

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**Національний університет
«Одеська юридична академія»**

Кафедра права інтелектуальної власності та патентної юстиції

ВІРТУАЛЬНА (ЦИФРОВА) ОСОБА

НАВЧАЛЬНО-МЕТОДИЧНИЙ ПОСІБНИК

для підготовки здобувачів вищої освіти
спеціальності D8 «Право» / 081 «Право»,
СЗ «Міжнародні відносини» / 29 «Міжнародні відносини»
та D9 «Міжнародне право» / 293 «Міжнародне право»

Одеса

УДК 347.15/17:004.7(073)
B526

*Рекомендовано навчально-методичною радою
Національного університету «Одеська юридична академія»
(протокол № _____ від _____ 2025 р.)*

Укладачі:

Харитонова О.І. – член-кореспондент НАПрН України, д.ю.н, професор, завідувач кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА» (ORCID ID: 0000-0002-9681-9605)

Галупова Л.І. – к.ю.н., доцент, доцент кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА» (ORCID ID: 0000-0001-6263-2773)

Кирилюк А.В. – к.ю.н., доцент, доцент кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА» (ORCID ID: 0000-0002-3051-6599)

Мартинюк І.В. – к.ю.н., доцент кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА» (ORCID ID: 0000-0001-7067-3188)

Рецензенти:

Яворська О.С. – завідувач кафедри інтелектуальної власності, інформаційного та корпоративного права Львівського державного університету ім. І. Франка, доктор юридичних наук, професор.

Булеца С.Б. – завідувач кафедри цивільного права та процесу Ужгородського національного університету, доктор юридичних наук, професор.

Дудченко В.В. – професор кафедри загальної теорії права та держави, доктор юридичних наук, професор, Вчений секретар ради НУ «ОЮА», Заслужений юрист України

Віртуальна (цифрова) особа : навч.-метод. посіб. для підготовки здобувачів вищої освіти спеціальності D8 «Право» / 081 «Право», СЗ «Міжнародні відносини» / 29 «Міжнародні відносини» та D9 «Міжнародне право» / 293 «Міжнародне право» / О.І. Харитонова, Л.І. Галупова, А.В. Кирилюк, І.В. Мартинюк Нац. ун-т «Одеська юрид. академія». – Одеса : Видавництво «Фенікс», 2025. – 160 с.

Навчально-методичний посібник містить завдання до практичних занять і самостійних робіт, теоретичні відомості з детальним описом матеріалу та контрольні запитання.

Призначений для підготовки здобувачів вищої освіти спеціальності D8 «Право» / 081 «Право», СЗ «Міжнародні відносини» / 29 «Міжнародні відносини» та D9 «Міжнародне право» / 293 «Міжнародне право» з метою закріплення лекційного матеріалу і підготовки до практичних і самостійних занять з дисципліни «Віртуальна (цифрова) особа».

**УДК 342.7:004.9
П201**

© О.І. Харитонова, Л.І. Галупова,
А.В. Кирилюк, І.В. Мартинюк, 2025

ISBN

ЗМІСТ

ВСТУП	4
ЗАГАЛЬНІ ПОЛОЖЕННЯ.....	6
ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ.....	10
ПЛАН ПРАКТИЧНИХ ЗАНЯТЬ	95
САМОСТІЙНА РОБОТА	97
ПИТАННЯ ДО ЗАЛІКУ	116
РЕКОМЕНДОВАНИЙ ПЕРЕЛІК ДЖЕРЕЛ.....	118

ВСТУП

Стрімкий розвиток цифрових технологій, Інтернет-комунікацій та штучного інтелекту зумовив появу нових соціально-правових феноменів, серед яких особливе місце посідає віртуальна (цифрова) особа. Сьогодні вона постає не лише як технічний інструмент або сукупність даних про фізичну особу, а як складне багатовимірне явище, що поєднує в собі ознаки правової категорії, соціальної конструкції та елементу комунікаційного простору. Її формування та функціонування безпосередньо пов'язані з трансформацією уявлень про приватність, ідентичність та немайнові права людини в умовах цифровізації суспільства.

Віртуальна особа є результатом взаємодії індивіда із цифровим середовищем. Вона відображає цифрову ідентичність користувача, його образ у соціальних мережах, цифрових сервісах та інформаційних системах, що надає нових вимірів традиційним уявленням про особу у праві. У сучасному інформаційному просторі саме цифрова репрезентація нерідко визначає репутацію, імідж та соціальний статус індивіда, а також впливає на його економічні та культурні можливості. Відтак, зростає значення правового регулювання відносин, пов'язаних з існуванням і функціонуванням віртуальної особи, зокрема у сфері захисту персональних даних, права на зображення, права на забуття, а також управління цифровою спадщиною.

Важливим аспектом є інтеграція віртуальної особи у правовий дискурс. Вона зумовлює необхідність комплексного підходу до дослідження проблем правового статусу суб'єктів у цифровому середовищі. Постає питання про можливість розширення традиційної категорії правосуб'єктності з урахуванням новітніх цифрових феноменів, зокрема цифрових аватарів, меморіальних акаунтів, штучно створених профілів та алгоритмів, які імітують поведінку людини. У зв'язку з цим актуалізується дискусія щодо співвідношення прав людини у фізичному та віртуальному вимірах, а також перспективи закріплення окремих гарантій для захисту прав у цифровій сфері.

Окрему увагу привертає питання охорони прав інтелектуальної власності, пов'язаних із цифровою особою. Контент, створений у віртуальному середовищі (фото, відео, блоги, цифрове мистецтво, алгоритми), стає частиною особистого немайнового та майнового надбання індивіда, що формує так звану «цифрову спадщину». Водночас наукова й практична проблематика управління цим спадком після смерті людини вимагає врегулювання з огляду на баланс між приватними інтересами спадкоємців, суспільними потребами та правами третіх осіб.

У глобальному масштабі віртуальна особа виступає предметом міждисциплінарних досліджень – від правових і філософських до соціологічних та культурологічних. З одного боку, вона уособлює новий рівень комунікації та самовираження особи в інформаційному суспільстві; з іншого – породжує низку правових викликів, пов'язаних із захистом честі, гідності, права на приватне життя, свободи вираження поглядів і права на інформацію.

Отже, актуальність вивчення дисципліни «Віртуальна (цифрова) особа» визначається необхідністю:

- теоретичного осмислення феномену цифрової особи як правової та соціальної категорії;
- формування доктринальних підходів до її правового статусу;
- вдосконалення законодавчого регулювання із врахуванням міжнародних стандартів та європейського досвіду;
- підготовки фахівців, здатних орієнтуватися у складних питаннях цифрових правовідносин, що мають ключове значення для розвитку сучасної правової системи.

Таким чином, дисципліна спрямована на комплексне дослідження сутності, правової природи та соціальної ролі віртуальної особи, а також на формування у здобувачів права глибокого розуміння сучасних викликів, що постають у процесі цифровізації суспільства і трансформації концепції прав людини у цифровому вимірі.

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Програма курсу зосереджує увагу на актуальних питаннях формування, функціонування та правового регулювання віртуальних (цифрових) осіб у сучасному інформаційному суспільстві, з урахуванням міжнародного досвіду та тенденцій цифровізації.

Предметом навчальної дисципліни є правові засади існування віртуальної особи як правового та соціального феномену.

Навчальна дисципліна є спеціальною та забезпечує підготовку здобувачів освіти до розуміння та аналізу проблем цифрової ідентичності, цифрової спадщини, а також правових наслідків використання штучного інтелекту у створенні та підтримці цифрових аватарів.

Програма курсу спрямована на підготовку фахівців, здатних орієнтуватися у складних питаннях сучасних цифрових правовідносин, що охоплюють сферу приватного права.

Міждисциплінарні зв'язки: курс пов'язаний з навчальними дисциплінами «Право інтелектуальної власності», «Медіаправо», «Інтернет-право», «Бренд особи в соціальних мережах», «Захист іміджевих прав» «Захист немайнових прав у сучасному інформаційному суспільстві».

Метою дисципліни є ознайомлення здобувачів освіти з поняттям віртуальної (цифрової) особи, особливостями її правового статусу, використанням у соціальних мережах, комунікаційних технологіях та бізнесі, а також з сучасними тенденціями у сфері цифрових прав людини.

Завдання курсу:

- розкрити поняття та сутність віртуальної (цифрової) особи у широкому та вузькому значенні;
- визначення особливостей правового статусу цифрової особи;
- дослідити співвідношення категорій «цифрове життя», «цифрова спадщина», «цифрове безсмертя»;
- сформувати уявлення про особливості охорони та захисту немайнових прав особи у віртуальному середовищі;

- розвинути навички правового аналізу та оцінки перспектив впровадження використання віртуальної особи в професійну діяльність юриста.

У процесі вивчення дисципліни вирішуються завдання:

- засвоєння теоретичних положень та відповідних норм чинного законодавства України, міжнародних актів і європейських стандартів у сфері цифрових прав людини та захисту персональних даних;
- вивчення наукових підходів і доктринальних концепцій до визначення правового статусу цифрової особи;
- аналіз зарубіжної практики у сфері правового регулювання цифрової ідентичності.

Після вивчення дисципліни здобувачі освіти

повинні знати:

- основні поняття: «цифрове життя», «віртуальна особа», «цифрова спадщина», «цифрове безсмертя»;
- особливості охорони зображення людини в цифровому середовищі;
- правові підходи до реалізації права на приватне життя, таємницю листування, право на забуття;
- міжнародні стандарти у сфері захисту персональних даних;
- етичні та правові аспекти використання цифрових аватарів і штучного інтелекту.

Вміти:

- користуватися спеціальною термінологією, аналізувати наукові джерела і нормативно-правові акти у сфері цифрових прав;
- визначати проблеми та пропонувати шляхи вдосконалення законодавства щодо охорони немайнових прав у цифровому середовищі;
- аналізувати судову практику у сфері захисту персональних даних;

Форми вивчення: лекції, практичні заняття, самостійна робота здобувачів освіти, індивідуальні завдання (реферати, презентації), підсумковий контроль (залік).

Лекції забезпечують теоретичне підґрунтя курсу та розкривають ключові питання правового статусу цифрової особи.

Самостійна робота включає підготовку до лекцій, опрацювання літератури, вирішення фабул та тестів.

Практичні заняття мають на меті закріплення знань, обговорення проблемних питань, аналіз кейсів, моделювання ситуацій, пов'язаних із використанням цифрової особи.

Індивідуальні завдання (реферати, доповіді, презентації) розвивають вміння формулювати аргументовану позицію з дискусійних питань.

Методи навчання та викладання включають поєднання традиційних і інтерактивних підходів:

Пояснювально-ілюстративний метод – подання навчальної інформації із використанням презентацій та візуальних матеріалів.

Дискусійний метод – обговорення спірних питань, організація дебатів та панельних дискусій.

Метод кейс-стаді – аналіз змодельованих ситуацій, пов'язаних із застосуванням цифрових технологій у правовому середовищі.

Інтерактивні методи навчання – рольові ігри, моделювання судових засідань, робота в малих групах.

Форми поточного контролю знань: опитування, можлива письмова контрольна робота або колоквиум (усно).

Форми підсумкового контролю знань: залік.

Критерії оцінювання знань здобувачів освіти:

Оцінка виставляється за національною шкалою: «зараховано» або «не зараховано». При оцінці за основу слід брати повноту і правильність виконання завдань.

1. Оцінка «5» (відмінно) ставиться в тому разі, коли відповідь здобувача освіти правильна, повна, послідовна, логічна; здобувач освіти впевнено володіє фактичним матеріалом з усього курсу, вміє застосовувати його щодо конкретно поставлених завдань.

2. Оцінка «4» (добре) ставиться в тому разі, коли відповідь правильна, послідовна, логічна, але здобувач освіти допускає у викладі окремі незначні пропуски фактичного матеріалу вміє застосовувати його щодо конкретно поставлених завдань.

3. Оцінка «3» (задовільно) ставиться у тому разі, коли здобувач

освіти володіє більшою частиною фактичного матеріалу, але викладає його не досить послідовно і логічно, допускає істотні пропуски у відповіді, невірно формулює основні теоретичні положення та причинно-наслідкові зв'язки.

4. Оцінка «2» (незадовільно) ставиться в тому разі, коли здобувач освіти виявляє незнання більшої частини фактичного матеріалу або відмовляється відповідати на поставлені питання.

Шкала оцінювання: національна та ECTS

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		Екзамен	Залік
90-100	A	Відмінно	зараховано
82-89	B	Добре	
74-81	C		
64-73	D	Задовільно	
60-63	E		
1-59	Fx	Незадовільно	не зараховано
1-34	F		

2. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Віртуальна реальність, кіберпростір як середовище існування віртуальних відносин (2 год).

1. Історія виникнення Інтернету.
2. Правова природа мережі Інтернет.
3. Доктринальні підходи до розуміння понять «віртуальна реальність» та «кіберпростір».
4. Ознаки кіберпростору.
5. Сфера правового регулювання віртуальної реальності.

Теоретичні відомості

1. Історія виникнення Інтернету

Інтернет, як глобальна мережа, що забезпечує обмін інформацією між мільйонами користувачів у всьому світі, має витоки у військово-наукових проєктах другої половини ХХ ст. Його історія безпосередньо пов'язана з розвитком інформаційних технологій, потребою в безпечних комунікаційних каналах та глобалізаційними процесами.

Перші кроки були зроблені у США в умовах «холодної війни». У 1957 р. запуск Радянським Союзом першого штучного супутника «Супутник-1» спонукав американський уряд до активізації наукових досліджень у сфері комунікацій та обчислювальної техніки. У 1958 р. було створено Агентство передових дослідницьких проєктів Міністерства оборони США (ARPA), яке стало центром розробки нових інформаційних систем.

У 1969 р. в межах проєкту ARPANET було реалізовано перші успішні спроби передачі даних між комп'ютерами, розташованими в різних університетах (Каліфорнійський університет у Лос-Анджелесі, Стенфордський дослідницький інститут, Університет Юти та Каліфорнійський університет у Санта-Барбарі). Ця мережа стала прототипом сучасного Інтернету. У 1973 р. Вінтон Серф і Роберт Кан розробили принципи протоколу TCP/IP, які згодом стали універсальним стандартом передачі даних у глобальній мережі.

У 1980-х роках до розвитку Інтернету активно долучилися науково-дослідні установи та університети. У 1983 р. протокол TCP/IP офіційно став базовим для ARPANET, що забезпечило сумісність мережевих систем у світі. У 1989 р. співробітник Європейської організації з ядерних досліджень (CERN) Тім Бернерс-Лі запропонував концепцію World Wide Web (WWW) – гіпертекстової системи, яка дозволяла зручно переглядати та поширювати інформацію у мережі. Це стало фундаментом для комерційного розвитку Інтернету у 1990-х роках.

З розширенням кількості користувачів, появою графічних браузерів (Mosaic, Netscape) та запуском пошукових систем (Yahoo!, Google) Інтернет із науково-військової мережі перетворився на універсальну інфраструктуру для комунікацій, бізнесу, освіти та розваг. На сучасному етапі Інтернет є не лише технічною мережею, але й простором формування соціальної, культурної та правової реальності, що вимагає комплексного правового регулювання.

2. Правова природа мережі Інтернет.

Інтернет є складним багаторівневим феноменом, що поєднує технічну інфраструктуру, інформаційний простір та соціально-правові відносини. Його правова природа залишається дискусійною, адже мережа не має єдиного центру управління, не підпорядковується конкретній державі та функціонує на основі відкритих стандартів.

Інтернет як глобальне публічне благо. Частина дослідників визначає Інтернет як глобальне публічне благо, подібне до космосу чи світового океану. Він забезпечує вільний доступ до інформації, сприяє розвитку науки, освіти, демократії. Водночас його функціонування підтримується як державами, так і приватними акторами та громадянським суспільством¹.

Інтернет як простір реалізації прав людини. З правової точки зору Інтернет є середовищем здійснення та захисту основоположних прав, зокрема свободи вираження поглядів (ст. 19 Міжнародного пакту про громадянські і політичні права), права на приватність

1 Mueller M. Networks and States: The Global Politics of Internet Governance. Cambridge, MA: MIT Press, 2010. 336 p.

(ст. 8 Європейської конвенції з прав людини), а також права на доступ до інформації та інші.

Транскордонний характер мережі Інтернет. Через транснаціональний характер Інтернет не може підпорядковуватися виключно юрисдикції однієї держави. Його регулювання здійснюється через міжнародні механізми:

- ООН (резолюції ГА щодо прав людини в Інтернеті);
- Міжнародний союз електрозв'язку (ITU) – розробка технічних стандартів;
- ICANN – адміністрування доменних імен та IP-адрес;
- Конвенція Ради Європи про кіберзлочинність, 2001.

Інтернет як простір приватноправових відносин

Мережа є платформою для електронної комерції, обігу інтелектуальної власності, укладання електронних договорів. Приклади:

- Регламент eIDAS (EU) № 910/2014 – електронна ідентифікація та довірчі послуги;
- Директива (EU) 2019/790 – авторське право у цифровому середовищі;
- UDRP (Uniform Domain-Name Dispute-Resolution Policy) – вирішення доменних спорів.

Правова природа Інтернету має комплексний характер: він є глобальним публічним благом; виступає середовищем реалізації прав людини; є предметом міжнародного та національного правового регулювання; створює приватноправові та публічно-правові відносини;

Таким чином, Інтернет доцільно визначати як світовий цифровий простір із багаторівневою правовою природою, де поєднуються міжнародно-правові, публічно-правові та приватноправові елементи.

Виділимо ключові характеристики мережі Інтернет, які, на наш погляд, мають суттєве значення для розуміння природи цього явища та формування його визначення як правової категорії.

