УДК 342.951(004.896)

КОСТЕНКО О.В., *доктор філософії (Ph.D.) з юридичних наук,* завідувач наукової лабораторії теорії цифрової трансформації і права наукового центру цифрової трансформації і права ДНУ ІІБП НАПрН України.
ORCID: https://orcid.org/0000-0002-**2131-0281.**
ЖУРАВЛЬОВ Д.В., *доктор юридичних наук, професор,* Офіс Президента України.
ORCID https://orcid.org/0000-0002-2205-6828.
ФУРАШЕВ В.М., *кандидат технічних наук, с.н.с.*, заступник директора з наукової роботи ДНУ ІІБП НАПрН України.
ORCID https://orcid.org/0000-0001-7205-724X.
ДНІПРОВ О.С., *доктор юридичних наук,* Офіс Президента України.
ORCID https://orcid.org/0000-0002-7157-9748.

ГЕНЕЗИС ПРАВОВОГО РЕГУЛЮВАННЯ WEB ТА МОДЕЛЬ ЕЛЕКТРОННОЇ ЮРИСДИКЦІЇ МЕТАВСЕСВІТУ*

Анотація. *У дослідженні розглядається трансформація наукових поглядів і підходів до проблеми доцільності та необхідності правового регулювання суспільних відносин, що виникають у зв'язку з еволюцією світової системи загальнодоступних електронних ресурсів у сфері передачі інформації та Інтернет-даних від Web 1.0, Web 2.0 до Web 3.0. Також досліджуються етапи формування ролі та місця електронної юрисдикції в публічних відносинах. Акцентовано увагу, що правове регулювання сучасних відносин у середовищах віртуальної та доповненої реальності з використанням технологій Web 3.0 на сьогодні відсутнє. Водночас існують прецеденти застосування окремих положень аналогового права для усунення правової невизначеності у віртуальному середовищі, наприклад, встановлення права власності на віртуальні немайнові активи, купівля/продаж віртуальних немайнових активів, відповідальність за незаконне привласнення віртуальних немайнових активів тощо. Очевидно, що проблема правового регулювання нормами аналогового права у віртуальному середовищі не може бути вирішена у повному обсязі. Вирішення цієї проблеми можливе шляхом створення комплексної електронної юрисдикції та розробки Великої хартії законів Metaverse для регулювання суспільних відносин у Metaverse та створення нової галузі електронного права. З огляду на актуальність проблеми, запропоновано модель електронної юрисдикції "Велика хартія законів Metaverse". Модель комплексної електронної юрисдикції Metaverse дозволить створити базовий понятійний апарат, доктринальні та нормативно-правові концепції, визначити об'єкти та суб'єкти правовідносин у Metaverse, встановити основні форми правовідносин та взаємовідносин у Metaverse. Це, в свою чергу, стане основою для реформування аналогового законодавства, часткової інтероперабельності в цифровому середовищі та розробки нових нормативно-правових актів у різних галузях права, а також стимулюватиме становлення нової електронної юрисдикції. У статті запропоновано конструкцію та основні елементи електронної юрисдикції, механізми відокремлення електронних правопорушень та взаємодії з аналоговими юрисдикціями. Електронна юрисдикція Великої хартії законів Metaverse забезпечить правове регулювання суспільних відносин як безпосередньо в Metaverse, так і в суспільних відносинах, пов'язаних з аналоговим та електронним світом.*

Ключові слова: *Метавсесвіт простір, Metaverse кіберпростір, електронні особистості, аватари, цифрові гуманоїди, електронна юрисдикція, віртуальна реальність, доповнена реальність, AI, кіберзаконодавство.*

Summary. *The study examines the transformation of scientific views and approaches to the problem of expediency and necessity of legal regulation of public relations, emerging from the evolution of the world system of public electronic resources in the transmission of information and Internet data from Web 1.0, Web 2.0 to Web 3.0. The stages of formation of the role and place of electronic jurisdiction in public relations are also investigated. Legal regulation of modern relations in virtual and augmented reality environments with the use of Web 3.0 technologies is not available today. At the same time, there are precedents for the application of certain provisions of analogue law to address legal uncertainties in the virtual environment, such as establishing ownership of virtual non-property assets, buying/selling of virtual non-property assets, liability for misappropriation of virtual non-property assets, etc. Obviously, the problem of legal regulation by the rules of analogue law in the virtual environment cannot be fully addressed. The solution to this problem is possible by creating a comprehensive e-jurisdiction and developing the Metaverse Grand Charter of Laws to regulate public relations in the meta-universe and to establish new branch of e-law. Given the urgency of the problem, the model of e-jurisdiction Grand Charter of Laws Metaverse is proposed. The model of complex electronic jurisdiction of Metaverse will allow to create basic conceptual apparatus, doctrinal and regulatory and legal concepts, to define objects and subjects of legal relations in Metaverse, to establish the basic forms of legal relations and mutual relations in Metaverse. This, in turn, will be the basis for reforming analogue legislation, partial interoperability in the digital environment and the development of new regulations in various areas of law and will stimulate the establishment of new e-jurisdiction. The study proposes the construction and basic elements of electronic jurisdiction, mechanisms for the separation of electronic offences and interaction with analogue jurisdictions. E-jurisdiction of the Metaverse Grand Charter of Laws will provide legal regulation of public relations both directly in Metaverse and in public relations related to the analogue and electronic world.*

Keywords: *Metaverse, Cyberspace, Electronic Personalities, Avatars, Digital Humanoids, Electronic Jurisdiction, Web 3.0 Decentraland, Virtual Reality, Augmented Reality, AI, Cyber Laws.*

Постановка проблеми. Історично наша цивілізація пройшла три комунікаційні епохи – вербальну, коли інформація в суспільстві передавалася лише усно; вербально-знакову, коли інформація передавалася як усно, так і за допомогою спеціальних символів – літер, слів, дій, подій; вербально-писемну, під час якої з'явилася друкована література. На сьогодні людство вступило в четверту епоху – епоху домінування електронної комунікації, де відбувається інтеграція інформаційно-комунікаційних технологій з попередніми формами комунікації. Ця епоха також пройшла шлях трансформації від архаїчних комп'ютерів до універсальних технологій. Метавсесвіт (далі – Metaverse) стає не тільки прогресивною епохою комунікації, але й новим науково-технічним центром розвитку суспільства, акумулятором і конструктором сучасних технологій, генератором нової гнучкості, інструментом, що допомагає людям виживати. Він стає самостійним середовищем, що функціонує паралельно з фізичним світом і законами, що вимагає певного переосмислення в нинішньому суспільстві [1].

Майбутній Metaverse стане великою відкритою масштабованою системою. Ця система створюється одночасно, охоплюючи кіберпростір, апаратні термінали, різних виробників і користувачів, надаючи широкий спектр сценаріїв застосування у віртуальній і доповненій реальності (AR/VR-середовищах), демонструючи кінцеву форму супер-екосистеми. Однак, без належного правового регулювання територія "віртуальної свободи" може перетворитися на деструктивний інструмент. Лише юриспруденція може забезпечити правове регулювання суспільних відносин у Metaverse [2].

Результати аналізу наукових публікацій. Сьогодні функціонує кілька різних Metaverse: Horizon Worlds, Ceek city, Baidu Xi Rang, Metaverse Facebook, Decentraland (Ethereum), Metaverse Emirates, Розширений віртуальний світ, Qualcomm Nvidia Omniverse із застосуванням технологій AI, AR/VR, голограм, XR-платформ, розподільчих реєстрів, нейронних мереж, квантових технологій та інших технічних рішень.

