона зводиться до двох блоків. По-перше, до розрізнення функцій: технічна допомога у виконанні окремих операцій (навіть складних) не є тотожною юридичній компетенції ухвалювати рішення, що породжують, змінюють чи припиняють права та обов'язки. По-друге, до питання відповідальності: наділення машин правосуб'єктністю фактично підміняє суб'єктів права об'єктами права і розмиває персоніфікацію відповідальності. Юридично значущі дії можуть бути здійснені лише людиною або колективом людей (органом державної влади, установою, організацією), а відповідальність за наслідки застосування автономних систем мають нести їх розробники, власники, оператори та користувачі – залежно від їхньої ролі, контролю й вигоди.



Перспективною є модель «взаємних зобов'язань на основі довіри» між людськими учасниками, які використовують автономні системи, з чітким розподілом обов'язків, стандартів безпеки, процедур аудиту та можливостей оскарження автоматизованих висновків. Водночас необхідно нормативно відмежувати: надання правової допомоги із застосуванням інструментів штучного інтелекту як допоміжної технології та здійснення юридично значущих дій, що потребує людської волі, усвідомлення та відповідальності.

Отже, одним із ключових напрямів розвитку цифрового права є формування доктрини про нові (цифрові) ролі учасників правовідносин і конкретизація їхнього статусу: визначення правоздатності, дієздатності, меж використання автономних систем і, головне, прозорого механізму покладення відповідальності на людських носіїв рішень, що забезпечить сумісність інновацій із засадничими гарантіями правопорядку.

У правовій доктрині суб'єкти права традиційно типологізуються за онтологічною природою носія прав і обов'язків. Базова тріада охоплює: індивідуальних суб'єктів (фізичних осіб); колективних суб'єктів; громадські утворення. Такий поділ відображає, відповідно, персоніфікований, організаційний і суспільно-комунітарний рівні правосуб'єктності.

Розгорнуті класифікації деталізують зазначені групи. Зокрема, у підході О. Скакун види суб'єктів правовідносин визначаються так [8]: індивідуальні суб'єкти (фізичні особи): громадяни (індивіди, що мають громадянство певної держави); іноземні громадяни; особи без громадянства (апатриди); особи з подвійним громадянством (біпатриди); колективні суб'єкти (юридичні особи): державні органи, установи, організації, підприємства; органи місцевого самоврядування; комерційні організації (акціонерні товариства, приватні фірми тощо – вітчизняні, іноземні, міжнародні); громадські об'єднання (політичні партії, професійні спілки тощо); релігійні організації; держава та її структурні одиниці, а також соціальні спільноти (держава як суверенний носій публічної влади; державні утворення; адміністративно-територіальні одиниці (область, місто, селище та ін.); соціальні спільноти (народ, нація, етнічні групи, спільноти громадян виборчого округу тощо).

Узагальнюючи, наведена типологія фіксує різнорівневу природу правосуб'єктності: від індивідуально-особистісного до інституційного й колективно-публічного вимірів. Вона є методологічною основою для подальшої спеціалізації – зокрема, для окреслення кола суб'єктів у цифровому праві, де поряд із традиційними носіями прав і обов'язків виокремлюються ролі, зумовлені функціонуванням цифрових платформ, інформаційних мереж та електронних комунікацій. Саме на цій базі вибудовуються критерії правоздатності, дієздатності та відповідальності учасників цифрових правовідносин.

Нижче подано узагальнену науково-теоретичну характеристику чотирьох підходів до правосуб'єктності «цифрових суб'єктів» у зарубіжній доктрині штучного інтелекту, з акцентом на критерії, наслідки та регуляторні ризики. Першою необхідно виділити Концепцію виключної правосуб'єктності [9], в межах якої зазначається, що суб'єктом цифрового права права може бути лише людина; і будь-які цифрові системи – лише об'єкти права або інструменти, що означає її будову за таким критерієм, як біологічна природа, воля й усвідомлення, що в результаті призводить до повної персоніфікації відповідальності (розробника, власника, оператора), та заборони «делегування» юридичної особи на машину, що при цьому характеризується такими ризиками як обмежена придатність у високій автоматизації, де складно простежити ланцюг контролю [10].

Іншою концепцією розуміння правосуб'єктності в цифровому праві необхідно виділити Концепцію мінімальної інклюзивності, де визнається обмежена автономність цифрових систем (вони можуть самостійно діяти в межах заданих правил), але без власної правоздатності, і яка побудована за таким критерієм, як функціональна спроможність діяти без постійного нагляду. Результативно реалізація Концепція мінімальної інклюзивності призводить до моделювання процесуальних ролей (реєстри дій, технічні «агенти»), однак права й обов'язки завжди належать людським та організаційним учасникам. До ризиків спокуса де-факто покладати «моральну провину» на алгоритм без належної атрибуції контролю Концепції мінімальної інклюзивності необхідно віднести спокусу де-факто покладати «моральну провину» на алгоритм без належної атрибуції контролю [11].