По-перше, Інтернет є інформаційно-телекомунікаційною мережею. Слід мати на увазі, що використання терміну «інформаційна мережа» щодо Інтернету є недостатньо коректним, оскільки він не конкретизує ані форму переданої інформації, ані суб'єктів її передачі, водночас охоплюючи як технічні мережеві утворення (телефонні,

телеграфні та інші), так і соціальні структури (агентурні мережі, бізнес-спільноти тощо), що здійснюють інформаційну взаємодію.

Разом із тим, поряд із Інтернетом існують інші мультисервісні мережі, які також функціонують на основі протоколу IP, зокрема Next Generation Network. У науковій літературі підкреслюється необхідність точного технічного визначення відмінностей Інтернету від інших подібних мереж, які використовують аналогічні програмні засоби та технології, проте не є Інтернетом.

По-друге, Інтернет виступає глобальною комп'ютерною мережею, що об'єднує десятки мільйонів користувачів у понад 150 країнах світу, забезпечуючи їх взаємодію за допомогою різноманітних каналів зв'язку.

По-третє, Інтернет передбачає всезагальний доступ користувачів. Зокрема, Рекомендації щодо розвитку та використання багатомовності та загального доступу до кіберпростору, ухвалені на 32-й сесії Генеральної конференції ЮНЕСКО, містять комплекс заходів із забезпечення такого доступу: формування відповідної державної та міжнародної політики; створення механізмів на локальному, національному, регіональному та міжнародному рівнях, які сприяють доступності Інтернету через прийнятні тарифи на телекомунікаційні та інтернет-послуги; стимулювання інтернет-провайдерів до встановлення пільгових тарифів для окремих категорій користувачів.

Крім того, право на доступ до Інтернету як універсальної (загальнодоступної) послуги закріплено Директивою Європейського Союзу про універсальну послугу в редакції 2009 року (2009/136/ЄС), яка передбачає обов'язок забезпечити кожному громадянину ЄС доступ до мінімального набору електронно-комунікаційних послуг належної якості та за прийнятною ціною, зокрема доступ до мережі Інтернет².

2 ДИРЕКТИВА ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ 2009/136/ЄС від 25 листопада 2009 року про внесення змін до Директиви 2002/22/ЄС про універсальну послугу та права користувачів щодо електронних комунікаційних мереж та послуг, Директиви 2002/58/ЄС про опрацювання персональних даних і захист приватності у сфері електронних комунікацій, Регламенту (ЄС) № 2006/2004 про співпрацю між національними органами, відповідальними за забезпечення виконання законів про захист прав споживачів. URL: [Директива Європейського ... | від 25.11.2009 № 2009/136/ЄС](#)

У науковій юридичній літературі навіть піднімається питання щодо можливості визнання права на доступ до Інтернету як самостійного конституційного (основного) права людини.

В українському законодавстві загальнодоступні (універсальні) телекомунікаційні послуги визначено як мінімальний набір певних послуг нормованої якості, доступний усім споживачам на всій території України. Водночас, передбачений статтею 62 Закону України «Про телекомунікації» перелік таких послуг не містить посилання на доступ до мережі Інтернет. З огляду на міжнародні стандарти та рекомендації Європейського Союзу така невідповідність є неприйнятною та потребує законодавчого врегулювання.

По-четверте, одним із фундаментальних принципів обміну інформацією в Інтернеті є принцип анонімності, закріплений у Декларації про свободу комунікацій в Інтернеті, прийнятій Комітетом міністрів Ради Європи 28 травня 2003 року. Анонімність передбачає, що з метою забезпечення свободи вираження поглядів, обміну інформацією та захисту від мережевого стеження слід поважати волю користувача не розкривати свою особистість. Серед інших проголошених у Декларації принципів виділяються: правила щодо змісту інформації (контенту); саморегуляція або спільна регуляція; відсутність попереднього державного контролю; ліквідація бар'єрів для участі індивідів в інформаційному співтоваристві; свобода надання послуг через Інтернет; обмежена відповідальність постачальників послуг за зміст інформації.

Разом із тим, незважаючи на проголошений принцип анонімності, постійно виникає потреба у визначенні ідентичності користувачів глобальної мережі, операторів послуг та власників розміщеної в Інтернеті інформації. Вирішення цього питання є надзвичайно важливим для запобігання вчиненню протиправних дій в мережі та забезпечення правового регулювання відносин, які формуються у віртуальному просторі та за своєю природою потребують регуляції. У зв'язку з цим на міжнародному рівні необхідно чітко окреслити межі допустимої анонімності в Інтернеті та визначити випадки її законодавчого обмеження.

По-п'яте, Інтернет має складну багаторівневу інфраструктуру. Інтернет є багат шаровим утворенням, яке об'єднує багаторівневі мережі. На найнижчому рівні розташована фізична інфраструктура, канали зв'язку та інфраструктура доступу до мереж. Над цим рівнем функціонує адресний простір (IP-адреси), над яким існує надбудова у вигляді доменних імен та системи DNS. На верхніх рівнях ієрархії Інтернету знаходяться прикладні сервіси та додатки, зокрема поштові сервіси, пошукові системи та веб-сайти. При цьому функціонування базових компонентів такої інфраструктури підпадає під юрисдикцію окремих держав, в яких закріплюється правовий режим об'єктів інфраструктури та порядок їх використання. Архітектура мережі Інтернет базується на принципі багаторівневої передачі повідомлень. Згідно з еталонною моделлю взаємодії відкритих систем ISO/OSI, на верхньому рівні формується повідомлення, яке під час передачі послідовно проходить усі рівні системи до найнижчого (фізичного) рівня, на якому воно безпосередньо доставляється адресату.

По-шосте, функціонування Інтернету носить транскордонний характер, що зумовлює необхідність одночасного транскордонного управління мережею та регулювання в межах національних юрисдикцій питань її використання. Так, функції управління кореневою зоною системи доменних імен верхнього рівня (DNS), координації розподілу глобального пулу IP-адресного простору та номерів портів регіональним Інтернет-реєстрам, а також забезпечення зберігання і розподілу імен та номерів Інтернет-протоколів виконуються Адміністрацією адресного простору Інтернету (Internet Assigned Numbers Authority, IANA). Крім того, до ключових організацій, що здійснюють транскордонне управління технологічною інфраструктурою Інтернету, належать п'ять регіональних Інтернет-реєстрів, відповідальних за призначення IP-адрес кінцевим користувачам у межах певних територій, а також локальні Інтернет-реєстратори, серед яких – інтернет-провайдери. Адміністрування адресного простору українського сегмента мережі здійснює об'єднання підприємств «Український мережевий інформаційний

центр» (UANIC) у координації з міжнародною системою адміністрування Інтернету.

Слід також зазначити, що у загальновизнаному визначенні поняття «управління Інтернетом», розробленому робочою групою при Генеральному секретарі ООН, реалізовано так званий «підхід усіх зацікавлених сторін». Його сутність полягає в тому, що, окрім органів державної влади та міжнародних міжурядових організацій, в управлінні Інтернетом беруть участь приватний сектор (комерційні організації, бізнес-спільнота тощо) та громадянське суспільство (технічні й академічні товариства, експерти та інші зацікавлені сторони).

По-сьоме, екстериторіальний характер побудови та функціонування мережі Інтернет зумовлює необхідність інтеграції міжнародного та національного правового регулювання. На сучасному етапі міжнародно-правове регулювання відносин в Інтернеті здійснюється переважно через механізми так званого «м'якого права», що реалізується у вигляді різноманітних рекомендацій, резолюцій та декларацій, які приймаються міжнародними організаціями, зокрема Міжнародним союзом електрозв'язку, Всесвітньою організацією інтелектуальної власності, ООН, ЮНЕСКО, Радою Європи, Інтернет-корпорацією з присвоєння імен та номерів (ICANN) та іншими.

Хоча положення таких документів формально не мають обов'язкової юридичної сили і їх виконання державами залежить виключно від авторитету організацій, що їх прийняли, існує нагальна потреба у створенні міжнародного договору, який би унормував питання поняття мережі Інтернет, її правового режиму, структури, застосованого права, вирішення спорів та інших аспектів функціонування мережі на національному, регіональному та глобальному рівнях. При цьому таке регулювання повинно враховувати закладені в основу функціонування мережі принципи децентралізації та саморегулювання.

Поряд із міжнародно-правовим регулюванням, на рівні національного законодавства повинна здійснюватися регламентація об'єктів фізичного рівня інфраструктури мережі Інтернет, а також різноманітних відносин, що виникають у процесі її використання.

Враховуючи викладене, можна запропонувати наступне визначення мережі Інтернет як правової категорії: Інтернет – це глобальна, загальнодоступна інформаційно-телекомунікаційна мережа зі складною багаторівневою інфраструктурою, яка функціонує на засадах транскордонного управління та забезпечує можливості створення, розміщення, поширення та доступу до інформації, а також надання пов'язаних із цим інформаційних послуг.

Інтернет слід розглядати як специфічне середовище існування людини, суспільства та держави. Більше того, існують процеси та явища, у яких участь людини можлива лише через цю мережу, зокрема онлайн-правочини, віртуальне спілкування, створення вебсайтів, ведення блогів та поширення інформації у режимі «один клік». Значення мають також сучасні гаджети, здатні відстежувати фізіологічні та активні показники людини, а алгоритми Інтернету аналізують вподобання, смаки та поведінку користувачів, що безпосередньо впливає на комунікацію та повсякденне життя.

3. Доктринальні підходи до розуміння понять «віртуальна реальність» та «кіберпростір».

Доктринальні підходи до розуміння понять «віртуальна реальність» та «кіберпростір» демонструють значну багатовимірність і відображають розвиток наукових уявлень про цифрову реальність. У сучасній літературі віртуальна реальність трактується не лише як технічний феномен, пов'язаний із використанням спеціалізованого обладнання для створення ефекту занурення у змодельоване середовище³, але й як нова форма соціальної взаємодії, що дозволяє індивіду відчувати «присутність» у штучно створеному просторі. М. Хейм, аналізуючи онтологічні аспекти віртуальної реальності, визначав її як «онтичне середовище», у якому людина набуває нових способів буття⁴. У правовій науці ж віртуальна реальність розглядається як об'єкт правового регулювання у контексті охорони інтелектуальної власності, захисту персональних да-

3 Lanier J. Dawn of the New Everything: Encounters with Reality and Virtual Reality. New York: Henry Holt and Company, 2017. 367 p.

4 Heim M. The Metaphysics of Virtual Reality. New York; Oxford: Oxford University Press, 1993. 224 p.

них, укладення електронних угод та регламентації діяльності, пов'язаної з використанням цифрових аватарів чи віртуальних образів⁵.

Поняття «кіберпростір» виникло у 1980-х роках завдяки культурному контексту (зокрема, у романі Вільяма Гібсона *Neuromancer*, 1984)⁶, проте з часом набуло стійкого наукового змісту. У технічному аспекті воно розуміється як сукупність інформаційно-комунікаційних мереж і систем, які забезпечують обмін даними та формують інфраструктурну основу глобального цифрового середовища⁷. Соціально-комунікаційний підхід трактує кіберпростір як новий вимір соціальної взаємодії та глобальної культури, у якому здійснюються різноманітні суспільні практики та формується новий тип мережевого суспільства. Правова доктрина, натомість, визначає кіберпростір як специфічний правовий простір, де діють як міжнародні норми (наприклад, Конвенція Ради Європи про кіберзлочинність 2001 року), так і національні закони з питань кібербезпеки та цифрової ідентифікації. Лоуренс Лессіг сформулював відому тезу «Code is Law», згідно з якою саме архітектура програмного забезпечення та алгоритми, що визначають правила доступу й використання мережі, є нормативними чинниками, здатними регулювати поведінку у кіберпросторі не менш ефективно, ніж державне законодавство⁸.

Таким чином, доктринальний аналіз свідчить, що віртуальна реальність і кіберпростір становлять взаємопов'язані, проте не тотожні категорії. Віртуальна реальність має передусім індивідуально-досвідний характер, оскільки спрямована на створення ілюзії занурення для конкретного користувача, тоді як кіберпростір є глобальним соціально-правовим простором, у межах якого функціонує Інтернет як мережа мереж. Юридичне осмислення цих понять є необхідною передумовою для формування адекватних механізмів правового регулювання цифрових відносин, що охоплюють як приватноправові аспекти (авторське

5 Koops B. J. Law, Virtuality, and the Experience of Law. Tilburg University Legal Studies Working Paper, 2010. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1616643

6 Gibson W. *Neuromancer*. New York: Ace Books, 1984. 271 p.

7 Denning D. E. *Information Warfare and Security*. Reading, MA: Addison-Wesley, 1999. 544 p.

8 Lessig L. *Code: Version 2.0*. New York: Basic Books, 2006. 410 p.

право, договірні зобов'язання, захист персональних даних), так і публічно-правові виміри (юрисдикція держав, боротьба з кіберзлочинністю, гарантії кібербезпеки).

Сьогодні, в літературі існують різні точки зору щодо правової природи віртуального середовища. Так, на думку Розгон О.В., правові аспекти віртуальної реальності обумовлені використанням у цифровому середовищі визнаних законодавцем різновидів складних об'єктів інтелектуальних прав (перш за все мультимедійних продуктів), а також появою принципово нових явищ, зокрема віртуальних об'єктів, що створюються або придбаваються користувачами комп'ютерних технологій⁹.

Як зазначає О. Дзьобань, у сфері права діє логіка віртуальності, адже правова реальність формується як множинність можливих сценаріїв, що виникають у результаті інформаційно-комунікативної взаємодії учасників правовідносин. Кожен суб'єкт створює свою симулятивну правову картину ситуації, яка може відрізнитися від інших. У такому контексті правове поле постає як динамічна система альтернативних світів, де одночасно співіснують різні версії подій – наприклад, можливі моделі вчинення правопорушення, варіанти ступеня вини, оцінка доказів чи сценарії винесення вироку. Ці варіанти взаємодіють між собою в складній, багатовимірній, синергетичній структурі права, що постійно змінюється та саморегулюється¹⁰.

Беляков К.І. пропонує розуміти віртуальну реальність як форму інформаційно-комп'ютерного середовища, де виникають віртуально-інформаційні правові відносини між суб'єктами¹¹.

Костенко О.В. розглядаючи метавсесвіт з точки зору права, влучно визначає його як віртуальне середовище, що утворено су-

9 Розгон О.В. Правові аспекти технології віртуальної реальності у сфері музейної справи. URL: https://ndipzir.org.ua/wp-content/uploads/2020/12/Tezy_18_09_2020_26.pdf
РЕАЛЬНОСТІ У СФЕРІ МУЗЕЙНОЇ СПРАВИ

10 Дзьобань О. П. Правовий дискурс справедливості як віртуальна реальність права / О. П. Дзьобань, Ю. В. Мелякова // Інформація і право. – 2013. – № 2. – С. 5-16. С. 13.

11 Беляков К. І. Понятійні та методологічні основи регулювання нових типів інформаційних відносин: «віртуальні правовідносини» / К. І. Беляков // Lex Portus. – 2016. – № 2. – С. 47-63.

купністю електронних суб'єктів та об'єктів, які взаємодіють між собою, а також електронні або інші технології, що забезпечують їх взаємодію¹².

На думку, Авруніна О.Г. та Россіхіна В.В. основні *функції віртуальної реальності* охоплюють породженність, актуальність, автономність та інтерактивність. Породженність (або генеративність) означає здатність віртуального простору створювати нові смисли, об'єкти та сценарії, які не мають аналогів у фізичному світі. Це не копіювання дійсності, а формування принципово нових реальностей, де людина може взаємодіяти в умовах, створених технологіями. Актуальність вказує на здатність VR відповідати на запити користувача, транслюючи ті змісти й елементи, які є релевантними в певний момент часу. Завдяки цьому віртуальна реальність ефективно застосовується для навчання, тренінгів, аналізу ситуацій або прийняття рішень. Автономність віртуальної реальності полягає в її здатності функціонувати як окрема система зі своєю логікою, законами часу й простору, незалежно від фізичної дійсності. Це дозволяє створювати моделі, що не підпорядковуються звичним законам, і реалізовувати експерименти, неможливі у реальному світі. Інтерактивність є фундаментальною рисою VR, що забезпечує безперервну взаємодію користувача із цифровим середовищем. У відповідь на дії людини змінюються об'єкти, запускаються події, реагують агенти, що створює ефект реальної присутності та глибокого занурення. У сукупності ці функції формують унікальний потенціал віртуальної реальності як технології, що перетворює уявлення про простір, досвід та саму природу взаємодії¹³.

12 Костенко О.В. Правові основи застосування штучного інтелекту в Метавесвіті. The 15th International scientific and practical conference “Science, innovations and education: problems and prospects” (September 21-23, 2022) CPN Publishing Group, Tokyo, Japan. 2022. 397 p. С. 365– 373. URL: <https://sci-conf.com.ua/wp-content/uploads/2022/09/SCIENCE-INNOVATIONSAND-EDUCATION-PROBLEMS-AND-PROSPECTS-21-23.09.22.pdf#page=365>

13 Аврунін О. Г., Россіхін В. В. “Штучний інтелект та віртуальна реальність” (філософські проблеми) / Харківський національний університет радіоелектроніки, Харківська медична академія післядипломної освіти. – Харків, 2020. URL: <https://openarchive.nure.ua/server/api/core/bitstreams/6ba12235-fee5-4105-8efa-5d6b8ad35507/content>

Різниця між віртуальною реальністю та фізичним (реальним) світом полягає насамперед у природі самого існування. Реальний світ – це об’єктивна фізична реальність, яка існує незалежно від технологій та сприйняття суб’єкта. Людина взаємодіє з нею безпосередньо за допомогою органів чуття, фізичного тіла, у просторі та часі, які мають фіксовану природу. У реальному світі правові відносини виникають між чітко ідентифікованими суб’єктами – фізичними, юридичними особами, державою – на основі усталених правових норм, звичаїв, моральних принципів і державного примусу.