Очевидно, що регулювання юридичних прав у Metaverse є кордоном між електронним ігровим програмним забезпеченням та прикладними продуктами, а їх правове регулювання є фрагментарним і ситуативним, із застосуванням існуючих аналогових законів та нормативно-правових актів, таких як кодекси, положення та стандарти.

Існує підхід проведення "експериментальних правових режимів", відомих у світі як "регуляторні пісочниці" (SandBox), в рамках яких уряд визначає особливе правове регулювання на певний період у певних сферах для розвитку AR/VR-середовища.

Практика використання Metaverse вже має кілька прецедентів застосування окремих положень для вирішення правової невизначеності у віртуальному середовищі, таких як встановлення права власності на віртуальні нематеріальні активи, купівля/продаж віртуальних нематеріальних активів, відповідальність за незаконне привласнення віртуальних активів з ознаками різних видів дискримінації та морального насильства, поширення ідеологій расизму та фашизму тощо. Водночас з'являється дедалі більше видів деліктів, які мають природу виключно в Metaverse і повинні регулюватися виключно в межах Metaverse.

Нового ракурсу набуває проблема правового регулювання використання ідентифікаційних (персональних) даних, які стануть основою для створення та функціонування в Metaverse віртуальних аватарів або електронних гуманоїдів.

Метою статті є оцінка перспектив дослідження регулювання суспільних відносин, що створюються у віртуальному середовищі.

Виклад основного матеріалу.

Правове регулювання суспільних відносин в електронному середовищі на етапі розвитку технологій Web 1.0.

Кінець 1990-х – початок 2000-х років ознаменувався розвитком інформаційно-комунікаційних технологій, пов'язаних з поширенням інформації через Інтернет. На той час середовище електронних ресурсів являло собою статичні веб-сайти, призначені для читання та перегляду – технології Web 1.0. Ці інформаційні ресурси не містили інтерактивних елементів, мультимедіа, не мали функцій, які дозволяли користувачам спілкуватися онлайн, обмінюватися файлами тощо. Інструментом створення веб-сайтів був набір тегів мови розмітки HTML, що виконували функцію дизайну. Крім того, швидкість Інтернет-з'єднання була недостатньою для передачі зображень і відео.

Водночас багато вчених вбачали в цій технології перспективи не тільки для застосування в широких галузях науки і техніки, а й для формування нових суспільних відносин, відмінних від існуючих. Вчені сподівалися, що Web 1.0. та Інтернет дозволять суспільству створити нове середовище, вільне від домінування держави або не обтяжене надмірними правовими вимогами. Такий погляд сформувався під впливом Декларації про незалежність кіберпростору, автором якої був Д. Барлоу, та "Кодексу та інших законів кіберпростору" дослідника Л. Лессіга. У Декларації автор представив кіберпростір як простір такої влади, яка необхідна для встановлення свободи. Фактично, Д. Барлоу [3] заявив, що кіберпростір – це ліберальний віртуальний екстериторіальний анклав, який не підлягає жодній державній юрисдикції і призначений для людей,

вільних від будь-яких привілеїв і дискримінації, що повністю заперечує втручання держави в кіберпростір.

Також Л. Лессіг [4] визначив, що кіберпростір є неминучим, але нерегульованим, а суспільство в реальному світі керується чотирма основними регуляторами: правом, соціальними нормами, ринковими відносинами та "архітектурою/кодом" (технологічними можливостями). Жодна нація не може жити без цього, але жодна нація не може контролювати поведінку в кіберпросторі. Кіберпростір – це місце, де люди вільні від реального контролю.

На нашу думку, відповідно до технологічних можливостей часу та стану суспільних відносин, Л. Лессіг [4] вважав ключовим регулятором кіберпростору його архітектуру, технічні компоненти чи можливості, або "код". Саме код визначає порядок використання кіберпростору, подібно до того, як суспільні відносини в реальному просторі підлягають державному управлінню. Л. Лессіг стверджує, що у фундаментальному сенсі код кіберпростору – це його Конституція. Кодекс визначає умови, за яких люди отримують доступ до кіберпростору, і встановлює правила, що контролюють їхню поведінку. Кодекс формує власний суверенітет, який є альтернативою реальному фізичному життю.

У своєму творі Л. Лессіг [5] вперше звернув увагу на необхідність законів, які б одночасно забезпечували регулювання в кіберпросторі та мінімізували обмеження прав і свобод людини. Аналізуючи цю книгу, А. Візеу [6] визначає, що Л. Лессіг пропонує кілька способів боротьби з "похмурим" майбутнім: відкритий код і розвиток законодавства. На думку Л. Лессіга, відкритий код повинен діяти як своєрідний конституційний контроль, гарантуючи, що всі громадяни можуть "читати" і впливати на "створене" навколишнє середовище. Законодавчі заходи полягають в адаптації Конституції (США) до умов кіберпростору, аби гарантувати, що сучасні цінності будуть захищені та збережені в кіберпросторі.

Сьогодні такий підхід можна назвати спробою "м'якого" або демократичного регулювання кіберпростору, яке в основному базується на створенні правової бази для використання певних технологій і майже не передбачає правового регулювання суспільних відносин.

На той час розвиток державного законодавства, що регулює кіберпростір, відбувався за двома основними напрямами: внесення змін та доповнень до кримінальних кодексів та законотворчість шляхом розробки низки окремих законодавчих актів.

Перший напрям обрали країни, такі як Канада, Естонія, Німеччина, Швеція, Фінляндія, Австрія, Італія, Латвія, Нідерланди, Іспанія, Польща та Україна. Наприклад, Україна ввела окремий розділ "Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку" у статтях 361 – 363 та 363[1] Кримінального кодексу.

Щодо створення окремого законодавства варто відзначити наступні країни. Так, у 2000 році Республіка Індія прийняла Закон "India, Information Technology Act, 2000", який забезпечує правове регулювання у сфері інформаційно-комунікаційних технологій та технологій електронного підпису. Цей Закон цікавий запровадженням спеціального Кібер-апеляційного трибуналу для розгляду правопорушень, вчинених з використанням сучасних кібер-технологій. Крім того, цей Закон вводить класифікацію низки злочинів, включаючи комп'ютерне розповсюдження дитячої порнографії, електронне шахрайство та кібертероризм, що передбачає застосування державного примусу у вигляді штрафів або обмеження волі (статті 66, 66A-66E, 67, 67A-C, 71-79).

У США були прийняті нормативні акти для контролю за розповсюдженням порнографії та маркетингу [7], щодо шахрайства та пов'язаної з ним діяльності, пов'язаних із засобами доступу [8], щодо шахрайства та пов'язану з ним діяльності у комп'ютерній сфері [9], щодо шахрайства та пов'язаної з ним діяльність у сфері електронної пошти [10], щодо перехоплення телеграфно-телефонних та електронних повідомлень, а також усних повідомлень [11] та щодо доступу до збережених дротових та електронних повідомлень і записів транзакцій [12].

У цей самий період, інші країни ухвалили відповідні закони: Ізраїльський Закон про комп'ютери [13], Британський Закон про зловживання комп'ютерами [14] та Французький Закон про обробку даних, файли та свободи [15].