Наступною концепцією розуміння правосуб'єктності в цифровому праві є Концепція помірної інклюзивності, сутність якої полягає у припущенні розуміння правоздатності цифрового суб'єкта у вузько визначених сферах (наприклад, укладення мікродоговорів у межах «розумних» контрактів) за умови чіткої прив'язки до відповідального людського або корпоративного оператора, що не має власної «особистості» [12]. Отже, в основу розуміння Концепції помірної інклюзивності покладається такий критерій, як стабільні правила поведінки, аудитованість, можливість припинення дій і відзиву повноважень, що призводить до розширення обороту, зниження транзакційних витрат, але при цьому має такі ризики як відсутність чітких меж встановлення відповідальності суб'єктів якщо механізми контролю та страхування не працюють.

Необхідно виділити також Концепцію повної інклюзивності [13], де цифрова система може бути самостійною «особою», наділеною правами, інтересами і потенційно – обов'язками, що будується за таким критерієм, як: високий рівень самостійності цифрової системи, що володіє здатністю до самокорекції та стійкою ідентичністю. Наслідком реалізації Концепції повної інклюзивності є радикальна перебудова догми про суб'єкта права та формування потреби в нових режимах відповідальності та майнового забезпечення, що при цьому містить у собі такі ризики, як етична й практична неприйнятність (зміщення відповідальності з людей на «штучні інтелектуальні» одиниці; колізії з правами людини).

Наведений аналіз існуючих концептів визначення змісту цифрової правосуб'єктності свідчить про наявність ідеї збереження людської відповідальності, що є спільним мінімумом навіть для інклюзивних моделей.

У правопорядках, що дотримуються еволюційної траєкторії впровадження цифрових технологій, доцільною є методологія мінімальної або помірної інклюзивності правосуб'єктності цифрових систем. Її нормативна архітектоніка вибудовується не через наділення штучних систем автономною правосуб'єктністю, а через інституціоналізацію контрольованої делегації технічних функцій за умов підвищеної підзвітності людських носіїв відповідальності. Валідність делегування технічних функцій алгоритмічним системам забезпечується визначеними на рівні норм механізмами контролю та підзвітності. До обов'язкових умов належать: формалізована прозорість із доступом до відомостей про логіку, параметри й межі функціонування до початку застосування та після його завершення; регулярна внутрішня і зовнішня перевірка відповідності технічним стандартам і правовим вимогам; наявність страхового покриття потенційної шкоди; реєстрація відповідального куратора системи з чітко окресленими повноваженнями контролю, призупинення та припинення делегованих дій; ведення верифікованих журналів подій для фіксації операцій та їх причинно-наслідкових зв'язків; процедурні обмеження й механізми відзиву повноважень у разі ризику неправомірної або небезпечної роботи.

Зазначений комплекс вимог формує режим відповідального використання алгоритмічних рішень у публічно-правовій та приватно-правовій сферах. Він дає змогу включати такі рішення у чинні інститути без зміни засад персоніфікованої відповідальності, дотримання процесуальних вимог і забезпечення захисту прав людини. Режим функціонує за умови фіксації ролей учасників, процедурного розмежування повноважень і постійного моніторингу технічної інфраструктури.

Повна інклюзивність нині радше теоретична гіпотеза з високими етичними й процесуальними бар'єрами.

Для національної доктрини доцільно спиратися на модель «відповідального використання»: цифрові системи можуть виконувати технічні та представницькі дії, але правосуб'єктність і відповідальність – у людей і організацій, які ініціюють, контролюють і отримують вигоду від таких дій, що узгоджує інновації з принципом персоніфікації відповідальності та гарантіями прав людини [13].

Висновки. Проведений аналіз дозволяє окреслити концептуальні межі суб'єктності у цифровому праві та задати робочу модель її правового оформлення. Цифрове середовище змінює фактичні умови виникнення і реалізації прав та обов'язків, але не скасовує потреби у класичній тріаді правосуб'єктності: правоздатності, дієздатності й деліктоздатності. В основі належного правового статусу учасника цифрових відносин мають бути ідентифікованість, простежуваність дій і можливість ефективного притягнення до відповідальності. Саме ці умови є критерієм відмежування суб'єкта від інструмента.