Натомість віртуальна реальність – це штучно створене комп’ютерне середовище, яке моделює простір і час, не обов’язково відтворюючи реальність у її фізичному вигляді. Ця реальність функціонує в межах цифрових систем і платформ, і її параметри визначаються алгоритмами, сценаріями розробників, а також самими користувачами. У VR взаємодія з довкіллям і з іншими учасниками здійснюється через аватари, програмні агенти, віртуальні об’єкти – тобто через цифрові проєкції особистості.

Суспільні відносини в реальному світі є наслідком взаємодії реальних індивідів, обмежених фізичними, соціальними, економічними та юридичними умовами. Вони ґрунтуються на документах, реєстрах, ідентифікації особи, реальному статусі людини. У віртуальному світі ці відносини трансформуються: особа може бути анонімною або діяти під псевдонімом, а об’єктами можуть виступати цифрові зображення, аватари, віртуальні активи, а також результати творчої діяльності, створені за допомогою штучного інтелекту¹⁴.

На відміну від традиційних юрисдикцій, віртуальне середовище не має територіальних меж у класичному розумінні. Тут діють правила конкретної платформи, які не мають загальнообов’язкової сили. Таким чином, віртуальна реальність створює унікальний феномен – простір, у якому можуть реалізовуватися права, свободи,

14 Булеца С.Б. Цифрові аватари: об’єкти приватного права. IT-право та кібербезпека в умовах гібридної війни : матеріали Всеукр. круглого столу (м. Одеса, 12 квіт. 2025 р.) / за заг. ред.: Є. О. Харитонова, Ю. Кривенко ; кафедра цив. права НУ «Одес. юрид. академія». – Одеса : Фенікс, 2025. – С. 10-15 С.11.

укладатися цифрові договори, але все це відбувається в «інституційній порожнечі», де традиційні правові інструменти часто виявляються неефективними¹⁵.

4. Ознаки кіберпростору.

Ознаки кіберпростору у сучасній науковій та правовій доктрині розглядаються як сукупність характеристик, що відрізняють його від традиційних соціальних і правових просторів та водночас визначають його особливе місце у структурі глобального інформаційного суспільства. Кіберпростір є явищем, що поєднує технічну інфраструктуру інформаційно-комунікаційних мереж, цифровий контент та комунікативні практики користувачів, і саме в цій багатомановитості криється складність його наукового визначення.

Насамперед доктрина акцентує на **віртуальності та нематеріальності** кіберпростору: він існує поза фізичними координатами, не має конкретної території, але водночас є реальною сферою соціальної активності, у якій відбувається обмін інформацією, формування відносин власності та здійснення владних повноважень¹⁶. Другою ключовою ознакою є **глобальність і транснаціональність**, адже кіберпростір не знає державних кордонів і охоплює практично всі країни світу, створюючи середовище, у якому юрисдикційні межі держав значною мірою втрачають свою абсолютність. Саме тому Конвенція Ради Європи про кіберзлочинність 2001 року була розроблена як інструмент міжнародної координації у сфері кримінального переслідування протиправних дій у цифровому середовищі, що виходять за рамки національних правопорядків.

До специфічних характеристик також належить **анонімність і децентралізованість**. Користувач може взаємодіяти у кіберпросторі без повної ідентифікації своєї особи, що створює умови для свободи вираження, але водночас породжує загрози у вигляді кі-

15 Костенко О. В., Журавльов Д. В., Фурашев В. М., Дніпров О. С. Генезис правового регулювання Web та модель електронної юрисдикції Metaverse // Інформація і право. – 2024. – № 1(48). С. 68-83. С. 81. URL: <https://il.ippi.org.ua/article/view/300772>

16 Castells M. The Rise of the Network Society. 2nd ed. Oxford: Blackwell Publishing, 2000. 597 p.

берзлочинності, терористичної діяльності та поширення дезінформації¹⁷. Водночас відсутність єдиного центру управління означає, що кіберпростір регулюється не лише правовими нормами, а й технічними протоколами та кодом, що втілює відому концепцію Л. Лессіга «Code is Law»¹⁸.

Ще однією ознакою є **динамічність та інтерактивність**: у кіберпросторі інформація змінюється з високою швидкістю, користувачі можуть безпосередньо взаємодіяти між собою та впливати на розвиток цифрового середовища. Це відрізняє кіберпростір від традиційних медіа і створює новий вимір комунікації, який дослідники ототожнюють із формуванням «мережевого суспільства»¹⁹. Нарешті, слід підкреслити **правову багатовимірність** кіберпростору: тут одночасно діють міжнародні договори, національні закони, приватні регламенти корпорацій (наприклад, політики платформ соціальних мереж) та технічні стандарти, що зумовлює його гібридну правову природу.

Отже, ознаками кіберпростору є його нематеріальність, глобальність і транснаціональність, анонімність та децентралізованість, динамічність та інтерактивність, а також правова багатовимірність. Сукупність цих характеристик визначає кіберпростір як унікальний соціально-правовий феномен, що потребує комплексного регулювання на перетині національного та міжнародного права, технічних стандартів та етичних норм.

5. Сфера правового регулювання віртуальної реальності.

Сфера правового регулювання віртуальної реальності є складною та багатовимірною, оскільки вона охоплює як приватноправові, так і публічно-правові відносини, що виникають у зв'язку з використанням технологій занурення та створенням штучних циф-

17 Denning D. E. Information Warfare and Security. Reading, MA: Addison-Wesley, 1999. 544 p.

18 Lessig L. Code: Version 2.0. New York: Basic Books, 2006. 410 p

19 Castells M. The Rise of the Network Society. 2nd ed. Oxford: Blackwell Publishing, 2000. 597 p.

рових середовищ. Віртуальна реальність трансформує традиційні уявлення про об'єкти права, суб'єктність у цифровому середовищі та межі відповідальності, а відтак вимагає комплексного нормативного підходу.

Насамперед віртуальна реальність виступає об'єктом права інтелектуальної власності, оскільки VR-контент (графіка, програмні алгоритми, ігрові сценарії, аудіовізуальні ефекти) охороняється авторським правом, а обладнання та технічні рішення можуть охоронятись як об'єкти права інтелектуальної власності.

Другою важливою сферою є правове регулювання договірних відносин, що виникають у VR-середовищах. Укладання угод, здійснення транзакцій та обмін цифровими активами у віртуальних просторах створюють нові правові виклики, адже часто такі правочини укладаються між суб'єктами, які перебувають у різних юрисдикціях, та з використанням смарт-контрактів. Це зумовлює необхідність застосування норм міжнародного приватного права та гармонізації правового регулювання²⁰.

Окремий пласт становить захист персональних даних і права на приватність. VR-технології збирають значний обсяг інформації про фізичну поведінку користувачів – від рухів тіла до біометричних характеристик, що створює ризики для порушення конфіденційності. У ЄС правове підґрунтя захисту таких даних забезпечується Загальним регламентом про захист даних (GDPR), у США – низкою галузевих актів і судовою практикою²¹.

До публічно-правової сфери належить регулювання безпеки та відповідальності за шкоду, заподіяну у VR-середовищі. Йдеться як про деліктну відповідальність за наслідки використання VR-обладнання (наприклад, шкоду здоров'ю через технологічні дефекти), так і про відповідальність за неправомірні дії у віртуальному просторі, включаючи кібербулінг, поширення забороненого контенту чи шах-

20 Grimmelmann J. Virtual World Feudalism. Yale Law Journal Pocket Part. 2009. Vol. 118. P. 126–129. URL: <https://yalelawjournal.org/forum/virtual-world-feudalism>

21 Guidelines 3/2019 on processing of personal data through video devices. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en

райство. Судова практика у США та країнах ЄС поступово формує підходи до визначення відповідальних суб'єктів – розробників програмного забезпечення, провайдерів платформ чи користувачів²².

Не менш важливим напрямом є регулювання використання VR у сфері освіти, охорони здоров'я та трудових відносин. У цих випадках на перший план виходять стандарти безпеки, ліцензування медичних чи освітніх VR-програм, а також питання охорони праці, коли VR застосовується у тренінгах або моделюванні виробничих процесів.

Питання для самоперевірки:

1. У чому полягають основні етапи становлення Інтернету як глобальної мережі?
2. Яке значення для розвитку інформаційного суспільства мало створення протоколу TCP/IP?
3. Чим правова природа Інтернету відрізняється від традиційних об'єктів правового регулювання?
4. Як співвідносяться концепції «Інтернет як публічне благо» та «Інтернет як сфера приватного регулювання»?
5. У чому полягає відмінність між поняттями «віртуальна реальність» та «кіберпростір»?
6. Які основні доктринальні підходи використовуються для визначення сутності віртуальної реальності?
7. Які ознаки дозволяють відрізнити кіберпростір від фізичного соціального простору?
8. Як анонімність та децентралізованість впливають на правове регулювання відносин у кіберпросторі?
9. Які основні сфери охоплює правове регулювання віртуальної реальності?
10. Чому VR-технології потребують особливої уваги з боку права інтелектуальної власності та захисту персональних даних?

22 Gregory S. Virtual Reality and the Law: Regulating New Frontiers of Immersive Technology. Stanford Technology Law Review. 2021. Vol. 24, No. 2. P. 112–147. URL: <https://law.stanford.edu/publications/virtual-reality-and-the-law/>

Тема 2. Поняття та типологія цифрової особи. Homo virtualis як феномер віртуального інформаційного суспільства (4 год).

1. Формування концепції цифрової ідентичності фізичної особи.
2. Підходи до розуміння терміну «симулякр».
3. Використання симулякрів як способів маніпуляції у віртуальному просторі.
4. Симулякри в праві.
5. Поняття та специфічні риси цифрової особи.
6. Співвідношення цифрової особи та цифрової особистості.
7. Цифрова ідентичність.
8. Поняття та особливості цифрового аватару.
9. Правові аспекти створення голограми відомої особи.
10. Електронний цифровий підпис як спосіб ідентифікації особи.

Теоретичні відомості

1. Формування концепції цифрової ідентичності фізичної особи.

Формування концепції цифрової ідентичності фізичної особи є однією з ключових проблем сучасного правового та соціально-технологічного дискурсу, оскільки цифрова ідентичність стає невід'ємною частиною соціальної присутності людини у глобальному інформаційному середовищі. Цифрова ідентичність визначається як сукупність інформації про фізичну особу, яка існує в цифровому середовищі, відображає її соціальні, професійні та особисті характеристики та використовується для ідентифікації, аутентифікації та комунікації з різними інформаційними системами.

У науковій доктрині виділяють кілька підходів до трактування цифрової ідентичності. Перший підхід розглядає її як технологічний феномен, що передбачає створення цифрових атрибутів особи – логінів, паролів, електронних сертифікатів та криптографічних ключів, які забезпечують аутентифікацію користувача у цифрових системах та сервісах²³. Другий підхід фокусується на

23 Pfützmann A., Hansen M. A Terminology for Talking About Privacy by Data Protection and Data Security. Version 2.1, 2010. URL: https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v2.1.pdf

соціально-психологічному вимірі, трактуючи цифрову ідентичність як проекцію соціальної ролі особи у мережевому середовищі, включаючи її активність у соціальних мережах, участь у форумах, електронних платформах та цифрових ком'юніті. Третій підхід підкреслює правову природу цифрової ідентичності, зокрема її значення для реалізації прав фізичної особи у цифровому середовищі, захисту персональних даних, прав на приватність та можливості участі в електронних правочинах²⁴.

Важливою характеристикою цифрової ідентичності є її множинність та динамічність. Особа може одночасно мати кілька цифрових профілів або аватарів, які взаємодіють у різних інформаційних середовищах і платформах, а їхні параметри та атрибути можуть змінюватися залежно від контексту використання. Це створює виклики для правового регулювання, адже необхідно забезпечити узгодженість між реальною фізичною особою та її цифровими проекціями, гарантувати достовірність даних та запобігти неправомірному використанню цифрових ідентифікацій.

Цифрова ідентичність є фундаментальною для функціонування сучасного суспільства, оскільки вона забезпечує участь фізичної особи у віртуальних економічних, освітніх, соціальних та правових відносинах. Сучасні тенденції розвитку блокчейн-технологій, децентралізованих ідентифікаційних систем та цифрових паспортів підкреслюють необхідність формування надійних, безпечних та юридично визнаних механізмів управління цифровою ідентичністю²⁵.

Отже, формування концепції цифрової ідентичності фізичної особи охоплює технічний, соціально-психологічний та правовий виміри, характеризується множинністю і динамічністю цифрових профілів та вимагає комплексного підходу для забезпечення безпеки, автентичності та правового захисту особи в цифровому середовищі.

24 Digital Identity Guidelines. 2020. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>

25 Hardjono T., Lipton A., Pentland A. Trustworthy Digital Identity: A Decentralized Approach. MIT Connection Science, 2019. URL: <https://arxiv.org/abs/1906.07123>

2. Підходи до розуміння терміну «симулякр».

Термін «симулякр» у науковій та філософській літературі відображає складну динаміку відносин між реальністю та її відтворенням, фактичним та символічним. Класично його розуміли як **копію або зображення реального об'єкта**, що зберігає ознаки, властиві первинному предмету, але не володіє його сутністю. Такий підхід виникає ще в античній філософії: Платон, аналізуючи мистецтво та імітацію у «Державі», визначав симулякр як другорядну копію істини, яка несе лише зовнішні риси, відокремлені від сутнісного змісту.

У XX столітті поняття зазнало радикальної трансформації. Жан Бодріар, центральний для постмодерністської теорії, розглядав симулякр як **знак, що втратив прив'язку до реального об'єкта** і формує нову автономну реальність. У його концепції симулякри проходять чотири стадії: від простого копіювання реальності до створення «гіперреального» середовища, де знак більше не посиляється на щось реальне, а існує сам по собі, формуючи власний сенс. Такий підхід особливо релевантний у віртуальному середовищі, де цифрові аватари, 3D-моделі, VR-об'єкти та голограми не відтворюють фізичну реальність, а створюють автономні соціально-технічні структури, у яких користувачі взаємодіють як з реальною «присутністю», так і з її цифровими проєкціями.

Соціологічні та культурологічні дослідження підкреслюють **вплив симулякру на сприйняття соціальної реальності**. У цифровому середовищі симулякри формують нові стандарти поведінки, соціальні норми та інтерпретації реального світу. Еко підкреслював, що симулякри можуть створювати «поверхневу реальність», яка маскує складні соціальні процеси, формує ілюзію достовірності та контролю. У цьому контексті цифрові технології, соцмережі та VR-платформи стають середовищем поширення гіперреальних симулякрів, що впливають на поведінку та світогляд користувачів²⁶.

З правової точки зору, симулякр також набуває особливого значення. Цифрові копії об'єктів, включно з особистим образом фізичної особи, графічними або музичними творами, можуть охоронятися нормами авторського права, торговельними марками або

26 Eco U. *Travels in Hyperreality*. New York: Harcourt Brace Jovanovich, 1986. 247 p.

нормами про права на імідж. Юридична наука підкреслює, що виникає питання **правової суб'єктності симулякру**, відповідальності за його використання, а також захисту від незаконного копіювання та експлуатації. Особливо складним є регулювання симулякрів, які використовуються у віртуальних світах та VR-середовищах, де ідентичність та авторство часто є децентралізованими або анонімними.

Сучасні технології штучного інтелекту та глибокого навчання додатково ускладнюють ситуацію, оскільки ШІ може створювати **нові симулякри, що імітують реальних людей** (deepfake), автоматично генеруючи контент, який зовні не відрізняється від реального, але повністю штучний. Це породжує необхідність комплексного регулювання та формування етичних норм, адже симулякри в такому вигляді можуть використовуватися у медіа, PR-кампаніях, освіті та кримінальних схемах, створюючи правові та соціальні ризики.

Таким чином, сучасне розуміння симулякру охоплює три основні підходи: класичний (як копію реального), постмодерністський (як автономну знакову систему, що створює гіперреальність) та цифрово-технологічний (як об'єкт у віртуальному середовищі з правовими та етичними наслідками). Ці підходи підкреслюють не лише філософську природу симулякру, але й його соціальну, психологічну та правову значущість у сучасному цифровому суспільстві.

3. Використання симулякрів як способів маніпуляції у віртуальному просторі.

Використання симулякрів у віртуальному просторі як інструментів маніпуляції є однією з найпотужніших технологій впливу в сучасному інформаційному суспільстві. Симулякр у цьому випадку виступає не лише як копія або відтворення реального об'єкта, а як автономна цифрова реальність, здатна формувати уявлення, переконання та поведінку користувачів, часто без їхнього усвідомлення.

Однією з основних сфер застосування симулякрів є політична та соціальна маніпуляція. Наприклад, у соціальних мережах створюються аватари та боти, які моделюють поведінку реальних людей, поширюють контент або взаємодіють із користувачами так, щоб

формувати громадську думку або емоційний стан аудиторії. Відомі випадки використання deepfake-технологій для створення відео з політичними діячами показали, що такі симулякри можуть підвищувати рівень довіри або навпаки викликати страх і невпевненість, маніпулюючи сприйняттям подій²⁷.

З точки зору психології впливу, симулякри діють на когнітивні та емоційні механізми користувачів. Завдяки високій візуальній та інтерактивній достовірності цифрових образів вони здатні формувати «гіперреальність», де користувачі реагують на цифрові події так само, як на реальні. Це дозволяє впливати на рішення, переконання та навіть соціальні поведінкові патерни, що особливо актуально у маркетингових стратегіях та PR-кампаніях²⁸.