Як бачимо, суспільство і держави по-різному відреагували на появу інформаційно-комунікаційних технологій Web 1.0. З одного боку, ми маємо позицію формування ліберальних підходів "м'якого" регулювання кіберпростору, з іншого боку, держава, як регулятор суспільних відносин, встановлює або санкціонує загальнообов'язкові правила, які в певному сенсі обмежують права і свободи громадян, але ці правила забезпечуються заходами державного впливу, в тому числі державним примусом.

Розвиток "електронного" законодавства періоду технологій Web 2.0.

Починаючи з 2004 року, термін "Web 2.0" набув широкого поширення як такий, що характеризує наступний етап у розвитку інформаційно-комунікаційних технологій. Надалі його часто використовуватимуть разом з терміном "науково-технічна революція 4.0", оскільки вони описують значні зміни в суспільстві, що відбуваються внаслідок цифровізації.

Термін Web 2.0 означає комплексне поєднання таких технологій, як високошвидкісні Інтернет-протоколи, мобільний зв'язок п'ятого покоління (5G), а також численні стандарти бездротових мереж, інтерактивних веб-сайтів, ресурсів і платформ. Основна відмінність Web 2.0 від Web 1.0 полягає в тому, що контент створюється і виробляється користувачами, які є одночасно споживачами контенту і не є власниками технічних ресурсів. У той же час становлення Web 2.0 як середовища, вільного від домінування держави та необтяженого надмірним законодавством, характеризується появою мережі Darknet, кіберзлочинності, шкідливого програмного забезпечення, анонімних хакерів, криптовалюти, піратського контенту, деструктивної інформації тощо.

Разом з цим, активно розвивалося "електронне" законодавство – національне та міжнародне; у сфері інформаційного, кримінального, цивільного, адміністративного права; права інтелектуальної власності; а також технічного регулювання інформаційно-комунікаційних технологій через регламенти, правила, сертифікацію тощо. Наприклад, регулювання використання пристроїв Інтернету речей здійснюється одночасно із запровадженням технічного та правового регулювання [16], а управління використанням AI формується багатьма країнами відповідно до прийнятих Стратегій розвитку AI [17; 18].

Значна кількість міжнародних документів з питань інформаційного суспільства була розроблена та прийнята за ініціативи та участі неурядових організацій. При вирішенні інфраструктурних питань організації Інтернету позиція суверенної держави не завжди була і є головним пріоритетом. Ефективними регуляторами глобального інформаційного суспільства стали інструменти "м'якого" міжнародного права, які хоч і не мають обов'язкової сили, але надзвичайно швидко реагують на нові виклики та відображають інтереси всіх зацікавлених суб'єктів. Однак, необов'язкові правила мають значну нормативну та переконливу цінність. Тобто, технологічні інновації мають враховуватися при розробці відповідних нормативних актів [19]. Наприклад, Україна певний час не поспішала розвивати сучасне законодавство у сфері інформаційних

технологій і досить повільно проводила оцифрування як органів державної влади, так і перекодифікацію чинного законодавства. Проте, нещодавно Верховна Рада України розробила та прийняла низку сучасних нормативно-правових актів, таких як закони України "Про захист інформації в інформаційно-комунікаційних системах" [20], "Про електронні довірчі послуги" [21], "Про основні засади забезпечення кібербезпеки України" [22], "Про критичну інфраструктуру" [23], "Про віртуальні активи" [24] та Розпорядження Кабінету Міністрів України "Про схвалення Концепції розвитку сфери штучного інтелекту в Україні" [25]. У 2019 році було створено Міністерство цифрової трансформації України, завданням якого є оцифрування органів державної влади та механізмів державного управління. У судовій системі України впроваджуються такі цифрові механізми, як електронне судочинство та електронні реєстри.

Сучасне глобальне правове регулювання кіберпростору має значні досягнення, але вони нівелюються двома проблемами:

1) зосередженість права на формуванні юридичної відповідальності за кіберзлочини, як особливі види злочинів, що вчиняються з використанням цифрових інструментів у національному та транскордонному інформаційно-комунікаційному середовищі [26];

2) відсутність єдиного транснаціонального права, яке б забезпечувало суспільні відносини не лише на національному, а й на транснаціональному рівні [27], у якому постулат про те, що юрисдикція не повинна бути прив'язана до певної території чи кордонів, поступово набуває суспільного значення, а технічні можливості регулювання кіберпростору обмежені як об'єктивно, так і суб'єктивно [28].

На сьогодні наукові дискусії ведуться навколо питання територіальності кіберпростору в цілому та його окремих елементів. У тому вигляді, в якому кіберпростір функціонує зараз, його зв'язок з кордонами, національним та міжнародним правом все ще є досить чітким і пропорційно залежним. Існує реальна можливість технічного поділу кіберінцидентів на юрисдикції національного та міжнародного права. Тобто, фізичні кордони поки що тотожні нормативним, і право виконує в цих межах переважну більшість своїх функцій, а саме: економічну, політичну, ідеологічну, культурно-просвітницьку, регулятивну, виховну, охоронну та превентивну, з урахуванням національних особливостей.

Н. Цагуріас [29] у своєму дослідженні зазначає, що держава поширює свій суверенітет на фізичний рівень, тобто на інфраструктуру, розташовану на її території. Держава здійснює суверенну владу на своїй території. Держава також може захищати свій контроль над кіберпростором і кіберзлочинністю, що відбувається на її території. Крім того, держава зобов'язана захищати свій суверенітет, у тому числі й інформаційний. Тобто вона не тільки має право, але й зобов'язана контролювати безпеку інформації, яка проходить через її інфраструктуру, відбувається або завершується на її території, або передається через національні технічні вузли. Це свідчить про те, що згідно з чинним міжнародним правом, правила територіальних обмежень можуть поширюватися на кіберпростір у його нинішньому вигляді. Різниця між фізичним світом та кіберпростором полягає в тому, що влада у фізичному світі організована і діє на певних територіях, тоді як у кіберпросторі влада є прямою, не фрагментованою або ідентичною кордонам кіберпростору. Люди можуть переносити певні види діяльності та дії в кіберпростір, вони можуть номінально/віртуально заселяти кіберпростір, але вони ніколи не зможуть вилучити себе з реального світу в реальному житті. Це означає, що кіберпростір та його організація не можуть бути незалежними від держав, а отже, кіберпростір не може бути суверенним, оскільки влада в кіберпросторі опосередковано здійснюється державами.

Саме тому багато дослідників, таких як П. Домбровський, Ч. Демчак, Л. Лессіг, І. Шумський та інші, схиляються до проекції Вестфальської системи на "державний устрій" кіберпростору, адже завдяки їй було сформовано поняття суверенної держави та її основні ознаки, принципи рівності у відносинах у системі міжнародного права, запроваджено інститут міжнародних гарантій, рівності держав, поняття суверенітету, вирішення міжнародних проблем мирними засобами [30]. Водночас А. Сегура-Серрано [31], аналізуючи чинне законодавство, пропонує концепцію Спільної спадщини людства (далі – ССЛ), згідно з якою регулювання кіберпростору має здійснюватися міжнародним правом. Концепція ССЛ передбачає необхідність створення міжнародних органів управління Інтернетом, досягнення консенсусу щодо інтелектуальної власності та захисту прав, питань приватності, застосування сили та самооборони в кіберпросторі.