Гібридна природа багатьох цифрових ролей поєднує приватно-правові та публічно-правові елементи, що зумовлює пріоритет публічного інтересу навіть у формально договірних відносинах. Інфраструктурний характер значної частини цифрових сервісів, включно



з «інтернетом речей», легітимує підвищені вимоги до безпеки, прозорості, захисту даних і підзвітності. Водночас ризики алгоритмічних рішень, зокрема можливість помилкових висновків та інформаційної асиметрії, підтверджують потребу у процесуальних гарантіях перевірки, оскарження та незалежного контролю.

Порівняння доктринальних підходів до правосуб'єктності «цифрових суб'єктів» свідчить, що повна інклюзивність із наданням машинним системам власної суб'єктності наразі не має достатніх юридичних і практичних підстав. Найбільш узгодженою з принципом персоніфікованої відповідальності є еволюційна модель мінімальної або помірної інклюзивності: алгоритмічним системам делегуються технічно визначені дії у межах чітко окресленого мандату, а права й обов'язки залишаються у людських та організаційних учасників, які ініціюють, контролюють і отримують вигоду від використання систем. Валідність такої делегації забезпечується нормативно зафіксованими вимогами до прозорості, аудитуваності, страхового покриття шкоди, реєстрації відповідального куратора, ведення верифікованих журналів подій і працездатних механізмів негайного зупинення та відзиву повноважень.

Для національної правової доктрини це означає доцільність поетапної кодифікації режиму «відповідального використання», який інтегрує цифрові ролі в чинні інститути без штучного розширення категорії «особа». Подальші зусилля варто спрямувати на розроблення узгоджених матеріальних і процесуальних стандартів ідентифікації та контролю у транскордонному обігу, а також на методики оцінки ризиків і механізми компенсації шкоди. Такий підхід забезпечує сумісність інновацій з базовими гарантіями правопорядку, зберігає цілісність системи суб'єктів права та створює передумови для безпечної й передбачуваної цифрової взаємодії.

Список використаних джерел:

1. Слабко С. М. Сутність та зміст правосуб'єктності людини: теоретичний, історичний та міжнародний аспекти. *Молодий вчений*. 2016. № 12. С. 615–618
2. Баранов О. А. Ідентифікація робота з штучним інтелектом як суб'єкта права. *Інтернет речей: проблеми правового регулювання та впровадження* : матер. Другої наук.-практ. конф. / упор. В. М. Фурашев, С. О. Дорогих. Київ, 2018. 168 с.
3. Bostrom N. *Superintelligence: Paths, dangers, strategies*. Oxford, 2014. 324 p.
4. Стефанчук М. О. Теоретичні засади цивільної правосуб'єктності фізичних осіб та особливості її здійснення : автореф. дис. ... д-ра юрид. наук : 12.00.03. Київ, 2020.
5. Bostrom N. *Superintelligence: Paths, dangers, strategies*. Oxford, 2014. 324 p.
6. Han-Wei Liu, Ching-Fu Liu, Yu-Jie Chen. Beyond State v Loomis: artificial intelligence, government algorithmization and accountability. *International journal of law and information technology*. 2019. URL: <https://www.researchgate.net/>
7. Скакун О. Ф. Теорія держави і права : підручник. Харків, 2021. 656 с.
8. Novelli C. A conceptual framework for legal personality and its application to AI An International Journal of Legal and Political Thought Volume 13, 2022 - Issue 2 <https://www.tandfonline.com/doi/full/10.1080/20403313.2021.2010936>
9. Company law actually provides us with several models under different legal systems, as shown by Shawn Bayern and others, 'Company Law and Autonomous Systems: A Blueprint for Lawyers, Entrepreneurs, and Regulators' (2017) 9 Hastings Science and Technology Law Journal 135
10. Ngair Naffine, *Law's Meaning of Life, Philosophy, Religion, Darwin and the Legal Person* (Hart Publishing 2009). A slightly different reading of legal personality as a cluster property is provided by Visa AJ Kurki, *A Theory of Legal Personhood* (Oxford Legal Philosophy 2019)
11. Digital inclusion and wellbeing. URL: <https://www.cedefop.europa.eu/en/print/pdf/node/144511>
12. Криклій О. А. Концепція цифрової інклюзії : сутність, фактори, елементи. *Економічні горизонти*. 2022. №3. С. 62-71 <http://eh.udpu.edu.ua/article/view/263631/259847>
13. Mulgan T. Corporate Agency and Possible Futures. *Journal of Business Ethics*. 2019. Vol. 154. P. 901–916. DOI: <https://doi.org/10.1007/s10551-018-3887-1>