Технологічний аспект маніпуляцій через симулякри включає використання штучного інтелекту та алгоритмів машинного навчання. AI здатен створювати аватари або відео, які не відрізняються від реальних, генерувати тексти, голоси або реакції, що максимально відповідають поведінці конкретних груп користувачів. Це дозволяє створювати персоналізовані маніпулятивні кампанії, адаптовані під індивідуальні психологічні та поведінкові характеристики цільової аудиторії.

З правової точки зору, використання симулякрів для маніпуляції викликає численні виклики та ризики. Основні з них:

- Порушення прав на честь, гідність та приватність – створення цифрових копій особи без її згоди, включаючи deepfake, аватари або автентичні голосові імітації.
- Порушення авторських права або суміжних прав - копіювання результатів творчої діяльності у цифровій формі для маніпулятивних цілей може порушувати права власників контенту.
- Порушення етичних норм - маніпуляції через симулякри можуть вводити користувачів в оману, формувати хибні уявлення про

27 Chesney R., Citron D. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review. 2019. Vol. 107, No. 6. P. 1753–1819. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954

28 Marwick A. E. Media Manipulation and Disinformation Online. New York: Oxford University Press, 2018. URL: https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf

реальність або нав'язувати поведінку, що суперечить етичним нормам суспільства.

- Симулякри змінюють традиційне сприйняття реальності та створюють «цифрові світи», де грає роль не фізичний факт, а створене уявлення. Це, в свою чергу, впливає на освіту, медіа, рекламу, політику та комунікації в бізнесі, формуючи нові норми поведінки у кіберпросторі²⁹.

Таким чином, симулякри як інструменти маніпуляції у віртуальному просторі є одночасно технологічним, соціально-психологічним та правовим феноменом. Вони формують гіперреальність, впливають на когнітивні та емоційні процеси користувачів, та потребують комплексного підходу до регулювання, що охоплює технології, етику, право та освіту користувачів.

4. Симулякри в праві.

Симулякри в праві виникають тоді, коли цифрові або віртуальні образи взаємодіють із правовими відносинами або можуть створювати правові наслідки для фізичних чи юридичних осіб. По суті, симулякр стає юридично значущим, коли його існування або використання може впливати на права, обов'язки чи відповідальність суб'єктів права.

Однією з таких ситуацій є створення цифрових образів особи без її згоди. Наприклад, деєrfake-відео або аватар, що відтворює зовнішність конкретної людини, може стати об'єктом прав на імідж та персональні дані, оскільки використання такого образу здатне завдати шкоди честі, гідності чи репутації. У цьому випадку симулякр виникає як юридично значущий об'єкт у момент створення або поширення цифрового образу, навіть якщо фізична особа не має безпосереднього контролю над ним³⁰.

29 Chesney R., Citron D. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review. 2019. Vol. 107, No. 6. P. 1753–1819. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954

30 Chesney R., Citron D. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review. 2019. Vol. 107, No. 6. P. 1753–1819. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954

Інша ситуація – створення симулякру як об'єкта права інтелектуальної власності. Віртуальні персонажі, 3D-моделі, графічні аватари або цифрові твори стають юридично значущими у момент їх створення, оскільки вони підпадають під охорону авторського права. Тут симулякр набуває значення об'єкта права інтелектуальної власності незалежно від того, чи був він використаний комерційно, а лише через його унікальність та здатність відтворювати оригінальний зміст або образ³¹.

Третій аспект стосується використання симулякру в комерційній сфері. Коли цифровий образ або аватар застосовується для реклами чи просування товарів і послуг, він набуває юридичної значущості як об'єкт комерційної таємниці або навіть як елемент торговельної марки. Фактично правове значення симулякру виникає з моменту його залучення до комерційних відносин, оскільки тоді він безпосередньо впливає на економічні права та інтереси як власника, так і третіх осіб.

Четвертий випадок стосується використання симулякру з потенційно протиправною метою у цифровому середовищі. Такий образ може слугувати інструментом шахрайства, маніпуляцій, кібератак або створення фальсифікованого контенту, що порушує права інших учасників цифрових відносин. У подібному контексті юридична значущість симулякру проявляється з моменту його застосування як засобу реалізації протиправних дій.

Отже, правове значення симулякрів визначається не самим фактом їх існування, а моментом створення чи використання, яке породжує правові наслідки. Саме взаємодія з суб'єктами та виникнення правовідносин надають симулякру статус юридично релевантного явища, перетворюючи його з технічного або цифрового образу на об'єкт права.

5. Поняття та специфічні риси цифрової особи.

Цифрова особа у сучасному правовому дискурсі розглядається як багатовимірний феномен, що поєднує у собі правові, соці-

31 Grimmelmann J. Virtual Worlds as Comparative Law. UC Davis Law Review. 2009. Vol. 42. P. 705–746. URL: https://lawreview.law.ucdavis.edu/issues/42/3/Symposium/42-3_Grimmelmann.pdf

альні та технологічні аспекти. Її поява зумовлена стрімким розвитком інформаційно-комунікаційних технологій, глобалізацією мережевих комунікацій та зміною традиційних уявлень про ідентичність людини. На відміну від класичного уявлення про право-суб'єктність, цифрова особа існує у віртуальному просторі, який не має чітко окреслених територіальних і юрисдикційних меж, що ускладнює як її ідентифікацію, так і захист її прав.

Специфічною рисою цифрової особи є те, що вона не є тотожною фізичній чи юридичній особі, а становить новий рівень репрезентації, втілений у сукупності цифрових слідів, персональних даних, профілів у соціальних мережах, аватарів, віртуальних ідентифікаторів, штучно згенерованих зображень чи голосу. Цифрова особа функціонує в межах алгоритмізованого простору, що створює додаткову залежність від цифрових платформ та їхніх правил, які часто виступають квазі-нормативними регуляторами. Водночас цифрова ідентичність формується не лише волею суб'єкта, а й активністю інших користувачів та алгоритмів, що здатні впливати на сприйняття та репутацію особи у віртуальному середовищі.

До характерних рис цифрової особи слід віднести її фрагментарність, множинність та динамічність. На відміну від цілісного уявлення про людину у фізичному світі, у цифровій реальності суб'єкт може мати кілька образів, які взаємодіють незалежно один від одного. Водночас її існування тісно пов'язане з категорією цифрових прав, до яких належать право на інформаційну автономію, право на захист персональних даних, право на «забуття», право на контроль за використанням власного цифрового образу. Саме через такі права цифрова особа поступово інтегрується у правову систему та стає предметом наукових дискусій щодо можливості її нормативного закріплення.

Дослідження у сфері цифрової ідентичності також порушують питання про співвідношення цифрової особи та особистих немайнових прав. Якщо традиційне право захищає честь, гідність, ділову репутацію та приватність, то у цифровій площині виникає необхідність їхнього розширеного тлумачення з урахуванням нових

викликів, таких як deepfake-технології, кібербулінг, незаконне використання віртуального образу чи біометричних даних. Це формує підґрунтя для розвитку концепції цифрової правосуб'єктності, яка у майбутньому може отримати нормативне оформлення на міжнародному та національному рівнях.

Наукова література підкреслює, що цифрова особа не є простою проекцією фізичної особи у віртуальному світі, а новою якісною категорією, що вимагає розробки спеціальних підходів до її розуміння та регулювання. У цьому контексті особливої актуальності набувають спроби поєднати правову доктрину із міждисциплінарними підходами, що інтегрують філософію інформації, кіберетику та цифрову соціологію.

Таким чином, цифрова особа постає як складний правовий феномен із власними специфічними рисами, що визначають її відмінність від класичних суб'єктів права. Її концептуалізація є не лише викликом для сучасної науки, а й перспективним напрямом розвитку правових систем, які мають адаптуватися до реалій цифрової цивілізації.

6. Співвідношення цифрової особи та цифрової особистості.

З метою встановлення співвідношення понять «цифрова особа» і «цифрова особистість» слід звернутися до тих характеристик, які склалися у теорії права, філософії тощо стосовно категорій «особа» і «особистість».

Так, зокрема, аналізуючи поняття «особа» Г. Кельзен зазначав, що традиційна теорія ототожнює поняття суб'єкта права з особою, де особа – це людина як суб'єкт прав та обов'язків. Але, оскільки не лише людина, а інші сутності, от як певні спільноти на кшталт об'єднань, акціонерних товариств, міських громад, держав, подаються як особи, поняття особи подається ще як «носій» прав та обов'язків, причому як носії можуть виступати не тільки люди, а також й інші сутності³². Відповідно, коли йдеться про людину як носія таких прав

32 Кельзен Ганс. Чисте правознавство: 3 дод. Проблеми справедливості / пер. з нім. О. Мокровольського. К.: Юніверс, 2004. 496 с.

і обов'язків, то це фізична особа, якщо про інші сутності – то це особи юридичні.

Отже, бути особою, за Кельzenом, це мати «правову персональність», означає мати правові обов'язки та суб'єктивні права, власне, бути єдиним комплексом таких прав і обов'язків, персоніфікацією цієї єдності.

Особистість належить до іншої категорії і є тісно пов'язаною з людиною, фізичною особою.

У філософській традиції особистість трактується як неповторна духовно-тілесна цілісність індивіда, що виявляє себе у формі суб'єкта життєдіяльності, наділеного власним «Я» та здатністю до самовизначення. Такий індивід виступає автономним і відповідальним суб'єктом, що усвідомлює наслідки власних дій, визначає зміст, цінності та цілі свого існування, формуючи життєву траєкторію. У психологічному вимірі особистість розуміється як інтегрований комплекс індивідуальних характеристик – звичок, уподобань, знань, досвіду, психофізіологічних параметрів, що зумовлюють повсякденну поведінку та соціальні взаємозв'язки. У цьому сенсі поняття особистості охоплює відносно стійкі риси, які відображають індивідуальність людини та визначають значимість її вчинків для соціуму. Йдеться про спрямованість прагнень, унікальність життєвого досвіду, розвиток здібностей, специфіку характеру й темпераменту. Отже, особистість являє собою цілісну психофізіологічну структуру, що включає тип темпераменту, фізичні та психічні особливості, інтелектуальний рівень, світоглядні орієнтири, а також життєві настанови й індивідуальні схильності³³.

Таким чином, навіть побіжний аналіз категорій «особа» і «особистість» свідчить про відсутність підстав їх отождення.

Говорячи про «електронну особистість», ми пропонуємо вести мову про віртуальний, цифровий відбиток реальної людини, за допомогою якого вона існує у віртуальному просторі.

У літературі зазначається, що категорія «віртуальна особистість» в широкому сенсі, як і її англomовний аналог «virtual

33 Особистість в психології. URL: http://psychologis.com.ua/lichnost_v_psihologii.htm

identity», є багатозначною і має низку синонімів, значення яких перетинаються лише частково. Основні значення терміна віртуальна особистість такі: 1) ідентифікатор для входу в комп'ютерну систему (login, user name); 2) прізвище або псевдонім, що використовуються для ідентифікації користувача в електронному середовищі (user name, nickname); 3) абстрактна репрезентація особистості, яка використовується для її цивільної, правової та іншої соціальної ідентифікації (номер паспорта, особистий код, відбитки пальців, DNA); 4) комп'ютерна програма, що моделює розумну поведінку (robot, bot); 5) те саме, але в поєднанні з тілом (android, cyborg); 6) вигадана особа, яка створена людиною або групою людей, що породжує семіотичні артефакти і / або описувана ззовні (virtual character, virtual persona); 7) будь-яка особа, як вона сприймається або моделюється ким-небудь; іншими словами, образи чи іпостасі особистості як щось відмінне від її сутності (наприклад, «я» (ego) в його протиставленні «самості» (self))³⁴.

У науковій літературі пропонується розгорнута класифікація типів віртуальних особистостей. Так, вони можуть: відображати реально існуючу людину, повністю або частково збігаючись з її прототипом; бути сконструйованими користувачем як втілення певних граней його реальної чи бажаної ідентичності, якими він у дійсності не володіє, але прагне проявити; виступати доповненням до реальної особистості, розширюючи її соціальну присутність у кіберпросторі; репрезентувати образ відомої особи минулого або цілковито вигаданий персонаж, що не має жодного відношення до реального світу; існувати як у формі єдиної, так і множинної ідентичності; створюватися індивідуально або групою користувачів.

Усі зазначені варіанти можуть не лише репрезентувати певне «Я» в цифровому середовищі, але й розвиватися в ньому. При цьому віртуальні особистості здатні мати динамічний характер, коли їхній розвиток підтримується користувачами, або статичний – якщо зв'язок із творцем втрачено. Окремі з них можуть існувати автономно, неза-

34 Огорокова В.В. Модель віртуальної людини доби постмодерну. «Філософія та політологія в контексті сучасної культури», 2018, Т.10. №1-2 (22). С. 40 С. 38-44.

лежно від свого первісного автора, а у випадку доступу до відповідних акаунтів можлива трансформація від статичної форми до динамічної через створення нових інтерпретацій. Нарешті, віртуальні особистості можуть виходити за межі віртуального простору, взаємодіючи з реальними людьми та впливаючи на їхню свідомість і поведінку³⁵.

Підсумовуючи, можна зробити висновок, що з точки зору права цифрова особистість є особливим поєднанням імені, дати народження, місця проживання, електронної пошти та сторінок, представлених на цих сторінках записів, фото та відео та особистих соціальних зв'язків, біометричні данні. Все те, що може бути використано для представлення особи в цифровому, віртуальному світі. Цей набір онлайн дій та даних сприяє формуванню враження, яке ми справляємо на інших і з точки зору права є об'єктом. Частина даних – є об'єктом прав інтелектуальної власності, інше – частиною немайнових прав особи. Розвиток законодавства у сфері регулювання персональних даних свідчить про те, що відбувається перегляд концепції персональних даних у напрямку поширення на них режиму власності³⁶.

Цифрова особа у правовому розумінні – це насамперед суб'єкт права, тобто носій прав та обов'язків у цифровому середовищі. Вона є проекцією традиційного поняття «особа» (фізична чи юридична) у віртуальний простір. Її сутність зводиться до правової персоналізації: цифрова особа – це комплекс персональних даних, ідентифікаторів, облікових записів та атрибутів, що дозволяють визначати суб'єкта у сфері цифрових відносин. Іншими словами, цифрова особа – це правовий статус у віртуальному середовищі.

Цифрова особистість натомість охоплює ширший феномен – це індивідуалізований цифровий образ людини, який складається не лише з формально-правових елементів (ідентифікаційні дані, облікові записи, цифрові підписи тощо), але й з соціально-психологіч-

35 Бугайова Н.М. Трансформація особистості в епоху цифрових технологій. URL: <https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/FFNDWMGfzFjXPzzwqddlccccSTmbgKtsx?projector=1&messagePartId=0.1>

36 Некіт К.Г. Право приватної власності в інформаційному суспільстві: теорія і практика: монографія. Одеса: Видавничий Дім «Гельветика», 2021. 554 с.

них характеристик, які відображають її «Я» у віртуальному просторі. До цифрової особистості належать особливості поведінки користувача, його самопрезентація, репутація, стиль комунікації, унікальні прояви у мережі, які можуть не збігатися з реальною особистістю, а подекуди існувати автономно.

Таким чином, співвідношення цих понять можна звести до такої формули:

Цифрова особа – це юридично значимий «носій» прав і обов'язків у цифровому середовищі, що фіксується переважно через правові та технічні механізми ідентифікації.

Цифрова особистість – це комплекс соціально-правових і психологічних проявів людини у цифровому світі, який відображає її індивідуальність, соціальну взаємодію і культурний слід.

Отже, цифрова особа становить правову оболонку, тоді як цифрова особистість – це змістовне наповнення цієї оболонки. Вони тісно пов'язані, але не тотожні: цифрова особа завжди передбачає правосуб'єктність, а цифрова особистість може існувати навіть поза формальною ідентифікацією, будучи образом, що формується як користувачем, так і суспільством у цифровому просторі.

7. Цифрова ідентичність.

Цифрова ідентичність у сучасному науковому розумінні є однією з ключових категорій інформаційного суспільства, що інтегрує в собі правові, технічні та соціокультурні виміри. Вона визначається як сукупність інформації, що прямо або опосередковано ідентифікує особу у цифровому середовищі, забезпечує її впізнаваність, підтверджує автентичність і дозволяє брати участь у різноманітних цифрових взаємодіях. При цьому йдеться не лише про класичні персональні дані, а й про широкий спектр цифрових атрибутів: профілі в соціальних мережах, електронні підписи, біометричні дані, історію пошукових запитів, поведінкові патерни, цифрові аватари та штучно згенеровані образи.

Особливістю цифрової ідентичності є її багаторівневність і динамічність. На відміну від статичної правової ідентифікації (ім'я,

паспорт, місце проживання), цифрова ідентичність постійно змінюється залежно від онлайн-активності суб'єкта, його взаємодії з платформами та іншими користувачами. Вона існує у вигляді мережі даних, які збираються, зберігаються й обробляються різними цифровими акторами – державними органами, приватними компаніями, соціальними мережами, штучними інтелектами. Це створює ситуацію, коли особа фактично втрачає повний контроль над своєю ідентичністю, що актуалізує необхідність правового захисту.

Цифрова ідентичність виконує низку функцій:

ідентифікаційну (забезпечує розпізнавання особи в мережі та доступ до сервісів),

комунікативну (слугує засобом репрезентації у віртуальних взаємодіях),

репутаційну (формує цифровий образ, що впливає на ділову та соціальну сферу).

У науковій літературі підкреслюється, що цифрова ідентичність має дуалістичний характер: з одного боку, вона є продовженням фізичної ідентичності особи, з іншого – може існувати автономно у вигляді віртуальних аватарів, нікнеймів, цифрових «масок». Це означає, що цифрова ідентичність не завжди повністю співвідноситься з реальною особою, а часто відображає лише фрагменти її життя, які можуть бути перебільшеними, модифікованими або сфальсифікованими.