Майбутнє електронного правосуддя в кіберпросторі – окреме питання. Наразі існує чимало прикладів успішних рішень щодо локальних електронних судових систем, наприклад, у Федеративній Республіці Бразилія, КНР та інших країнах.

Е. Кедделл [32], Ю. Размєтаєва та С. Размєтаєв [33] слушно наголошують на певних ризиках електронного правосуддя, які полягають у складнощах синхронної інтеграції основних електронних інструментів у національні системи правосуддя, а також можливій упередженості алгоритмів електронного правосуддя. Причому це може бути як навмисна упередженість, закладена розробниками, так і ненавмисна упередженість, що дублює упередження, сформовані в аналоговому правосудді.

Прикладом ризикованого правосуддя є дослідження Н. Д. Гервассіс [34]. Він поділяє теорію Л. Лессіга про кіберпросторове право, засноване виключно на кіберпросторовому коді, і пропонує використовувати протокол CyberLaw. CyberLaw – це перероблений відповідно до правил існуючих правових систем мережевий протокол, який трансформується в альтернативну форму непрямого "невидимого" законодавства. Тобто, частина правових ризиків у кіберпросторі блокується і коригується протоколом CyberLaw ще на етапі їх створення. Слід зазначити, що сам автор визнає, що такий підхід має великий потенціал для зловживань у разі неправильного застосування.

Metaverse структура на основі технологій Web 3.0.

Сьогодні ми є спостерігачами, учасниками та користувачами новітніх інформаційних технологій, які вже отримали загальну назву Web 3.0. Технології Web 3.0 – це інформаційно-комунікаційні децентралізовані електронні віртуальні екомережі, які функціонують на основі блокчейну, електронних нейронних мереж, машинного навчання, штучного інтелекту, Інтернету речей, криптовалют, віртуальної та доповненої реальності, постійної доступності. Згідно з дослідженнями E. Özkahveci, F. Cívek та G. Ulusoy [35], термін "Metaverse" наразі є найпопулярнішим, має багато інтерпретацій і використовується для опису процесів оцифрування майже в усіх сферах людського життя.

Web 3.0 є стартовим майданчиком для початку науково-технічної революції 5.0 і наступного етапу розвитку людства – електронних гуманоїдів і Metaverse. Однозначного визначення Метапростору (Метавсесвіту) не існує.

Metaverse характеризує нескінченну кількість віртуальних світів, в яких і між якими соціально взаємодіють фізичні та цифрові суб'єкти та об'єкти, наділені певними властивостями: правами, обов'язками та відповідальністю. Ключовим елементом децентралізованого світу є ідентифікація фізичних та цифрових суб'єктів та об'єктів. Ідентифікаційні дані є перепусткою до Metaverse.

Враховуючи основні риси постіндустріального суспільства і тенденції перехідного періоду до нього від індустріального, можна спрогнозувати, що Metaverse пройде наступні три фази розвитку:

- перша фаза – оболонка Metaverse (базовий рівень програмного забезпечення та інженерії), суб'єкти та об'єкти повністю залежні від розробників та власників оболонки;
- друга фаза – оболонка Metaverse, суб'єкти та об'єкти належать розробникам і частково належать власникам/користувачам;
- третя фаза – Metaverse не належить конкретним розробникам, управління суб'єктами та об'єктами здійснюється або власником (апаратна біоідентифікація), або автономно (суб'єкти та об'єкти наділяються функціоналом та правами, притаманними власнику).

Суб'єктами Metaverse вважатимуться лише фізичні особи, а до категорії об'єктів будуть віднесені юридичні особи, аватари, електронні особистості, віртуальні цифрові твори AAI та ASI, цифрові гуманоїди, нематеріальні електронні активи всіх форм і видів тощо. Ймовірно, що на третьому етапі розвитку Metaverse ряд об'єктів, таких як аватари, електронні особистості, віртуальні цифрові твори класу ASI та цифрові гуманоїди, будуть переведені до категорії суб'єктів, оскільки на законодавчому рівні вони будуть наділені певними правами та обов'язками, притаманними лише суб'єктам.

Наразі Metaverse перебуває на початковому етапі свого становлення та розвитку [36]. Його структуру можна класифікувати як взаємопов'язані технологічні інформаційні домени або електронні інформаційні корпорації. Метакорпорації конкурують у боротьбі за користувача, фінанси, продукти і технології. Користувачі корпоративних мета-всесвітів все ще можуть бути анонімними або використовувати псевдоніми для реєстрації облікових записів і створення безособових аватарів чи електронних особистостей [37], а це знижує довіру до Метавсесвіту в цілому і залишає підґрунтя для зловживань і правопорушень.

На нашу думку, в найближчому майбутньому Metaverse буде більш структурованим і складатиметься з таких елементів: Персональний Metaverse (Personal Metaverse, PM), Колективний Metaverse (Collective Metaverse, CM), Корпоративний Metaverse (Corporate Metaverse CorpM), Metaverse Конфедерації (Confederate Metaverse (CfM), Державний Metaverse (State Metaverse, SM) та Мега Metaverse (MMV/WM) (Рис. 1).

Персональний Metaverse (PM) означає, що кожен суб'єкт (учасник Metaverse) може створити власний електронний Metaverse (аватар, електронний гуманоїд, електронна особистість) за власною уявою і перебувати в ньому свідомо і виключно особисто, наприклад, за аналогією з романом "Робінзон Крузо" англійського письменника Д. Дефо.

Колективний Metaverse (CM) – добровільне електронне об'єднання суб'єктів та об'єктів Metaverse, яке функціонує за взаємною згодою, але з обов'язковим дотриманням загальноприйнятих базових вимог або правил права MMV.

Корпоративний Metaverse (CorpM) – добровільне, виробниче, наукове, комерційне, релігійне або інше електронне об'єднання суб'єктів та об'єктів Metaverse, яке діє за корпоративними правилами, якщо вони не суперечать загальноприйнятим основним вимогам або правилам MMV.

Конфедеративний Metaverse (CfM) – політичне об'єднання суб'єктів та об'єктів Metaverse, кожен з яких зберігає свою незалежність, а всі разом поважають взаємно узгоджені норми права.

Державний Metaverse (SM) – це електронна держава, що має зовнішні та внутрішні електронні характеристики держави, а також електронні предметно-просторові, інформаційно-публічні, нормативно-правові та інституційні ознаки.

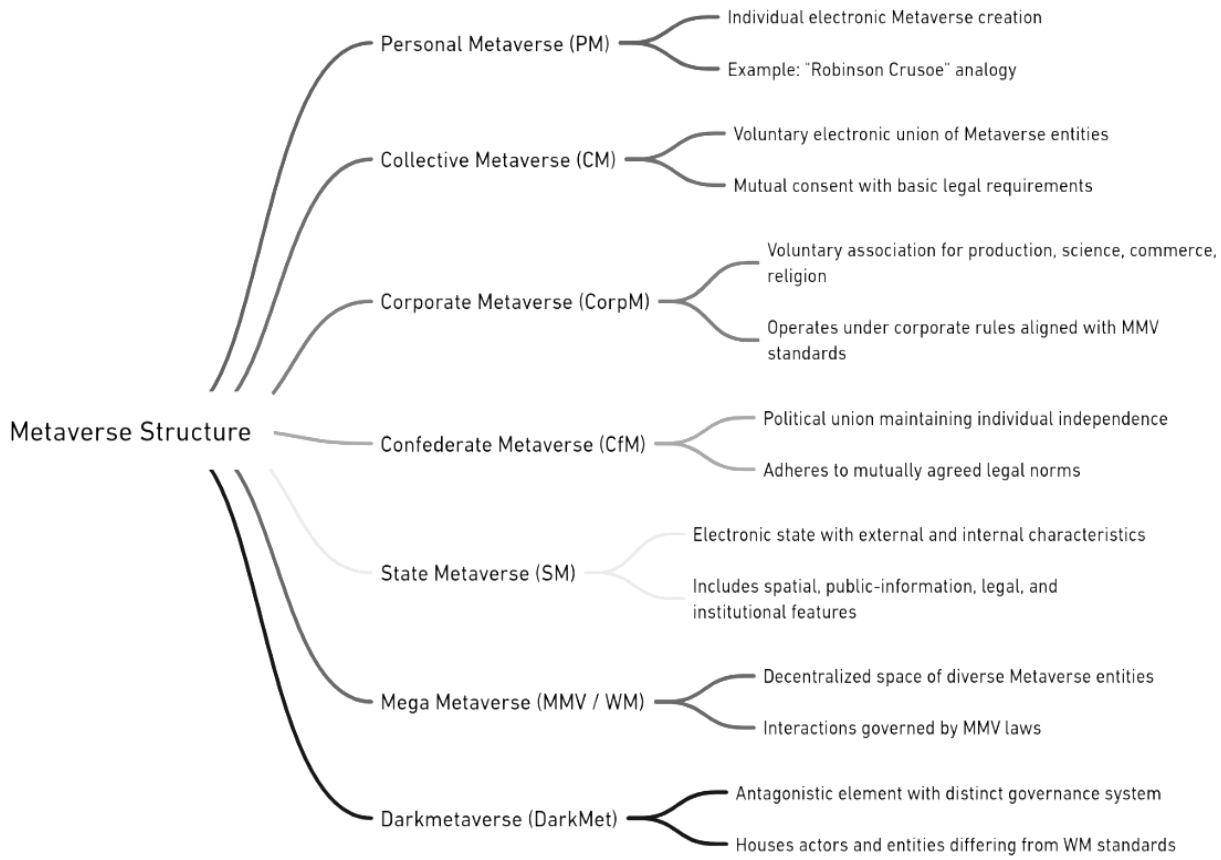

Рис. 1. Структура Metaverse.

Мега Metaverse або Білий Metaverse (MMV or WM) – це загальний децентралізований електронний простір, в якому існує безліч персональних, колективних, корпоративних, конфедеративних і державних Metaverse, які взаємодіють один з одним за законами WM.

Доцільно в Metaverse також передбачити можливість існування Darkmetaverse (DarkMet) як необхідного антагоністичного елементу Metaverse, в якому можуть бути зосереджені суб'єкти, об'єкти і Metaverse з системою самоврядування, відмінною від тієї, що прийнята у WM.

Оскільки Metaverse розглядається як інформаційно-комунікаційна соціальна екосистема, що створює, підтримує, розвиває і забезпечує функціонування суспільних відносин в електронній віртуальній формі, доречно зазначити, що "електронна юрисдикція" Metaverse – це комплексна галузь права, яка регулює суспільні відносини, що становлять її предмет – суспільні відносини в Metaverse, наприклад, між Metaverse і фізичним світом [38]. Кожен суб'єкт матиме особистий унікальний аватар, а суб'єкти/об'єкти матимуть унікальні паспорти власності. Суб'єкти та об'єкти можуть здійснювати різні види діяльності – фінансову, наукову, творчу, соціальну, громадську тощо.

Наприклад, Республіка Барбадос у 2021 році оголосила про відкриття свого віртуального посольства в Metaverse, а його дипломатичний комплекс будується в Decentraland. Посол Барбадосу в Об'єднаних Арабських Еміратах стверджував, що "уряди можуть діяти разом, коли земля перестає бути фізичною землею, а обмеження більше не є частиною рівняння". Він також зазначив, що малі країни не мають фізичної та фінансової можливості підтримувати 197 дипломатичних місій по всьому світу, але Metaverse забезпечує паритет з такими великими країнами, як Америка чи Німеччина.

Інші країни також мають досвід віртуальних посольств – Швеція та Естонія відкрили посольства в Metaverse Second Life.

Об'єднані Арабські Емірати вже стали лідером у Metaverse, будуючи сучасну цифрову економіку, впроваджуючи політику та розвиваючи нормативно-правову базу в таких сферах, як віртуальні активи, штучний інтелект та захист даних.

Так, державний регуляторний орган ОАЕ Управління з управління віртуальними активами Дубаю (VARA) відкрив представництво у віртуальному світі The Sandbox, яке працюватиме з приватним сектором та відповідними державними установами над створенням законодавчої та наглядової бази для цифрових активів. Крім того, будуть розроблені правила боротьби з відмиванням грошей і відстеження транскордонних транзакцій, щоб забезпечити прозорість і безпеку для бізнесу та інвесторів. Цифрові активи, такі як криптовалюта, невзаємозамінні цифрові активи, токени (NFT) тощо, підтримуватимуться єдиною законодавчою та регуляторною базою.

Авіакомпанія Emirates оголосила про створення бренду в сфері Метавсесвіту (Emirates Metaverse), а також колекційних і корисних незамінних токенів для своїх клієнтів і співробітників. Також у Metaverse з'явився перший у світі центр обслуговування клієнтів, розроблений Міністерством охорони здоров'я та профілактики ОАЕ.

Як показує реальність – суспільні відносини в Metaverse створюються, встановлюються і розвиваються всупереч скептицизму окремих вчених, експертів і політиків.

Проблеми правового регулювання суспільних відносин у Metaverse.

Відмінність сучасного кіберпростору Web 2.0 від Metaverse Web 3.0 полягає в тому, що переважна більшість процесів і процедур у сучасному кіберпросторі регулюється нормативно-правовими актами, у тому числі й певне коло суспільних відносин. Однак, з огляду на вищезазначене, саме процеси моделювання/прогнозування трансформації існуючих та становлення нових суспільних відносин у Metaverse потребують особливої уваги, а саме визначення їх спрямованості та характеристик. Це є основою для створення механізмів та засобів їх правового регулювання. Крім того, необхідно визначитися з наступним:

- що саме вважати "суспільними відносинами в Metaverse" та "відносинами в Metaverse";
- коли, як і в якому обсязі електронні суб'єкти та об'єкти наділяються правами, притаманними людині;
- яка форма правосуддя буде застосовуватися в Metaverse.

Вже зараз електронні особистості, аватари та електронні гуманоїди можуть якісно дублювати зовнішність і поведінку як уявної людини, так і реального власника аватара або його користувача. Ідентичне відтворення людини, реальної особи вже не вважається прерогативою медицини і вимагає надійного контролю за використанням ідентифікаційних даних людини "червоної" групи (за авторською класифікацією) [39] або надчутливих персональних даних (за класифікацією GDPR). Віртуальні активи, смарт-контракти, NFT, віртуальні землі (Метавсесвіти Decentraland та The Sandbox) – це реальні електронні нематеріальні активи Metaverse, з якими відбуваються цілком реальні, юридично значимі дії. Правила і норми поведінки в Metaverse все ще створюються шляхом проекції фізичного світу і мають корпоративний характер. Однак, намітилася тенденція міграції і перенесення норм суспільної моралі в Metaverse шляхом моделювання космополітичних е-соціальних відносин за відсутності чітких атрибутів електронної держави і державного устрою Metaverse.