Ключовою загрозою для цифрової ідентичності є вразливість до маніпуляцій і зловживань. Викрадення персональних даних, клонування акаунтів, використання deepfake-технологій, несанкціонований збір біометрії – усе це ставить під сумнів безпеку цифрової ідентичності та вимагає адекватних правових механізмів реагування. Європейський Союз у цьому контексті запроваджує систему eIDAS, спрямовану на створення єдиного простору електронної ідентифікації. Водночас міжнародні стандарти захисту персональних даних (зокрема, GDPR) формують нормативний каркас, що встановлює межі використання цифрової ідентичності та гарантує право на інформаційну автономію.

На теоретичному рівні цифрова ідентичність пов'язується з концепцією «цифрової особи» та «цифрових прав». Вона розглядається не лише як інструмент автентифікації, а як елемент особистої свободи і простору самореалізації у віртуальному середовищі. Її розвиток породжує дискусії про доцільність введення окремої категорії цифрової правосуб'єктності, що забезпечить баланс між технічними інноваціями та фундаментальними правами людини.

Таким чином, цифрова ідентичність – це не лише технічний механізм, а комплексне соціально-правове явище, яке відображає взаємодію людини з цифровим середовищем. Вона має стратегічне значення для забезпечення безпеки особи, її приватності, репутації та правового статусу у глобальному інформаційному просторі. Її правове врегулювання є одним із головних викликів сучасної юриспруденції, адже від ефективності захисту цифрової ідентичності залежить реальний зміст прав і свобод у цифрову епоху.

8. Поняття та особливості цифрового аватару.

Цифровий аватар у сучасному правовому та міждисциплінарному дискурсі визначається як віртуальне втілення особи у цифровому середовищі, яке може мати як репрезентативний, так і функціональний характер. Він виступає формою візуалізації або символічного відображення індивіда, групи чи навіть штучного інтелекту в кіберпросторі, слугуючи посередником між реальною та віртуальною ідентичністю. У науковій літературі аватар розглядається не лише як технічний образ (графічний персонаж, 3D-модель, іконка), але й як елемент соціальної взаємодії та правової категорії, оскільки через нього особа може здійснювати правочини, набувати зобов'язань чи порушувати права інших.

Особливості цифрового аватару полягають у його багатогранності та здатності відображати різні аспекти особистості. По-перше, аватар може бути реалістичним (максимально наближеним до зовнішності людини, створеним з використанням біометричних даних або технологій *deepfake*) чи вигаданим (символічним образом, що втілює бажану чи альтернативну ідентичність). По-друге, він має подвійний статус: з одного боку, це засіб самовираження у віртуаль-

них спільнотах, соціальних мережах та метавсесвітах; з іншого – потенційний об'єкт правового регулювання, коли його використання зачіпає інтереси третіх осіб або економічний обіг (наприклад, у сфері реклами, геймінгу чи електронної комерції).

Правова значущість цифрового аватару проявляється у кількох аспектах. Він може стати об'єктом інтелектуальної власності (як авторський твір, 3D-модель або графічний дизайн), об'єктом договірних відносин (ліцензійні угоди щодо використання образу), а також предметом судового захисту у випадках неправомірного використання чи маніпуляцій. Окремо слід відзначити ризики підробки або викрадення аватарів, що створює небезпеку для приватності, іміджевих прав і навіть економічних інтересів особи.

Важливим є й соціально-психологічний вимір: аватар може функціонувати як продовження реальної особи, так і як повністю автономна «цифрова маска», яка здатна впливати на поведінку користувача та формування його репутації у віртуальних і реальних соціальних просторах. У зв'язку з розвитком метавсесвітів і штучного інтелекту з'являється дискусія щодо правосуб'єктності аватарів, створених алгоритмами, та їх відповідальності у правовій площині.

Таким чином, цифровий аватар – це не лише технічний інструмент персоналізації у віртуальному середовищі, але й складне соціально-правове явище, яке поєднує у собі риси цифрової ідентичності, іміджевих прав та об'єкта правової охорони. Його особливості полягають у динамічності, гнучкості репрезентації та здатності виступати як інструмент комунікації, так і юридично значущий актив у цифровому правопорядку.

Створення цифрового аватара – процес комплексний, і він зачіпає не лише сферу бізнесу, а й досить великий спектр прав людини. Зокрема, впливає на право на зображення, право виражати свою ідентичність і займатися саморозвитком, захист персональних даних, а також низку інших прав (захист від дискримінації, вільні вибори – свободи, які зазнають впливу ситуативно). Тому наразі надважливо визначити застосовні стандарти й оцінити ризики для прав людини.

9. Правові аспекти створення голограми відомої особи.

Правові аспекти створення голограми відомої особи охоплюють комплекс питань, пов'язаних із балансом між свободою творчості, розвитком технологій та захистом особистих немайнових і майнових прав. Голограма як відтворення образу публічної особи (актора, політика, музиканта, спортсмена тощо) у віртуальному чи фізичному просторі не є лише технічним феноменом, а набуває правової значущості з моменту її використання у комерційних, культурних або інформаційних цілях.

Насамперед постає питання іміджевих прав (право на ім'я, право на зображення, право на повагу до приватного життя). Відтворення голограми без згоди особи або її спадкоємців може розглядатися як порушення права на зображення, навіть якщо воно здійснюється в публічному інтересі. Особливо гостро це питання стоїть після смерті відомої особи: створення «постумних голограм» (наприклад, відомих співаків на концертах) зачіпає сферу спадкових і суміжних прав, а також викликає етичні дискусії щодо допустимості «цифрового воскресіння».

З правової точки зору слід враховувати також авторське право та суміжні права. Якщо голограма відтворює виступ або зовнішність, захищену авторським правом чи правами виконавця, використання такого цифрового образу потребує відповідних ліцензій. У багатьох юрисдикціях діє принцип, що візуальне або аудіовізуальне відтворення образу є охоронюваним елементом, і будь-яке комерційне використання без дозволу вважається неправомірним.

Крім того, голограма може набувати статусу об'єкта інтелектуальної власності, якщо вона є результатом творчої діяльності розробників (3D-модель, сценарій виступу, технічне втілення). У цьому випадку виникає складне поєднання прав: з одного боку, права творців голограми, з іншого – особисті немайнові права зображуваної особи.

Особливу увагу слід приділяти і захисту споживачів від введення в оману. Використання голограми може створювати ілюзію реальної присутності особи, що викликає питання автентичності, достовірності та етики цифрових технологій. У деяких країнах вже обговорюються вимо-

ги маркування контенту, створеного із застосуванням deepfake чи подібних технологій, щоб уникнути обману публіки.

Таким чином, правові аспекти створення голограми відомої особи зводяться до кількох ключових напрямів: захист іміджових прав і права на зображення; дотримання авторських і суміжних прав; врегулювання питань спадкового права у випадку «постумних голограм»; визначення правового статусу голограми як об'єкта інтелектуальної власності; етичні та правові гарантії від введення в оману споживачів.

У майбутньому можна прогнозувати формування спеціальних норм у сфері цифрового права та суміжних інститутів, які забезпечать баланс між комерційними інтересами, свободою творчості та охороною особистих немайнових прав.

10. Електронний цифровий підпис як спосіб ідентифікації особи.

Електронний цифровий підпис (ЕЦП) є ключовим юридико-технічним механізмом ідентифікації особи в цифровому середовищі, що забезпечує правову визначеність у процесах електронного документообігу, дистанційних транзакцій та електронного урядування. Його поява стала результатом глобальної трансформації суспільства, переходу від паперових до електронних форм взаємодії, що вимагає гарантій достовірності та цілісності даних, а також захисту від підробок і маніпуляцій.

У правовій доктрині ЕЦП трактується як електронні дані, які за допомогою криптографічних методів зв'язуються з іншими електронними даними і використовуються для ідентифікації підписанта та підтвердження його волевиявлення. На міжнародному рівні базові стандарти визначені Модельним законом ЮНСІТРАЛ про електронні підписи (2001 р.), Директивою ЄС 1999/93/ЄС та чинним Регламентом ЄС №910/2014 (eIDAS), що встановлюють рівні електронного підпису: простий, удосконалений і кваліфікований. В Україні правове регулювання закріплене в Законі «Про електронні довірчі послуги», який гармонізований із європейськими стандартами.

Юридична значущість ЕЦП полягає в наданні електронним документам такої ж доказової сили, як і паперовим, підписаним власноруч. Особливу роль відіграє кваліфікований електронний підпис (КЕП), створений із використанням захищеного засобу та кваліфікованого сертифіката відкритого ключа. Він має повну юридичну рівність із власноручним підписом і печаткою, що підтверджено судовою практикою та міжнародними актами.

ЕЦП виконує комплекс функцій:

- ідентифікаційна – дозволяє достеменно встановити особу підписанта;
- автентифікаційна – підтверджує авторство електронного документа;
- захисна – гарантує цілісність і незмінність документа після підписання;
- волевиявлення – фіксує згоду особи на правочин або іншу юридично значущу дію;
- доказова – використовується як доказ у судових справах;
- економічна – сприяє зниженню транзакційних витрат та прискоренню ділового обороту.

З технічної точки зору, ЕЦП базується на асиметричній криптографії, яка передбачає використання пари ключів: приватного (належить виключно підписанту і використовується для створення підпису) та публічного (доступний іншим особам для перевірки підпису). Цей механізм забезпечує високу надійність і практично унеможливорює підробку.

Застосування ЕЦП охоплює широкий спектр сфер:

- електронне урядування та державні реєстри (подання податкової звітності, звернення до судів, отримання адміністративних послуг);
- корпоративний сектор (укладення договорів, обмін бухгалтерською документацією, електронний документообіг між підприємствами);
- банківсько-фінансова сфера (онлайн-транзакції, відкриття рахунків, підтвердження фінансових операцій);

- міжнародні комунікації (взаємне визнання підписів у рамках транскордонних відносин).

Проблемними аспектами є питання безпеки ключів, ризику їх компрометації, а також неоднаковий рівень визнання електронного підпису в різних юрисдикціях. Крім того, існує проблема правового співвідношення між різними рівнями електронного підпису (простим, удосконаленим і кваліфікованим), адже не всі з них мають однакову юридичну силу.

У перспективі розвиток ЕЦП пов'язаний із інтеграцією біометричних технологій, блокчейн-рішень та систем ідентифікації нового покоління, що має посилити рівень довіри до цифрових комунікацій і створити основу для формування єдиного глобального ринку електронних послуг.

Таким чином, електронний цифровий підпис виступає не лише технічним атрибутом електронного документа, а й фундаментальним правовим інститутом, що гарантує легітимність і правову визначеність у цифрових відносинах. Його впровадження є ключовою умовою становлення електронної держави, розвитку електронної комерції та забезпечення прав громадян у кіберпросторі.

Питання для самоперевірки:

1. Пояснити сутність та основні етапи формування концепції цифрової ідентичності фізичної особи.
2. Охарактеризувати різні підходи до розуміння терміну «симулякр» у контексті цифрового середовища.
3. Розкрити способи використання симулякрів як інструментів маніпуляції у віртуальному просторі.
4. Навести приклади застосування симулякрів у правовій сфері та їх правові наслідки.
5. Визначити поняття цифрової особи та описати її специфічні риси.
6. Проаналізувати співвідношення понять «цифрова особа» та «цифрова особистість».
7. Охарактеризувати складові цифрової ідентичності та її роль у віртуальному інформаційному середовищі.

8. Пояснити сутність цифрового аватару та визначити його особливості у контексті комунікації та самоідентифікації.
9. Розглянути правові аспекти створення та використання голограми відомої особи, враховуючи захист її немайнових прав.
10. Пояснити функціональне призначення електронного цифрового підпису як способу ідентифікації особи у цифровому середовищі.

Тема 3. Форми існування цифрової особи. 4 год

1. Цифрове життя: поняття та специфічні риси.
2. Цифрові права. Поняття та особливості
3. Право людини на зображення в мережі Інтернет та його захист.
4. Захист честі та гідності в мережі Інтернет.
5. Право на приватне життя та право на таємницю листування.
6. Право на забуття.
7. Поняття цифрової смерті та цифрової спадщини.
8. Правові наслідки смерті власника акаунту: за правилами користування окремих соціальних мереж.
9. Цифрове безсмертя.

Теоретичні відомості

1. Цифрове життя: поняття та специфічні риси.

Цифрове життя є феноменом сучасного інформаційного суспільства, що охоплює сукупність соціальних, комунікативних, економічних та культурних процесів, які здійснюються за допомогою цифрових технологій. Воно формується в умовах глобальної мережевої взаємодії, де цифрові платформи, соціальні мережі, штучний інтелект і віртуальна реальність стають не лише інструментами, а й середовищем існування людини. Науковці підкреслюють, що цифрове життя вже не є «паралельним» реальному, а інтегрується в нього, створюючи нову гібридну реальність³⁷.

³⁷ Castells M. The Rise of the Network Society. 2nd ed. Oxford: Blackwell Publishing, 2000. 597 p.

Специфічні риси цифрового життя проявляються у кількох вимірах. По-перше, це **мережевість і глобальність**: будь-яка дія у цифровому середовищі має потенційно транснаціональний характер, що змінює межі приватного й публічного. По-друге, **ідентичність у цифровому житті набуває множинності та фрагментарності**, оскільки особа може одночасно мати кілька цифрових образів – від аватарів у віртуальних світах до професійного профілю у LinkedIn чи особистої сторінки у Facebook. Це породжує феномен «цифрової особистості» як окремої соціально-правової категорії³⁸.

По-третє, важливою рисою є **тотальна медіатизація**, за якої будь-яка подія життя людини може бути зафіксована, відтворена та поширена у цифровій формі. У цьому аспекті формується новий тип публічності, де кордони між приватним і публічним життям стираються, а соціальні мережі стають головним простором самопрезентації. По-четверте, цифрове життя передбачає **безперервність та інтерактивність**, адже технології дозволяють бути постійно включеним у комунікацію, а також модифікувати соціальні ролі і відносини в режимі реального часу.

Сьогодні правова система стикається з викликом динамічності та невизначеності цифрових процесів, що вимагає розвитку доктрини «цифрових прав людини» та нових підходів до правосуб'єктності у віртуальному просторі.

Таким чином, цифрове життя – це інтегрований простір, де поєднуються біологічна, соціальна й віртуальна складові існування людини, що формує нову ідентичність, нові моделі комунікації та нові правові виклики.

На основі вищезазначених рис цифрового життя можемо запропонувати його визначення у широкому та вузькому значеннях. У **широкому значенні** цифрове життя – це сукупність усіх форм соціальної, економічної, культурної, комунікативної та правової активності людини, що здійснюється в цифровому середовищі за допомогою інформаційно-комунікаційних технологій. Воно охоплює

38 Turkle S. Alone Together: Why We Expect More from Technology and Less from Each Other. MIT Press, 2011. 384 p.

не лише віртуальні взаємодії, а й інтеграцію цифрових технологій у повсякденне «офлайнове» існування людини, формуючи єдину гібридну реальність. У цьому контексті цифрове життя постає як новий цивілізаційний вимір, що змінює межі приватного і публічного, трансформує ідентичність та породжує комплекс цифрових прав людини.

У **вузькому значенні** цифрове життя можна визначити як діяльність особи у віртуальному середовищі, що включає використання соціальних мереж, онлайн-сервісів, цифрових платформ, віртуальної та доповненої реальності. У цьому вимірі акцент робиться на індивідуальному вимірі – цифровій ідентичності, персональних даних, онлайн-комунікації та репрезентації особи у віртуальному просторі. Саме вузьке розуміння є більш прикладним і дозволяє визначити конкретні механізми правового регулювання та захисту прав особи у цифровому середовищі.

Таким чином, у широкому вимірі цифрове життя розглядається як соціокультурний феномен глобального масштабу, а у вузькому – як індивідуальний досвід людини у цифровому середовищі.

2. Цифрові права

В основі концепції поділу прав людини на покоління лежить генераційний підхід, тобто їх поділ на три покоління відповідно до їх історичного формування та розвитку. Перше покоління прав людини – громадянські і політичні права, це основа інституту прав людини (право на життя, право на свободу та особисту недоторканість, право на гідність особи тощо). Друге покоління прав людини – соціальні, економічні і культурні права (право на працю, відпочинок, соціальне забезпечення, медичну допомогу, захист материнства і дитинства тощо). Третє покоління прав людини називають солідарними (колективними) правами, тобто правами всього людства – правами людини, правами народів, правами нації, правами спільноти та асоціації: право на мир, безпеку, право на самовизначення народів тощо³⁹.

39 Маложен О.І. Четверте покоління прав людини в контексті української сучасності. *Юридичний науковий електронний журнал*. 2021. № 12. С. 41 (41-44)

Четверте покоління прав людини почало формуватися з розвитком науки, все більшою свободою і автономністю людини, зокрема, появою інформаційних технологій і все більшим зануренням людини у створюваний ними світ. До цього покоління прав відносять право на зміну статі, гендерну ідентичність, трансплантацію органів, штучне запліднення, вільну від дитини сім'ю, незалежне від державного втручання життя, на евтаназію тощо.

Вперше застосування поняття прав людини до управління мережею Інтернет відбулося під час Всесвітнього саміту з питань інформаційного суспільства в Женеві в 2003 році та отримало широке схвалення на Туніській зустрічі в 2005 році. На III Форумі з управління Інтернетом в Хайдарабаді (Індія) у 2008 році учасники einstайно дійшли висновку, що розвиток прав людини і принципи розвитку мережі Інтернет тісно пов'язані, а цифрове середовище має підтримувати права людини.