Від віртуального до реального: йдеться вже не про імітацію реального світу, а про саморозвиток на основі віртуального світу, який може не тільки формувати незалежну від реального світу систему цінностей, а й впливати на реальний світ [40].

Основною проблемою правового регулювання суспільних відносин у Metaverse є відсутність єдиного правового механізму регулювання суспільних відносин, що виникають у Metaverse.

Створення механізмів правового регулювання суспільних відносин у Metaverse має вирішити багато законодавчих проблем, пов'язаних з відмінностями в нормативних актах різних юрисдикцій. У більшості правових систем діють архаїчні нормативно-правові акти, які сформульовані без урахування можливого виникнення суспільних відносин з використанням електронних технологій Metaverse. В окремих випадках ці закони можуть регулювати окремі питання використання інформаційних технологій, але сфера їх дії часто є або вузькою, або неоднозначною, що створює ситуацію правової невизначеності.

Модернізація національного законодавства з метою забезпечення правової сумісності в різних юрисдикціях часто підміняється прийняттям тимчасових правил або підзаконних актів. Наразі правові інститути національних правових доктрин все ще мають важелі регулювання загальних процесів цифровізації суспільства. Окремі випадки "електронних правопорушень" розглядаються судовою системою через проекцію чинного законодавства, формуючи таким чином основу для майбутнього електронного правосуддя в Metaverse. Різні культурні особливості та державні пріоритети призводять до суттєвих відмінностей у мотивації та вироках, а сучасне законодавство, хоча і є прогресивним за своєю суттю, не має повноцінного практичного застосування або перетворюється на малоефективні закони, що носять декларативний характер.

Однак певні технології Metaverse вже існують і потребують регулювання, оскільки формують нові суспільні відносини, в яких є суб'єкти та об'єкти, в тому числі й ті, що мають властивості суб'єктів.

Поки що ці властивості штучно створюються розробниками і формуються ними відповідно до їхньої уяви або уяви науковців чи замовників проектів.

Електронне правосуддя, як і загальноприйняте законодавство, в Metaverse взагалі відсутнє, або в його ролі використовуються окремі положення місцевих, національних нормативно-правових актів і традиційне "аналогове" правосуддя, яке дуже повільно трансформується відповідно до розвитку електронних суспільних відносин в Metaverse.

Metaverse модель електронної юрисдикції на основі технологій Web 3.0.

Становлення права в Metaverse об'єктивно починається з етапу проекції законів фізичного суспільства на електронні суспільні відносини. Але, з огляду на те, що Metaverse є всеосяжним, проекція законів різних країн не матиме бажаного ефекту. Саме випереджальний розвиток відповідних базових положень глобального електронного законодавства Metaverse надасть поштовх для модернізації та вдосконалення національного законодавства у сфері оптимізації та підвищення ефективності його використання.

Правове регулювання суспільних відносин у Metaverse потребує розробки комплексної електронної юрисдикції, що ґрунтується на новітньому базовому законодавстві – Великій хартії законів Metaverse (GLM). На нашу думку, GLM має включати наступні ключові частини:

- Конституція – Велика хартія законів.
- Загальні норми, склад законів Великої хартії.
- Загальне право WM.
- Судова система WM.

- Закон про електронний Офіс WM.
- Режим транскордонної взаємодії у WM.
- Кодекс фундаментальних технічних регламентів WM.
- Сертифікат управління ідентифікацією WM.
- Кодекс немайнових електронних активів WM.
- Кримінальний електронний кодекс WM.
- Кодекс кіберзахисту WM.
- Військовий регламент WM.
- Великий електронний судовий кодекс WM.
- Інші нормативно-правові акти.

Електронна юрисдикція, електронне правосуддя є одним з ключових елементів електронних суспільних відносин у Metaverse. Е-правосуддя на початковому етапі може базуватися на традиційному "аналоговому" правосудді, яке трансформується відповідно до розвитку електронних суспільних відносин у Metaverse.

Створення механізмів правового регулювання суспільних відносин у Metaverse має вирішити багато законодавчих проблем, пов'язаних з відмінностями в нормативних актах різних юрисдикцій, що регулюють використання інформаційно-комунікаційних технологій, процедури ідентифікації, авторське право, право власності на немайнові активи, відповідальність за заподіяння шкоди, перелік злочинів і примусові заходи держави за їх вчинення.

Чинне "законодавство аналогової епохи" слід взяти за основу і почати формувати Велику хартію законів Metaverse. Конституція, Статут, загальне право, судова система повинні мати структури, які максимально сприятимуть демократичному та легітимному функціонуванню WM.

Комплекс основоположних технічних регламентів – це техніко-юридичні документи, які мають зафіксувати еталонні програмні коди, що будуть використовуватися для визначення на законодавчому рівні правового статусу та права власності на немайнові електронні активи, такі як NFT або контент.

Кодекс немайнових електронних активів WM призначений для врегулювання відносин з немайновими активами та встановлення права електронної власності та електронної інтелектуальної власності.

Кримінальний електронний кодекс WM призначений для визначення видів правопорушень з розвитком і використанням інформаційно-комунікаційних технологій та технологій Metaverse, а також встановлення державних та інших примусових заходів у разі вчинення правопорушень. Кодекс кібербезпеки – техніко-юридичний документ, який має встановити на законодавчому рівні еталонні програми, адміністративні, управлінські та технічні заходи щодо забезпечення кібербезпеки, які будуть обов'язковими для виконання всіма суб'єктами та об'єктами WM.

Військовий регламент WM – це сукупність статутів, інструкцій та правил на випадок військових дій у віртуальному просторі. Великий електронний судовий кодекс WM міститиме правила та алгоритми електронної юрисдикції, визначатиме її суб'єкти, об'єкти, територіальність, спеціалізацію тощо. Важливу роль у WM відіграватиме електронний Офіс WM. Фактично, це ядро електронної юрисдикції WM (Рис. 2).

Електронний Офіс WM працюватиме з використанням AAI та ASI і виконуватиме завдання Центрального аналітичного центру та Розпорядника електронних повідомлень щодо електронних інцидентів (електронних правопорушень). Електронний Офіс WM прийматиме запити про е-інциденти від усіх WM та об'єктів WM, аналізуватиме склад правопорушень відповідно до законодавства WM та самої Великої хартії законів

Metaverse, формуватиме ланцюжок "територіальної відповідальності" та складатиме перелік учасників провадження у справах. Наприклад, якщо електронне правопорушення стосується національного "аналогового" законодавства, то таке правопорушення буде розглядатися в межах національної юрисдикції. У випадку, якщо електронне правопорушення стосується CfM або SM юрисдикцій різних Metaverse, таке правопорушення розглядатиметься Палатою Великого електронного суду WM. На даному етапі становлення WM і його Великої хартії законів Metaverse національне законодавство потребує реконфігурації або модернізації для забезпечення правової сумісності та функціонування Metaverse, що формується, з метою упорядкування суспільних відносин та діяльності у сфері інформаційних технологій.

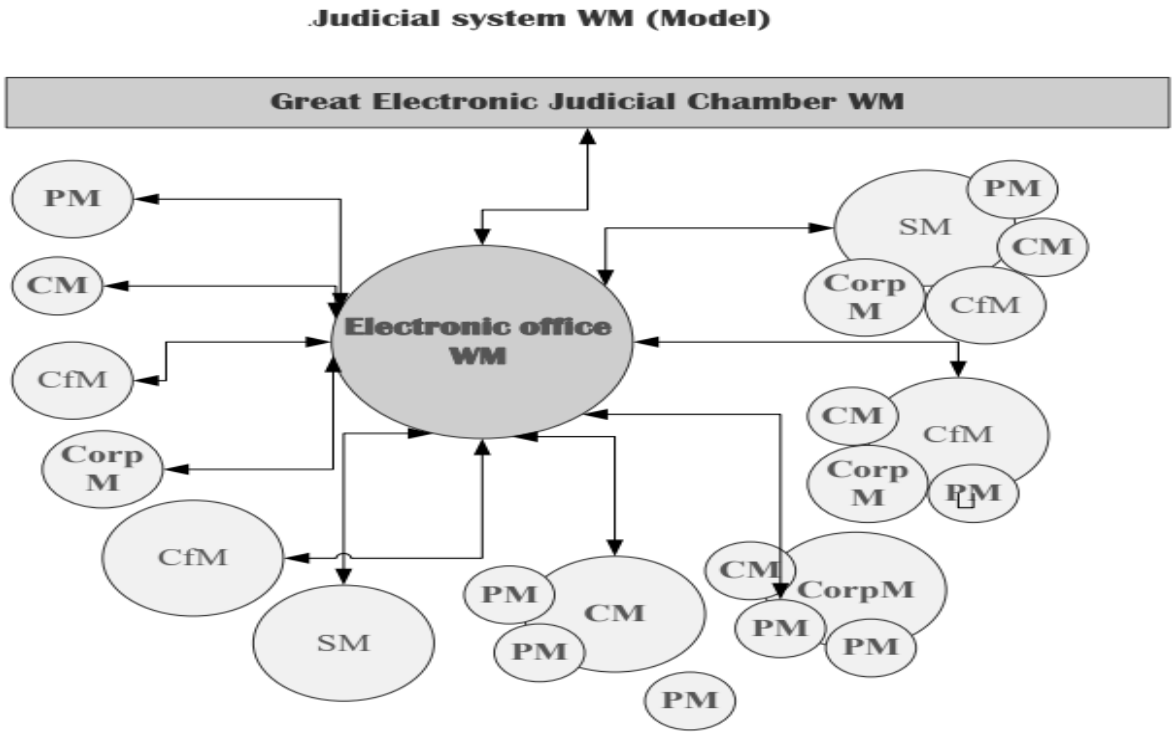

Рис. 2. Судова система WM (модель).

Правила і норми поведінки у WM все ще створюються відповідно до проекції фізичного світу і мають корпоративний характер. Однак спостерігається тенденція міграції і перенесення норм суспільної моралі в Metaverse шляхом моделювання космополітичних е-соціальних відносин за відсутності чітких атрибутів електронної держави і державного устрою Metaverse. Розвиток глобального електронного законодавства Metaverse дасть поштовх до модернізації національних законодавств.

Модель електронної юрисдикції окреслить WM найбільш важливі та проблемні питання, які виникають в процесі еволюції людства та розвитку технологій віртуальної реальності, а також сформує основу електронного права для регулювання суспільних відносин у Metaverse.

Основними цінностями та об'єктами Metaverse, що підлягають захисту в електронній юрисдикції, є:

1. Довіра та репутація, які формуються кожним суб'єктом та об'єктом Metaverse з моменту його реєстрації в Metaverse за допомогою технології блокчейн.

2. Цілісність, достовірність та обґрунтованість ідентифікаційних даних, за допомогою яких здійснюється ідентифікація фізичних та юридичних осіб, інших суб'єктів та об'єктів у Metaverse:

- біометрична ідентифікація фізичних осіб, як особливо цінний та унікальний атрибут або код доступу до Metaverse;
- ідентифікаційні дані IoT (універсальні ідентифікатори об'єктів систем ідентифікації (OID), електронний код продукту (EPC), універсальний унікальний ідентифікатор (UUID) та міжнародний ідентифікатор мобільного зв'язку (IMEI));
- ідентифікаційні дані AI, AAI та ASI (електронні сертифікати квантових криптографічних систем, які захищатимуть ядро AI від зовнішніх атак);
- ідентифікаційні дані інших типів об'єктів.

3. Права інтелектуальної власності та право власності на немайнові електронні активи в Metaverse.

4. Інформаційна безпека та кібербезпека.

Створення Великої хартії законів Metaverse потребує залучення великої кількості фахівців у галузі права та сучасних електронних технологій, а також спеціалістів, які проводитимуть міждисциплінарні дослідження у багатьох сферах.

Проект "Велика хартія законів Metaverse" – це проект, який буде розроблятися за ініціативи та участі організацій, корпорацій Metaverse та науково-дослідних інститутів, а також провідних фахівців Metaverse, які працюють у галузі права та сучасних електронних технологій.

Висновки.

Епоха індустріалізації та індустріального суспільства добігає кінця. Людство чітко взяло курс на побудову нового суспільного устрою, який на сьогоднішній день найбільше визначається як постіндустріальне суспільство. Вже очевидно, що точка "повернення" пройдена. Людство перебуває на етапі переходу від індустріального до постіндустріального суспільства. Цей шлях буде непростим, потребуватиме вирішення і врегулювання дуже складних питань і протиріч, у тому числі питань національної та міжнародної юрисдикції. Однією з особливостей постіндустріального суспільства є максимальне охоплення кіберпростору та його ефективне використання у поєднанні з природним простором практично у всіх сферах життєдіяльності людини. Тобто, по суті, формуючи постіндустріальне суспільство, людство формує кіберцивілізацію у Metaverse.

Таким чином, людство, будуючи постіндустріальне суспільство, змушене одночасно вирішувати питання формування Metaverse і алгоритми забезпечення ефективності його використання. Очевидно, що розвиток Metaverse буде поступовим, послідовним.

Ранній етап розвитку Metaverse є перспективним стартом для дослідження суспільних відносин, що створюються у віртуальному середовищі, можливості орієнтуватися на закони і правила, що буде актуальним при поетапному створенні суспільства цифрових гуманоїдів у Metaverse. Це особливо важливо з огляду на те, що ці технології, як і багато інших, мають багатоцільовий характер.

Основною проблемою правового регулювання суспільних відносин у Metaverse є відсутність єдиного правового механізму регулювання навіть фундаментальних суспільних відносин, що виникають у Metaverse.

Вирішення цієї проблеми можливе шляхом створення комплексної електронної юрисдикції та Великої хартії законів Metaverse для регулювання суспільних відносин у Metaverse та формування нової галузі права.

Створення комплексної електронної юрисдикції Metaverse потребує:

- проведення досліджень у галузі інформаційного права щодо напрямів розвитку базового понятійного апарату, доктринальних і нормативно-правових концепцій; розпізнавання структур комбінованих понять і концептуальних схем, визначення об'єктів і суб'єктів правовідносин у Metaverse;
- вивчення та перекодування чинних і прогнозованих норм сучасного інформаційного, адміністративного, цивільного, кримінального, трудового права, права власності, інтелектуальної власності, захисту персональних даних та інших галузей та інститутів права, а також інститутів державної безпеки, інформаційної та кібербезпеки.