У 2011 році Комітет Міністрів Ради Європи в Декларації про принципи управління Інтернетом окреслив своє бачення Інтернету, орієнтованого на людину й побудованого на засадах поваги до прав людини. У 2012 році Комітет Міністрів Ради Європи створив Комітет експертів з прав інтернет-користувачів, завданням якого стала реалізація існуючих прав людини в цифровому середовищі. В Керівництві з прав людини для інтернет-користувачів Рада Європи наголошує, що діти та молодь мають право на освіту, щоб набути компетентності щодо захисту себе від інтернет-загроз, а також право на особливий захист від загроз під час використання мережі Інтернет, у тому числі від сексуальної експлуатації та насильства, інших форм злочинності.

У 2014 році Комітет Міністрів Ради Європи прийняв Рекомендації CM/Rec (2014) 6, в яких зазначив, що держави-члени зобов'язані забезпечити захист всіх прав людини та основних свобод, закріплених в Конвенції Ради Європи про захист прав людини і основоположних свобод. У Рекомендаціях підкреслюється, що існуючі права людини та основні свободи рівною мірою відносяться як до офлайн-простору, так і до онлайн-простору. Ніхто не повинен бути об'єктом незаконно-

го втручання в реалізацію їх прав та основних свобод під час перебування в мережі Інтернеті, не повинні поширюватися заходи загально-го спостереження чи перехоплення інформації. Втручання у приватне життя щодо персональних даних дозволяється лише за виняткових обставин, передбачених законом, наприклад, у разі здійснення кримінального розслідування. Зазначається, що Інтернет має цінність як суспільна служба. Люди, спільноти, органи державної влади та приватні компанії здійснюють свою діяльність через Інтернет і законно сподіваються на те, що матимуть доступ до Інтернет-послуг, які будуть надаватися без будь-якої дискримінації, за розумну ціну, а також будуть безпечними, надійними та безперебійними⁴⁰.

На 32-й сесії ООН 27 червня 2016 року Рада ООН з прав людини ухвалила резолюцію «Заохочення, захист і здійснення прав людини в Інтернеті»⁴¹, в якій зазначено, що ті ж самі права, які людина має в офлайн-просторі, повинні також захищатися в онлайн-просторі.

Таким чином, до окремої групи прав належать права, пов'язані з можливостями реалізації людиною своїх прав і інтересів у мережі, які визначають як сукупність прав, тісно пов'язаних з розвитком інформаційно-комунікаційних технологій, глобального інформаційного простору та формуванням інформаційного суспільства⁴².

Слід зазначити деяку термінологічну плутанину, яка існує у працях науковців, що займаються відповідною проблематикою. Ці права називають інформаційними, віртуальними, цифровими (digital rights), Інтернет-правами (Internet rights), правами на комунікацію (rights to communicate).

Ми не поділяємо точку зору, відповідно до якої до основних цифрових прав належать: право на доступ до Інтернету, право на вираження поглядів онлайн, право на приватність і захист персональних

40 Рекомендація СМ/Rec(2014)6 Комітету міністрів Ради Європи державам-членам щодо використання Посібника з прав людини для Інтернет користувачів. <https://www.refworld.org/sites/default/files/attachments/55cb538a4.pdf>

41 Рада ООН з прав людини ухвалила резолюцію про права онлайн - Центр демократії та верховенства права

42 Вакарюк Л. Основні підходи до розуміння поняття «інформаційні права людини». *Підприємництво, господарство і право*. 2018. № 2. С. 155-159.

даних, право на свободу та особисту безпеку онлайн, право на мирні зібрання, асоціації та/або використання електронних інструментів демократії, а також право на цифрове самовизначення (або право на забуття)⁴³. На наш погляд, тут змішуються декілька груп прав: інформаційних, інформаційних мережевих і власне цифрових прав. Ця класифікація дасть можливість чіткого розмежування різних категорій прав і уникнути їх змішування.

При цьому, ті права, які надають людині можливість доступу до інформації, реалізації права на інформацію – є інформаційними. Та категорія прав, яка надає можливість доступу до мережі Інтернет мала б називатися відповідно інформаційно-мережевими правами. В свою чергу, інформаційні мережеві права є базовими для виникнення цифрових прав.

Ті права, які дають можливість безпосередньо функціонувати в мережі, створюючи чи використовуючи контент тощо є правами цифровими. До них можна віднести, наприклад, право на свободу та безпеку в Інтернеті, конфіденційність персональних даних у мережі, право на отримання переваг та вигоди від контенту, право на працю в мережі, право на конфіденційність, право на свободу від стеження, право на використання шифрування, право на захист віртуальної особистості, право залишатися анонімним, право на цифрове самовизначення (або право на забуття) тощо.

Крім цього, інформаційна складова цих прав доповнюється також складовою комунікаційною, що відрізняє їх від суто інформаційних прав і від інформаційно-мережевих прав.

Поняття цифрових прав має акцентувати увагу на особливостях прав, які отримує особа, перебуваючи безпосередньо у віртуальному просторі, вони пов'язані зі сферою сучасних інформаційних технологій, зокрема Інтернет-мережею.

Наразі ми маємо справу з формуванням і розвитком цифрової екосистеми, тобто нової реальності технологічного існування людства, де технологічні платформи на принципах розподіленого реє-

43 Тверезовська К. С. Поняття, види та значення цифрових прав людини. *Юридичний науковий електронний журнал*. 2024. № 6. С. 473 (472-476).

стру (blockchain та ін.), Інтернет речей (Internet of Things), штучний інтелект і машинне навчання (artificial intelligence), хмарні сервіси і обчислення (cloud computing), «розумні» комплекси та пристрої (Smart Everything), аналітичні бази великих даних (Big Data), віртуальна і доповнена реальність (augmented & additive reality), умови кібербезпеки (cybersecurity), а також соціальні мережі і платформи (Telegram, Facebook), електронні сервіси, які застосовуються в найрізноманітніших сферах людської діяльності, створили нові умови, новий «технологічний базис» для зміни традиційних правових інститутів і їх адаптації до нових реалій.

Цифрові права можуть включати широке коло основних прав, які реалізуються в цифровому середовищі і вимагають дослідження з точки зору властивостей цього середовища. При цьому базові цифрові права є перш за все похідними від інформаційних прав, але до них не зводяться. На сьогодні вже активно виділяють такі цифрові права, як: право на доступ до інформації; право на доступ до інформаційних платформ і технологій; право на захист персональних даних (особистих і біометричних); право на свободу зібрань та об'єднань онлайн; право на цифрову освіту та доступ до цифрових знань; права, пов'язані із захистом генетичної інформації; права на участь в обороті майна в цифровій сфері; право бути забутим; можливість реалізації особистих, соціальних, економічних, політичних і культурних прав на основі нових технологічних платформ. Тобто, традиційні та розповсюджені у всьому світі права та свободи людини трансформуються, наповнюються новими аспектами та змістом, розгалужуються на такі, що пов'язані саме з процесом цифровізації.

3. Право людини на зображення в мережі Інтернет та його захист.

Право людини на власне зображення сьогодні набуває особливого ваги в системі інформаційного, цивільного та інтелектуального права, перетворюючись на одну з ключових тем сучасного правового дискурсу. Якщо раніше воно розглядалося переважно в контексті

класичних прав на недоторканність приватного життя, то цифрова епоха радикально змінила масштаби та зміст цієї проблематики, відкривши нові виклики та загрози.

В умовах глобалізованого інформаційного суспільства візуальні образи людини вільно циркулюють у віртуальному просторі: соціальних мережах, онлайн-медіа, на вебресурсах державних інституцій, комерційних компаній чи творчих платформ, присвячених дизайну та фотографії. При цьому зображення особи нерідко опиняється у відкритому доступі без її відома та згоди. Особливої гостроти проблема набуває у випадках, коли фотографії використовуються для введення в оману з метою уникнення відповідальності за протиправні дії, а також у випадках несанкціонованого застосування образу людини у рекламі товарів, послуг чи комерційних проєктів.

Такі ситуації порушують баланс між суспільними інтересами та фундаментальними правами особи, актуалізуючи дискусію щодо меж і змісту права на власне зображення. Це право, яке охоплює можливість контролювати публічний показ, відтворення та поширення візуального образу, тісно пов'язане з гарантіями особистої недоторканності, честі, гідності й ділової репутації. Відповідно, воно повинно перебувати під ефективним захистом держави.

Міжнародні стандарти у цій сфері підкреслюють пріоритетність охорони приватності. Так, стаття 8 Конвенції про захист прав людини і основоположних свобод гарантує кожному право на повагу до приватного і сімейного життя, житла та кореспонденції, а стаття 12 Загальної декларації прав людини 1948 року забороняє будь-яке свавільне втручання в особисте і сімейне життя. У національному вимірі ці положення конкретизовані у статті 32 Конституції України, яка передбачає заборону збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, окрім випадків, прямо визначених законом і виправданих інтересами національної безпеки, економічного добробуту чи прав людини. Конституційні гарантії включають також право на судовий захист, зокрема на спростування недостовірної інформації та вимогу вилучення неправомірно поширених відомостей.

Відповідно до Закону України «Про захист персональних даних» персональні дані – це відомості або сукупність відомостей про фізичну особу, яка вже ідентифікована або може бути конкретно ідентифікована. Таким чином, зображення людини розглядається як її персональні дані, що безпосередньо пов'язані із захистом приватного життя.

У зазначеному Законі визначено перелік підстав для обробки конфіденційної інформації, серед яких – згода особи. Відповідно до статті 2 цього ж Закону, згода – це поінформоване, добровільне волевиявлення людини. Із положень цієї статті випливає, що існує кілька способів надання згоди:

- у письмовій формі;
- усна згода або випадок, коли особу було попереджено, і вона не висловила заперечень.

Крім того, згода повинна відповідати таким ознакам:

- поінформованість;
- добровільність;
- форма, яка дає змогу чітко встановити погодження чи заперечення щодо обробки персональних даних.

Поінформованість означає, що особа має бути обізнана, ким і з якою метою здійснюватиметься обробка її персональних даних. Добровільність передбачає право людини самостійно вирішувати, чи надавати згоду на обробку своїх даних, чи відмовитися від цього. При цьому згода може бути відкликана, за винятком випадків, прямо визначених законом.

Зображення людини охороняється як немайнове право. У статті 307 Цивільного кодексу України (далі – ЦК України) встановлено, що фізична особа може бути знята на фото-, кіно-, теле- чи відеоплівку виключно за її згодою. Водночас така згода вважається наданою, якщо зйомка здійснюється відкрито на вулиці, під час зборів, конференцій, мітингів та інших заходів публічного характеру. При цьому особа, яка погодилася на знімання, має право вимагати припинення публічного показу свого зображення у тій частині, яка стосується її особистого життя.

Відповідно до статті 308 ЦК України, фотографія або інші художні твори, на яких зображена людина, можуть бути публічно показані, відтворені чи розповсюджені лише за її згодою, а у разі смерті – за згодою осіб, визначених частиною четвертою статті 303 цього Кодексу.

Зображення людини нерідко використовується в маркетингових цілях. З огляду на це, у статті 8 Закону України «Про рекламу» встановлено загальне правило, відповідно до якого забороняється використання зображення фізичної особи або її імені без письмової згоди.

Надання дозволу на використання чужого зображення породжує юридичні наслідки. Це означає, що особа повинна усвідомлювати зміст і характер своїх дій на момент їх вчинення, а також мету, на досягнення якої вони спрямовані. Інакше кажучи, для надання такої згоди особа має володіти необхідним обсягом дієздатності⁴⁴. Відповідно, згода на використання зображення є правомірною вольовою дією, що спрямована на виникнення певних правових наслідків та може бути надана лише дієздатною особою. З цього випливає також заборона на приховану фото- чи відеозйомку людини, за винятком випадків, прямо передбачених законом. При цьому незаконне отримання інформації із застосуванням спеціальних (негласних) технічних засобів тягне за собою кримінальну відповідальність⁴⁵.

Окрему проблему становить використання зображень дітей без згоди їхніх батьків або законних представників. Серед батьків усе частіше виникає занепокоєння щодо відео- чи фотозйомки та подальшого поширення зображень їхніх дітей сторонніми особами. Згідно зі статтею 6 Сімейного кодексу України, правовий статус дитини має особа до досягнення повноліття: малолітньою вважається дитина віком до 14 років, а неповнолітньою – від 14 до 18 років.

44 Сліпченко С.О. Надання згоди фізичною особою, що зображена на фотографії, як юридичний факт за ЦК України. Право України. 2008. № 3. С. 110-114.

45 Шадська У. Правовий аналіз регулювання права людини на своє зображення. URL: [Правовий аналіз регулювання права людини на своє зображення – Українська Гельсінська спілка з прав людини](#)

Відео- чи фотозйомка (як форма збору інформації) розглядається законодавством як один із способів обробки персональних даних, що підпадає під дію Закону України «Про захист персональних даних». На відміну від дорослої людини, яка здатна самостійно оцінити ризики та ухвалити рішення щодо згоди на збір інформації про себе, дитина такої можливості не має. Саме тому законодавство приділяє особливу увагу питанням обробки даних малолітніх або недієздатних осіб. У випадках, коли сторонні особи бажають здійснити збір інформації про дитину (наприклад, сфотографувати її та надалі використати зображення), вони зобов'язані отримати дозвіл від батьків чи усиновлювачів, які усвідомлюють значення таких дій і можливі їхні наслідки.

Згідно зі статтею 10 Закону України «Про охорону дитинства», розголошення чи публікація будь-якої інформації про дитину, здатної завдати їй шкоди, забороняється без згоди законного представника. Типовою помилкою є переконання, що дозвіл на фото- чи відеозйомку на території школи чи дитячого садка можуть надати вчителі або вихователі. Насправді, відповідно до статті 242 Цивільного кодексу України, такими законними представниками є лише батьки чи усиновлювачі (інші особи – лише у випадках, прямо передбачених законом).

Таким чином, будь-хто, хто має намір здійснювати обробку даних дитини, зобов'язаний отримати згоду саме від батьків. Вони, у свою чергу, мають право заборонити такі дії, вимагати видалення зображень, а у разі невиконання їхніх законних вимог – оскаржити ситуацію в суді або звернутися до Уповноваженого Верховної Ради України з прав людини.

Окремо варто враховувати положення статті 20 Закону України «Про рекламу», якими забороняється використання у рекламних матеріалах зображень дітей у небезпечних ситуаціях, а також демонстрування неповнолітніх у процесі споживання продукції, призначеної виключно для дорослих або забороненої для дітей.

Однак ризики для дітей не обмежуються сферою реклами. Особливо вразливою сферою є інтернет. Наприклад, у країнах ЄС діє Загальний регламент захисту даних (GDPR), який встановлює суворі вимоги до обробки персональних даних дітей. Регламент підкреслює,

що діти потребують особливого захисту, адже можуть бути менш обізнаними щодо ризиків та наслідків обробки їхніх персональних даних. Особливий захист поширюється, зокрема, на використання даних дітей у маркетингових цілях, створення профілів користувачів та збирання даних під час користування онлайн-послугами (п. 38). Відповідно, компанії, що працюють з дітьми з ЄС, зобов'язані отримати згоду батьків, інакше вони ризикують бути оштрафовані на суму до 20 мільйонів євро або 4 % від річного обігу.

У США також діє федеральний Закон про захист конфіденційності дітей в інтернеті (Children's Online Privacy Protection Act – COPPA), який забороняє збір будь-якої інформації про дітей, молодших 13 років, без згоди їхніх законних представників. Крім того, у низці штатів запроваджені додаткові нормативні акти, що передбачають відповідальність за переслідування чи цькування неповнолітніх у соціальних мережах.

Водночас право на приватне життя не є абсолютним. Закон допускає обробку конфіденційної інформації без згоди особи виключно в інтересах національної безпеки, економічного добробуту чи захисту прав людини. Згідно зі статтею 308 ЦК України, допускається використання зображення людини без її згоди, якщо цього вимагає необхідність захисту її інтересів або інтересів інших осіб.

Охорона інтересів фізичної особи, зображеної на фотографіях чи інших художніх творах, передбачена статтею 307 ЦК України. Водночас між положеннями статей 307 і 308 існує принципова відмінність: у першому випадку йдеться переважно про механічне відтворення зображення людини (наприклад, фотографування на фотоплівку), тоді як у другому – про творче відтворення у картинах, скульптурах та інших формах мистецького вираження. Саме тому норми статті 308 ЦК України більшою мірою стосуються сфери інтелектуальної власності, зокрема подальшого використання створеного твору, ніж власне факту отримання зображення особи⁴⁶.

46 Шадська У. Правовий аналіз регулювання права людини на своє зображення. URL: [Правовий аналіз регулювання права людини на своє зображення – Українська Гельсінська спілка з прав людини](#)

Закон України «Про захист персональних даних» встановлює ще одну підставу обробки без згоди особи – «захист життєво важливих інтересів суб'єкта персональних даних». Під цим поняттям слід розуміти інтереси, безпосередньо пов'язані з охороною життя та здоров'я людини. Це може стосуватися випадків, коли особа через свій стан не може надати згоду на обробку персональних даних у медичних цілях, або коли необхідна публікація зображення для її розшуку.

Згода як підстава для збору даних може не застосовуватися також тоді, коли діють інші положення статті 11 Закону «Про захист персональних даних», які допускають обробку даних без згоди, якщо це прямо передбачено законом для виконання відповідних повноважень. Так, наприклад, Національна поліція має право здійснювати фото- чи відеофіксацію особи без її згоди, оскільки таке право визначено у профільному законодавстві.