Використана література

1. Shaoying, P., Pengzhi, C., Xinru, F., Lifu, Q., Junhui, H., and Liwen, J. (2022). Ten conjectures: Interpretation of the development trend of the most comprehensive metaverse. *IT Times.* Available at: https://m.jiemian.com/article/7078158.html

2. Pengfei, Z. (2022). If the metaverse is the future then what is the future of the metaverse? Xinhuanet. Available at: http://www.xinhuanet.com/techpro/20220120/264c62d021974eee81d70c35083ef91a/c.html

3. Barlow, J. P. (1996). Declaration of the Independence of Cyberspace. Available at: https://www.eff.org/cyberspace-independence

4. Lessig, L. (1999). Code and other laws of cyberspace. New York: Basic Books.

5. Lessig, L. (1998). The Laws of Cyberspace. Taiwan Net '98 Conference. Available at: https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf

6. Viseu, A. (2001). Code and Other Laws of Cyberspace. By Lawrence Lessig. *Canadian Journal of Communication*, 26(1), 179-180.

7. USA, 15 U.S.C. §§ 7701-7713 (2003).

8. USA, 18 U.S.C. § 1029 (2015). USA, 18.

9. U.S.C. § 1030 (2020). USA, 18.

10. U.S.C. § 1037 (2003).

11. USA, 18 U.S.C. §§ 2510-2523 (2022).

12. USA, 18 U.S.C. §§ 2701-2713 (2018).

13. Israel, The Computer Law (1995).

14. United Kingdom, Computer Misuse Act (1990).

15. France, Act Relating to Data Processing, Files and Freedoms (1978).

16. Kostenko, O. (2021b). Identyfikatsiia IoT. *Juris Europensis Scientia*, 1, 77-83. Available at: https://doi. org/10.32837/chern.v0i1.177.

17. Zhang, D., Mishra, S., Brynjolfsson, E., Etchemendy, J., Ganguli, D., Grosz, B., Lyons, T., Manyika, J., Niebles, J., Sellitto, M., Shoham, Y., Clark, J., and Perrault, R. (2021). Artificial Intelligence Index Report, 2021.

18. Zhang, D., Maslej, N., Brynjolfsson, E., Etchemendy, J., Lyons, T., Manyika, J., Ngo, H., Niebles, J., Sellitto, M., Sakhaee, E., Shoham, Y., Clark, J., and Perrault, R. (2022). Artificial Intelligence Index Report, 2022.

19. Kyryliuk, O. (2015). Miake Pravo Yak Normatyvna Osnova Hlobalnoho Informatsiinoho Suspilstva. Actual problems of international relations, Release 125 (part I), pp. 106-117. Available at: http://apir.iir.edu.ua/index.php/apmv/article/view/2664/2368

20. Ukraine, Act on Protection of Information in Information and Communication Systems (1994).

21. Ukraine, Act on Electronic Trust Services (2017).

22. Ukraine, Act on The Main Principles of Ensuring Cyber Security of Ukraine (2017).

23. Ukraine, Act on Critical Infrastructure (2022).

24. Ukraine, Act on Critical Infrastructure (2022). Ukraine, Act on Virtual Assets (2022).

25. Ukraine, Order of The Cabinet of Ministers on The Approval of The Concept of The Development of Artificial Intelligence in Ukraine (2020).

26. Riek, M. and Böhme, R. (2018). The costs of consumer-facing cybercrime: an empirical exploration of measurement issues and estimates. Journal of Cybersecurity, 4(1), 2057-2085. Available at: https://doi.org/10.1093/cybsec/tyy004

27. Razmetaeva, Y., Ponomarova, H., and Bylya-Sabadash, I. (2021). Jurisdictional Issues in the Digital Age. Ius Humani. Law Journal, 10(1), 167-183. Available at: https://doi.org/ 10.31207/ih.v10i1.240

28. Vartanian, T. (2000). Whose Laws Rule the Internet? A U.S. Perspective on the Law of Jurisdiction in Cyberspace. International Law FORUM du droit international, 2(3), 96-201. Available at: https://doi.org/10.1163/157180400322765009

29. Tsaugourias, N. (2018). Law, Borders and the Territorialisation of Cyberspace. *Indonesian Journal of International Law,* 15(4). Available at: https://doi.org/10.17304/ijil.vol15.4.738

30. Demchak, C. and Dombrowski, P. (2014). Cyber Westphalia: Asserting State Prerogatives in Cyberspace. *Georgetown Journal of International Affairs*, International Engagement on Cyber III: State Building on a New Frontier 2013-14, 29-38.

31. Segura-Serrano, A. (2006). Internet Regulation and the Role of International Law. In A. von Bogdandy and R. Wolfrum, (eds.), Max Planck Yearbook of United Nations Law, 10, 191-272.

32. Keddell, E. (2019). Algorithmic Justice in Child Protection: Statistical Fairness, Social Justice and the Implications for Practice. Social Sciences, 8(10), 281-303. Available at: https://doi. org/10. 3390/socsci8100281

33. Razmetaeva, Y. and Razmetaev, S. (2021). Justice in the Digital Age: Technological Solutions, Hidden Threats and Enticing Opportunities. Access to Justice in Eastern Europe, 2(10), 104-117. Available at: https://doi.org/10.33327/AJEE-18-4.2-a000061.

34. Gervassis, N. (2004). From Laws for Cyberspace to Cyber Laws (Literally): Integration of Legal Norms into Internet Protocols and Law for Closed Digital Management Communities. SCRIPT-Ed, 1(2), 259-271. Available at: https://doi.org/10.2966/scrip.010204.259

35. Özkahveci, E., Cívek, F. and Ulusoy, G. (2022). Endüstri 5.0 Döneminde Metaverse (Kurgusal Evren)'Ün Yeri. *Journal of social, humanities and administrative sciences*, 50(8), 398-409. Available at: https://doi.org/10.31589/joshas.929

36. Özgökçeler, D. (2021). The methods and ways of implementation of the metaverse concept that can be transferred to the general audience of its cultural and commercial potential in-converted. Academia.edu. Available at: https://www.academia.edu/70076301/he_Methods_And_Ways_Of_Implementation_Of_The_Metaverse_Concept_That_Can_Be_Transferred_To_The_General_Audience_Of_Its_Cultural _And_Commercial_Potential_In_converted

37. Kostenko O. (2022). Electronic Jurisdiction, Metaverse, Artificial Intelligence, Digital Personality, Digital Avatar, Neural Networks: Theory, Practice, Perspective. *World Science*, 73(1), 1-13. Available at: https://doi.org/10.31435/rsglobal_ws/30012022/7751

38. Wyss, J. (2021). Barbados Is Opening a Diplomatic Embassy in the Metaverse. Bloomberg. Available at: https://www.bloomberg.com/news/articles/2021-12-14/barbadostries-digital-diplomacy-with-planned-metaverseembassy?leadSource=uverify%20wall

39. Kostenko, O. (2021a). Identification Data Management: Legal Regulation and Classification. *Scientific Journal of Polonia Universit*, 43(6), 198-203. Available at: https://doi.org/10.23856/4325

40. Pu, Q. L., Pang, Y., Peng, B., Hu, C. J., and Zhang, A. Y. (2022). Metaverse report − Future is here. Global XR indurstry insight. Available at: https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/technologymedia-telecommunications/deloitte-cn-tmt-metaverse-report-en-220321.pdf

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~