Щодо суспільного інтересу, який у певних випадках може переважати над правом особи на конфіденційність, стаття 29 Закону України «Про доступ до публічної інформації» передбачає можливість обробки даних, якщо вони свідчать про загрозу державному суверенітету чи територіальній цілісності, забезпечують реалізацію конституційних прав і свобод, вказують на можливість порушення прав людини, введення громадськості в оману, завдання шкоди довкіллю тощо. Це означає, що кожен випадок має розглядатися індивідуально, з урахуванням того, чи виправдане використання зображення людини без її згоди в інтересах держави, суспільства або самої особи.

При цьому отримання зображення має здійснюватися відкрито, із поінформованістю суб'єкта. Прихований збір даних дозволяється лише у виняткових ситуаціях. Зокрема, Закон України «Про оперативно-розшукову діяльність» визначає перелік органів державної влади, які наділені правом проводити таємну фото- чи відеофіксацію, а також умови, за яких такі дії є допустимими.

Отже, правове регулювання використання зображення людини в Україні базується на балансі між особистими немайновими правами та суспільними інтересами. З одного боку, згода особи є основною гарантією захисту її приватності та контролю за власним образом,

а з іншого – закон допускає винятки, коли суспільна безпека, права інших осіб або життєво важливі інтереси потребують пріоритетного захисту. Такий підхід відповідає європейським стандартам охорони прав людини й водночас дозволяє забезпечити публічний порядок та належне функціонування державних інституцій.

4. Захист честі та гідності в мережі Інтернет.

Захист честі та гідності в мережі Інтернет є однією з ключових проблем сучасного інформаційного суспільства. Честь і гідність виступають фундаментальними немайновими правами людини, що мають як внутрішній, так і зовнішній вимір: гідність відображає внутрішню цінність особи, її право на повагу, а честь – це соціальна оцінка й репутація людини в очах суспільства. В умовах цифрового середовища посягання на ці права набуває нових форм: поширення неправдивих відомостей, принизливих коментарів, зображень без згоди особи, маніпуляцій та образ у соціальних мережах чи на інтернет-порталах. Особливістю онлайн-простору є швидкість та масштаб поширення інформації, а також анонімність користувачів, що значно ускладнює механізми захисту та встановлення відповідальності.

Міжнародні стандарти у сфері прав людини, зокрема Європейська конвенція з прав людини, гарантують право на повагу до приватного життя (стаття 8) та свободу вираження поглядів (стаття 10), тому Європейський суд з прав людини у своїй практиці формує підхід, заснований на балансі між цими правами. У відомій справі *Delfi AS v. Estonia* (2015) ЄСПЛ визнав новинний портал відповідальним за образливі коментарі, які тривалий час залишалися без модерації, підкресливши важливість активної позиції платформ щодо видалення незаконного контенту. Подальша практика Суду деталізує критерії, які потрібно враховувати при вирішенні таких спорів: характер поширеної інформації, статус особи (публічна чи приватна), наявність суспільного інтересу, форма висловлювань та їх вплив на репутацію. У справі *Özlu v. Türkiye* (2024) Суд також акцентував увагу на пропорційності втручання держави в право на свободу вираження, наголошуючи, що надмірно суворе покарання може саме по собі становити порушення Конвенції.

В Україні правові механізми захисту честі та гідності передбачені Конституцією, Цивільним кодексом (зокрема статтями про спростування недостовірної інформації та компенсацію моральної шкоди), Законом «Про захист персональних даних» і низкою спеціальних законів. Українські суди визнають право особи вимагати спростування недостовірних відомостей, відшкодування шкоди та видалення принизливого контенту. Однак на практиці залишається низка проблем: відсутність уніфікованих критеріїв оцінки шкоди, складність доведення факту поширення недостовірних даних в умовах анонімності інтернет-користувачів, а також недостатня ефективність процедур блокування інформації на платформах.

Важливо враховувати й категорію суспільного інтересу, яка може переважати над правом особи на захист честі та гідності. Згідно зі статтею 29 Закону України «Про доступ до публічної інформації», поширення відомостей може бути виправдане, якщо вони стосуються загроз державному суверенітету, порушень прав людини, безпеки громадян або значущих екологічних ризиків. Тому кожна ситуація повинна оцінюватися окремо, з урахуванням балансу між приватними і публічними інтересами.

Таким чином, захист честі та гідності в інтернеті є сферою, де переплітаються право на свободу слова, право на приватність і право на репутацію. Ефективність такого захисту залежить від узгодженості міжнародних та національних стандартів, належної судової практики, а також від технічної спроможності платформ швидко реагувати на повідомлення про порушення. Лише поєднання цих факторів дає можливість забезпечити реальний захист особистих прав у цифрову епоху.

5. Право на приватне життя та право на таємницю листування.

Право на приватне життя та право на таємницю листування належать до фундаментальних особистих немайнових прав, що гарантуються як національним законодавством України, так і міжнародними актами у сфері прав людини. Конституція України у статті 32

закріплює право кожного на невтручання в особисте і сімейне життя, а також забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, за винятком випадків, визначених законом і лише в інтересах національної безпеки, економічного добробуту та прав людини. Окремо у статті 31 Конституції проголошено право на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, яке може бути обмежене лише за вмотивованим рішенням суду.

Міжнародні стандарти у сфері прав людини також послідовно захищають приватне життя та комунікації. У статті 8 Європейської конвенції про захист прав людини і основоположних свобод йдеться про право кожної особи на повагу до її приватного і сімейного життя, житла та кореспонденції. Європейський суд з прав людини у своїй практиці неодноразово наголошував, що держава має не лише утримуватися від втручання, але й забезпечувати позитивні зобов'язання зі створення ефективних механізмів захисту. Так, у справі *Klass and others v. Germany* Суд визначив, що навіть у випадках, коли допускається обмеження таємниці комунікацій з міркувань національної безпеки, воно має бути пропорційним, законодавчо врегульованим та супроводжуватися ефективними гарантіями проти зловживань.

В українському праві право на приватність та таємницю листування закріплене у Цивільному кодексі, який у статтях 301–303 визначає, що фізична особа має право на особисте життя, невтручання в кореспонденцію та захист від незаконного збирання чи поширення інформації про неї. Закон «Про захист персональних даних» деталізує правила щодо згоди на обробку конфіденційної інформації, включаючи дані про комунікації. Водночас існують спеціальні закони, що регулюють питання оперативно-розшукової діяльності, контррозвідальної діяльності та боротьби з тероризмом, які передбачають можливість обмеження цих прав, але виключно на підставі судового рішення та з дотриманням принципу необхідності.

У цифрову епоху право на приватне життя та таємницю листування отримує нові виклики. Зокрема, йдеться про електронну по-

шту, месенджери, соціальні мережі, хмарні сервіси. Судова практика як в Україні, так і в Європі підтверджує, що електронні форми комунікацій підлягають такому самому захисту, як і традиційні листи чи телефонні розмови. Разом з тим, з огляду на поширеність кіберзлочинів, незаконного стеження та масового збору даних, особливої актуальності набуває питання забезпечення балансу між правом особи на приватність і суспільними інтересами.

Право на приватне життя у сучасному праворозумінні розглядається як фундаментальна складова людської автономії та свободи, що передбачає можливість особи самостійно визначати межі доступу інших до відомостей про себе, до власного життєвого простору та до тих сфер, які не повинні ставати предметом стороннього втручання⁴⁷. Його суть полягає у визнанні того, що кожна людина має внутрішній простір, який охороняється законом і який не може бути порушений без її згоди чи без достатніх правових підстав. Власне приватність охоплює різні аспекти – від захисту фізичної недоторканності й особистих стосунків до інформаційної безпеки в цифровому середовищі.

Особливість права на приватне життя полягає в тому, що воно має багатовимірний характер: поєднує особисту, сімейну, соціальну та інформаційну сфери. В умовах цифровізації та глобальної мережевої комунікації його межі стають дедалі складнішими для окреслення. Людина залишає цифрові сліди в соціальних мережах, месенджерах, онлайн-торгівлі, а також у сфері електронних державних послуг. Це зумовлює ризики неконтрольованого збирання, поширення й використання даних, що підкреслює значення права на приватність не лише як особистого блага, але й як елементу інформаційної безпеки та довіри до правової системи.

Важливим є і те, що право на приватне життя є тісно пов'язаним із людською гідністю: порушення приватності сприймається не лише як вторгнення у таємницю чи персональні дані, а й як приниження, знеці-

47 Кравченко І.М. Проблеми нормативного визначення поняття «приватне життя» з огляду на допустимість меж обмеження прав працівників під час здійснення роботодавцем заходів контролю. Науковий вісник Національної академії внутрішніх справ. 2021. № 1 (118). С. 82-93

нення особи. Тому його охорона має не тільки юридичний, але й етичний вимір, а також виступає індикатором демократичності суспільства.

Право на таємницю листування є однією з найдавніших і водночас найактуальніших гарантій приватності, адже воно безпосередньо пов'язане зі свободою комунікації та можливістю обмінюватися інформацією без страху стороннього контролю. У класичному розумінні це право стосується листів у паперовій формі, телефонних переговорів чи телеграм, однак у сучасному цифровому середовищі воно поширюється на електронну пошту, повідомлення у месенджерах, соціальних мережах та будь-які інші канали приватного спілкування. Його суть полягає в тому, що ніхто – ані приватні особи, ані держава – не має права ознайомлюватися зі змістом кореспонденції без чітких правових підстав і належних процесуальних гарантій⁴⁸.

З огляду на розвиток інформаційних технологій і практику Європейського суду з прав людини (наприклад, справа “Copland v. the United Kingdom” (2007)), право на таємницю листування розглядається широко: воно охоплює не лише зміст повідомлень, але й метадані – відомості про те, з ким, коли і як довго спілкувалася особа. Саме тому втручання у приватну комунікацію може відбуватися лише в умовах крайньої необхідності – для запобігання злочинам, охорони національної безпеки чи захисту прав інших осіб – і завжди має супроводжуватися судовим контролем.

Особливим викликом сьогодні є масове збирання та зберігання даних про користувачів, що здійснюється як державними органами, так і приватними корпораціями. Питання доступу до переписки у месенджерах, зокрема з використанням наскрізного шифрування, стає предметом міжнародних дискусій між інтересами безпеки і необхідністю захисту приватності. Саме право на таємницю листування тут набуває особливого значення, оскільки воно є одним із фундаментальних засобів захисту свободи вираження поглядів і водночас гарантією довіри до цифрового середовища.

48 Шимон С. І., Лупало О. А. Право особи на таємницю кореспонденції: питання публічно-правової та приватно-правової термінології. Науковий вісник Ужгородського Національного Університету, 2022. С. 118-125. <https://visnyk-juris-uzhnu.com/wp-content/uploads/2022/10/22.pdf>

Багато в чому захист цього права виступає своєрідним маркером зрілості демократичних інституцій: чим більше держава здатна гарантувати реальну таємницю приватного спілкування, тим вище рівень свободи і прав людини в суспільстві.

6. Право на забуття

Правом на забуття визнається право людини, що дозволяє їй вимагати за певних умов видалення своїх особових даних із загального доступу через пошукові системи, тобто посилань на ті дані, які, на її думку, можуть заподіяти їй шкоду.

Іншими словами, правом на забуття визнається право особи вимагати в пошуковиків, зокрема в Google, видалення своїх даних із результатів пошукових запитів. Водночас слід розуміти, що мова йде лише про видалення результатів пошуку, тоді як видалення небажаного контенту із сайтів здійснюється шляхом контакту з власниками сайтів, на яких розміщено саму інформацію.

Право на забуття є відносно новим концептом у сфері захисту персональних даних, яке виникло у відповідь на цифровізацію суспільства та масове поширення інформації про особу в Інтернеті. Воно передбачає можливість для людини вимагати видалення або обмеження доступу до інформації про себе, яка стала недостовірною, застарілою або неактуальною, а також такої, що порушує її приватність чи гідність. Концепція права на забуття виникла як юридична відповідь на ситуації, коли інформація, доступна в глобальних мережах, здатна завдавати шкоди репутації або порушувати особисті права, навіть багато років після її публікації.

В Європейському Союзі право на забуття було закріплене у рішенні Європейського суду справедливості у справі **Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González (2014)**⁴⁹, де суд визнав, що фізична особа має право вимагати від пошукових систем видалення посилань на

49 Court of Justice of the European Union. Case C-131/12. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Judgment of 13 May 2014. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131>

інформацію про неї, якщо вона є застарілою, недостовірною або надмірною стосовно цілей її обробки. На практиці це право не є абсолютним і передбачає баланс між приватністю особи та правом на свободу вираження та доступ до інформації.

В Україні концепт права на забуття поки що імплементується через **Закон України «Про захист персональних даних»**, де визначено, що суб'єкт персональних даних має право вимагати припинення обробки своїх персональних даних або їх видалення у разі порушення законних прав, а також у разі втрати мети збору та обробки таких даних. Практичне застосування цього права в Україні пов'язане з викликами, зокрема технічними та організаційними, оскільки глобальні пошукові системи та соціальні мережі, на які посилаються заявники, перебувають за межами юрисдикції національних органів влади.

Підходи до розгляду поняття «право на забуття» у науковій та правозастосовній літературі різняться залежно від акценту на праві на приватність, контролі над персональними даними або на балансі між приватним і публічним інтересом. Перший підхід розглядає право на забуття як розширення права на приватне життя: воно полягає у можливості особи контролювати інформацію про себе, яка циркулює в цифровому середовищі, і вимагати видалення даних, що порушують її приватність або застаріли. З точки зору цього підходу ключовим є захист гідності та автономії особи, а цифрове середовище виступає лише середовищем реалізації прав.

Другий підхід акцентує на праві на контроль над персональними даними, яке тісно пов'язане із законодавством про захист персональних даних та інформаційну безпеку. Тут право на забуття розглядається як юридичний механізм забезпечення принципу мінімізації обробки даних та можливості суб'єкта даних самостійно визначати термін і обсяг їх зберігання. Цей підхід найбільш близький до регламенту ЄС GDPR (2016/679), де у статті 17 прямо встановлено право на видалення персональних даних («right to erasure»), включно з вимогами щодо балансу між правами особи та суспільним інтересом.

Третій підхід розглядає право на забуття як інструмент врегулювання інформаційних потоків у суспільстві. Тут акцент робиться на збалансуванні права на інформацію і публічний інтерес із правом особи на приватність. З цього погляду право на забуття не є абсолютним: воно не дає можливості вилучити будь-яку інформацію, що вже потрапила в мережу, а передбачає процедури оцінки її актуальності, суспільної значущості та потенційного шкодочинного впливу на репутацію.

Крім того, у наукових колах виділяють і техніко-правовий підхід, який зосереджується на проблемах реалізації права на забуття у цифровому середовищі: питання видалення даних із серверів, кешованих копій, резервних баз та пошукових індексів. Цей підхід підкреслює необхідність співпраці між законодавчими, технічними та корпоративними механізмами для ефективного здійснення права.

Отже, у сучасній доктрині право на забуття розглядають багатопланово: як елемент захисту приватності, як механізм контролю за персональними даними, як інструмент регулювання суспільної інформаційної сфери та як технічну проблему у цифровому середовищі. Цей багатовекторний підхід забезпечує комплексну оцінку його значення для фізичних осіб, бізнесу та держави.

Таким чином, право на забуття є механізмом реалізації права на приватне життя та контролю за персональними даними.

7. Поняття цифрової смерті та цифрової спадщини.

Поняття цифрової смерті та цифрової спадщини є новими категоріями у правовій науці та практиці, що виникли у зв'язку з масовим поширенням цифрових технологій і активним використанням Інтернету для зберігання персональної інформації. **Цифрова смерть** визначається як стан, коли фізична особа припинила своє життя, а її цифрові сліди, акаунти, дані та активність у мережі залишаються доступними у віртуальному середовищі. Така концепція охоплює не лише соціальні мережі та електронну пошту, а й банківські акаунти, хмарні сховища, блоги, медіа-контент та будь-які інші цифрові активи, що ідентифікують особу.

Цифрова спадщина, у свою чергу, розглядається як сукупність цифрових активів та персональних даних померлої особи, які мо-

жуть бути передані у власність чи управління визначеним спадкоємцям або особам, уповноваженим на їх використання. У цьому контексті постає питання правового статусу таких активів: чи належать вони до майна померлої особи, як їх можна розпоряджатися, і яким чином забезпечити захист приватності та конфіденційності посмертної інформації.

З розвитком інформаційних технологій і соціальних мереж цифрова спадщина набуває особливого значення для PR-технологій та корпоративної практики, оскільки акаунти померлих осіб можуть містити комерційно цінну інформацію або бути частиною бренду. У науковій літературі виділяють кілька підходів до регулювання цифрової спадщини: один із них акцентує на майнових правах, коли цифрові активи прирівнюються до майна і можуть успадковуватися; інший підхід – на немайнових правах, що передбачає захист приватності, репутації та іміджу померлої особи.

На практиці в різних юрисдикціях створено механізми управління цифровою спадщиною. Наприклад, у ЄС та США соціальні мережі (Facebook, Google) надають користувачам можливість за життя визначити спадкоємців своїх акаунтів або встановити політику видалення після смерті. Це питання тісно пов'язане з правом на приватне життя, захистом персональних даних та етичними нормами щодо пам'яті про померлих.

Таким чином, цифрова смерть і цифрова спадщина стають предметом міждисциплінарного аналізу, що охоплює правові, технологічні, етичні та соціальні аспекти, і мають важливе значення для управління інформаційними ресурсами в умовах сучасного цифрового суспільства.

8. Правові наслідки смерті власника акаунту: за правилами користування окремих соціальних мереж.

Правові наслідки смерті власника акаунту в соціальних мережах визначаються, передусім, умовами використання конкретної платформи та міжнародними та національними нормами щодо цифрової спадщини та захисту персональних даних. Соціальні мережі роз-

робляють спеціальні політики, що регламентують, що відбувається з акаунтами померлих користувачів, і ці правила зазвичай передбачають декілька можливих сценаріїв.

Власник акаунту може за життя визначити, що повинно статися з його цифровими даними після смерті. Наприклад, Facebook надає можливість призначити «керівника акаунту після смерті» (Legacy Contact), який зможе керувати обліковим записом у обмеженому режимі: публікувати меморіальні повідомлення, відповідати на запити друзів або завантажувати контент, не маючи доступу до приватних повідомлень користувача. Також акаунт може бути остаточно видалений на вимогу власника або спадкоємців після підтвердження смерті. Google (YouTube, Gmail) реалізував «Inactive Account Manager», що дозволяє користувачеві заздалегідь визначити, кому будуть надані дані у разі тривалого бездіяльного періоду або смерті, або ж встановити автоматичне видалення акаунту.

З точки зору права, смерть власника акаунту не припиняє існування цифрових активів, які можуть розглядатися як частина цифрової спадщини, що підлягає управлінню спадкоємцями. В українському правовому полі відсутні спеціальні норми щодо соціальних мереж, але положення Цивільного кодексу України та Закону України «Про захист персональних даних»⁵⁰ дозволяють спадкоємцям або уповноваженим особам звертатися до адміністрацій платформ для отримання доступу до цифрових активів або їх видалення, зберігаючи при цьому баланс між правом на приватне життя померлого та суспільним інтересом.

Таким чином, правові наслідки смерті власника акаунту визначаються поєднанням правил користування конкретної платформи, права власності та немайнових прав померлої особи, а також регуляторних вимог щодо обробки персональних даних. Важливо, щоб спадкоємці або призначені особи діяли в рамках закону та умов користування сервісом, оскільки невиконання цих правил може призвести до блокування або втрати доступу до цифрових активів.

50 Про захист персональних даних: Закон України № 2297-VI від 1 червня 2010 року. Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481.URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

Права інтелектуальної власності на контент, що став цифровою спадщиною, набувають особливого значення у правовому полі цифрових технологій, оскільки цифрові твори, створені померлою особою, можуть мати як майновий, так і немайновий характер. До цифрової спадщини належать текстові матеріали, аудіо- та відеоконтент, фотографії, графічні та художні твори, програмне забезпечення, бази даних та будь-які інші об'єкти авторського або суміжного права, створені користувачем у цифровому середовищі.

Майнові права на такі твори можуть успадковуватися. Це означає, що спадкоємці мають право відтворювати, поширювати, комерційно використовувати або надавати ліцензії на використання контенту відповідно до волі померлого, якщо вона була визначена за життя, або згідно з національними нормами спадкування майнових прав. Наприклад, в Україні Цивільний кодекс⁵¹ та Закон України «Про авторське право і суміжні права» передбачають, що майнові права на твори після смерті автора переходять до спадкоємців на строк дії авторського права, а немайнові права – залишаються в нерозривній залежності від особистості творця.

Немайнові права охоплюють право на ім'я автора, на захист репутації твору та неприпустимість його спотворення. Ці права зберігаються після смерті автора і, за законом, не підлягають відчуженню. У цифровому середовищі це означає, що спадкоємці чи уповноважені особи не можуть змінювати або видавати контент у способі, який порушує честь, гідність чи авторський задум померлого.

Практично питання прав інтелектуальної власності у цифровій спадщині стосується і соціальних мереж, де створений користувачем контент стає частиною платформи. Наприклад, знімки, відео та тексти у Facebook чи Instagram, які створив користувач, юридично залишаються його творами, але умови користування платформою надають адміністрації право на обмежене використання контенту. У разі смерті користувача доступ до такого контенту може здійснюватися тільки за волею спадкоємців або у межах меморіального режиму платформи.

51 Цивільний кодекс Відомості 16 січня 2003 року № 435-IV. Верховної Ради України (ВВР), 2003, №№ 40-44, ст.356. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>

Таким чином, цифрова спадщина як об'єкт інтелектуальної власності поєднує майнові та немайнові права, а її використання вимагає дотримання балансу між правами спадкоємців, немайновими правами померлого автора та умовами користування цифровими сервісами. Цей правовий баланс забезпечує захист авторства, конфіденційності та можливість ефективного управління цифровими активами.

9. Цифрове безсмертя.

Цифрове безсмертя – це концепція, що передбачає збереження, підтримку та відтворення інформації про людину після її смерті в цифровому середовищі, завдяки чому її особистість, досягнення, творчість і навіть комунікаційна активність залишаються доступними для живих.

У вузькому сенсі цифрове безсмертя охоплює підтримку акаунтів у соціальних мережах, блогах, електронній пошті та інших онлайн-сервісах у «меморіальному режимі», де контент користувача зберігається, а взаємодія з ним можлива лише в обмежених формах.

У широкому сенсі цей термін також включає збереження цифрових відомостей про особу у вигляді відеоархівів, аудіозаписів, текстових документів, фото-, відеоматеріалів, програмних алгоритмів, штучного інтелекту, який імітує поведінку та стиль спілкування померлого, а також аватарів та віртуальних асистентів, що відтворюють його присутність у мережі.

Цифрове безсмертя набуває значення не лише в контексті приватного життя та спадкування, а й у сфері інтелектуальної власності. Контент, створений людиною за життя, стає її цифровим надбанням, а управління ним після смерті вимагає визначення спадкоємців або уповноважених осіб, які можуть здійснювати контроль над використанням цифрових ресурсів. При цьому важливо враховувати баланс між правом на приватність померлого, інтересами спадкоємців та суспільним інтересом, наприклад, у випадках публікації інформації, яка має історичну, культурну або наукову цінність⁵².

52 Право на забуття vs суспільний інтерес: як збалансувати журналісту. URL: <https://imi.org.ua/advices/pravo-na-zabuttia-vs-suspilnyj-interes-yak-zbalansuvaty-zhurnalistu-i31930>

Інструменти цифрового безсмертя сьогодні включають сервіси з меморіальними акаунтами у Facebook, LinkedIn та інших соцмережах, платформу Google Inactive Account Manager для передачі доступу до акаунтів спадкоємцям або автоматичного видалення, а також спеціалізовані онлайн-сервіси для створення цифрових архівів, зберігання спогадів, відеоповідомлень та імітацій поведінки людини за допомогою штучного інтелекту.

Особливу увагу привертає використання штучного інтелекту для «спілкування» з цифровими аватарами померлих. Завдяки алгоритмам машинного навчання можна створювати імітації голосу, манери спілкування та стилю мислення людини, що дає відчуття її присутності серед живих. Це відкриває можливості психологічної підтримки близьких, але одночасно вимагає чітких правових рамок, щоб уникнути зловживань та етичних конфліктів.

Крім того, цифрове безсмертя сприяє формуванню нових бізнес-моделей: компанії пропонують послуги з «цифрового архівування життя», створення AI-аватарів, меморіальних сайтів та платформ для управління цифровою спадщиною. При цьому необхідність юридичного регулювання таких сервісів стає очевидною, адже сучасні закони щодо спадкування та авторських прав часто не охоплюють питання, пов'язані з віртуальною присутністю померлого.

Цифрове безсмертя поступово формує нову парадигму взаємодії людини та технологій, де життя людини продовжується у віртуальному просторі, а межа між фізичним існуванням та цифровим представленням стає все більш умовною. Це явище стимулює дискусії про майбутнє прав людини, конфіденційності, етики та суспільної відповідальності в епоху цифрових технологій.

Питання для самоперевірки:

1. Охарактеризувати поняття цифрового життя та його специфічні риси.
2. Назвати основні цифрові права та надати їх характеристику.
3. Пояснити правові аспекти права людини на власне зображення в мережі Інтернет та механізми його захисту.

4. Розкрити особливості захисту честі та гідності особи в цифровому середовищі.
5. Проаналізувати право на приватне життя та право на таємницю листування у контексті цифрової взаємодії.
6. Пояснити концепцію права на забуття та умови його реалізації в Інтернеті.
7. Визначити поняття цифрової смерті та цифрової спадщини, розглянувши їх соціальні та правові аспекти.
8. Охарактеризувати правові наслідки смерті власника акаунту з урахуванням правил користування окремих соціальних мереж.
9. Проаналізувати феномен цифрового безсмертя та його вплив на суспільні та правові відносини.

Тема 4. Проблема суб'єктності штучного інтелекту.

1. Правова природа штучного інтелекту.
2. Правосуб'єктність штучного інтелекту в сфері інтелектуальної власності.
3. Правове регулювання штучного інтелекту: зарубіжний досвід та досвід України.
4. Правовий статус творів, створених штучним інтелектом.

Теоретичні відомості

1. Правова природа штучного інтелекту.

Штучний інтелект дедалі більше набуває значення у правовій площині, оскільки його використання охоплює сфери від побутових сервісів до критичної інфраструктури, медицини, транспорту та правосуддя. Правова природа ШІ постає як багатовимірна категорія, що не має усталеного визначення, але перебуває у центрі наукових і практичних дискусій. У сучасному праві ШІ здебільшого сприймається як об'єкт правовідносин, що може охоронятися через режими інтелектуальної власності, зокрема авторського права, патентного захисту чи комерційної таємниці. У такому разі він прирівнюється до складного технологічного продукту, а відповідальність за його створення і

функціонування покладається на розробника, власника чи користувача. Проте дедалі частіше виникає питання щодо можливої суб'єктності ІІІ, особливо у випадках, коли він проявляє автономність у прийнятті рішень, виконує функції без безпосереднього контролю людини та створює результати, що мають самостійну цінність. Ідея надання ІІІ статусу «електронної особи» обговорюється у доктрині, але має значні обмеження, адже штучні системи позбавлені свідомості, моральної відповідальності та здатності до вольового самовираження. Водночас науковці наголошують на необхідності формування нових підходів до регулювання авторства, коли продукти, створені алгоритмами, вимагають правової визначеності у сфері інтелектуальної власності⁵³. Дискусійним залишається і питання відповідальності: якщо автономна система завдає шкоди, чи повинні її наслідки нести розробники, експлуатанти, користувачі чи створюватися спеціальні механізми компенсації. Практика окремих країн підтверджує різні варіанти вирішення цього питання. Наприклад, у випадку проєкту DABUS, де ІІІ було визначено як винахідника, деякі юрисдикції (Австралія, Південна Африка) визнають таку можливість, тоді як інші категорично відмовляють, вимагаючи, щоб винахідником була фізична особа⁵⁴. Складність правової природи ІІІ посилюється його технічними характеристиками, зокрема автономністю, здатністю до самонавчання та непередбачуваністю результатів, що унеможливує повний контроль з боку людини. Внаслідок цього виникає потреба у спеціальному правовому режимі, який формується у сучасному законодавстві ЄС через Регламент про штучний інтелект (Artificial Intelligence Act), що класифікує системи ІІІ за рівнями ризику та встановлює вимоги до безпеки, прозорості та відповідальності. Таким чином, правова природа ІІІ є гібридною: з одного боку, він залишається об'єктом права, а з іншого – вимагає поступового формування елементів спеціальної правосуб'єктності, пов'язаної з його здатністю автономно функціонувати. Це засвідчує, що право не може обмежуватися тради-

53 Радутний О.Е. Штучний інтелект як суб'єкт злочину. Інформація і право. 2017. № 4(23). С. 106–115.

54 Artificial Inventor Project. https://en.wikipedia.org/wiki/Artificial_Inventor_Project

ційними підходами, а має виробляти нові механізми для врегулювання відносин, пов'язаних із використанням ШІ, включно з розподілом відповідальності, регулюванням авторства та запобіганням ризикам, які створюють алгоритмічні системи.

2. Правосуб'єктність штучного інтелекту в сфері інтелектуальної власності.

Правосуб'єктність штучного інтелекту у сфері інтелектуальної власності – один із найскладніших і найактуальніших питань сучасної юриспруденції, що поєднує проблеми доктрини (питання хто є «автор», «винахідник» та що є «право»), технічні властивості сучасних моделей (автономність, самонавчання, непрозорість) та практичні наслідки для власників, розробників і суспільства. У вузькому змісті «правосуб'єктність ШІ» означає можливість присвоєння ШІ статусу суб'єкта права (тобто носія прав і обов'язків), або – прагматично – встановлення правил, за яких продукти діяльності ШІ отримують правову охорону і кому належать відповідні права. WIPO і міжнародні організації трактують цю проблему як багатовимірну: ШІ одночасно є об'єктом правової охорони (ПО/ПАТ/комерційна таємниця тощо), джерелом створення охоронюваних результатів і викликом для традиційних інституцій інтелектуальної власності⁵⁵.

У патентному праві ключовим є питання винахідництва – хто може бути визнаний «винахідником» у патентній заявці. Судова практика та офіційні позиції патентних відомств демонструють послідовний висновок: у багатьох юрисдикціях винахідником має бути природна особа, а не машина. Серія рішень, пов'язаних із системою DABUS, ілюструє цю тенденцію: Апеляційна дошка ЕПО підкреслила, що машина не може виступати як винахідник відповідно до чинної практики ЄРВП (рішення J 0008/20), Федеральний окружний суд і Федеральний апеляційний суд США підтвердили позицію USPTO, а Вищий суд Великої Британії також відхилив ідею визнання штуч-

⁵⁵ Artificial Intelligence and Intellectual Property. URL: <https://www.wipo.int/en/web/frontier-technologies/artificial-intelligence/index>

ної системи винахідником. Водночас деякі національні органи (наприклад, формальна процедура в Південно-Африканській Республіці) тимчасово дозволили вказувати машину як «винахідник» у формальності через національні особливості процедур, а австралійський Федеральний суд у своєму рішенні 2021 р. в одній із інстанцій зробив висновок, що формально можна назвати DABUS винахідником (хоча подальша практика і перегляди дали різні результати). Ці прецеденти демонструють, що патентне право в практичному вимірі вимагає або:

- 1) залишити вимогу людського винахідника і адаптувати інші механізми (наприклад, право власності на результати створення – *proprietary claims* власника машини),

- 2) змінити законодавство з метою надання нової форми правосуб'єктності або спеціального режиму для «AI-generated inventions». Офіційні настанови патентних відомств вже містять аналіз, як вирішувати питання винахідництва та відповідальності, наголошуючи на необхідності чіткої нормативної регламентації.

У сфері авторського права правові виклики мають іншу природу: традиційна доктрина авторства у багатьох системах (зокрема в США) вимагає людської авторської участі як умови охороноздатності. Офіс США з авторського права у своїх настановах 2023–2025 рр. чітко сформулював, що твори, створені виключно машиною без належного людського внеску, не підлягають реєстрації як твори з людським авторством; натомість там рекомендують фіксувати людський внесок і документувати його. Для порівняння, британська правова система має унікальну конструкцію – положення §9(3) Закону про авторське право (CDPA 1988), яке вважає «автором» комп'ютерно-згенерованого твору особу, яка здійснила необхідні «arrangements» для створення твору (тобто введено юридичну фікцію авторства для комп'ютер-згенерованих робіт). Це породжує складну дискусію: чи відповідає така фікція вимозі «авторської оригінальності» та чи є вона адекватним інструментом для розв'язання проблем, спричинених генеративними моделями, які тренуються на масивних наборах даних, зібраних зі сторонніх джерел. Наявність цих різних підходів показує, що правосуб'єктність ШІ у

сфері авторського права радше вирішується через атрибуцію результату, ніж через приписування прав самій машині⁵⁶.

Поза патентами й авторським правом існує ще цілий спектр правових режимів, у яких «правосуб'єктність ІІІ» набуває практичного значення: режим комерційної таємниці і власності на модель/код, право на бази даних і sui generis-захисти, товарні знаки і право на зовнішній вигляд, а також питання перерозподілу доходів і ліцензування. Крім того, тренувальні набори даних створюють величезну правову напругу: питання законності збору та використання захищених матеріалів у тренуванні моделей, порушення суміжних прав, а також потенційні претензії на виплати компенсації авторським правовласникам активно розглядаються в судових спорах і політичних дебатах у 2023–2025 рр. Міжнародні організації (OECD, WIPO) і національні органи закликають до прозорості щодо тренувальних даних і розробляють рекомендації зі збалансування інтересів інноваторів та правовласників⁵⁷.

Юридичні рішення щодо правосуб'єктності ІІІ у сфері ІВ можуть бути згруповані як кілька практичних моделей:

- 1) збереження класичної моделі;
- 2) фіктивна або делегована атрибуція – законом приписується право конкретній людині (наприклад, «особа, що зробила necessary arrangements» у §9(3) CDPA);
- 3) особливий (sui generis) режим – створення нового типу прав для творів/винаходів, значуще створених ІІІ;
- 4) надання обмеженої правосуб'єктності ІІІ (електронна/агентна особа) – радикальніший підхід, що ставив би питання про можливість ІІІ мати права та навіть обмежені обов'язки. Практика й обґрунтування схилиються до першої або другої моделі в ближчій перспективі, оскільки політики прагнуть зберегти принцип інте-

56 Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence. URL: https://www.copyright.gov/ai/ai_policy_guidance.pdf

57 INTELLECTUAL PROPERTY ISSUES IN ARTIFICIAL INTELLIGENCE TRAINED ON SCRAPED DATA: OECD ARTIFICIAL INTELLIGENCE PAPERS. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/02/intellectual-property-issues-in-artificial-intelligence-trained-on-scraped-data_a07f010b/d5241a23-en.pdf

лектуальної відповідальності та економічної відповідності. WIPO і регулятори рекомендують комбінувати законодавчі уточнення з адміністративними та договірними механізмами для мінімізації соціально-економічних ризиків⁵⁸.

З практичної точки зору, для належного регулювання правосуб'єктності ІІІ в ІВ необхідні кілька взаємопов'язаних кроків. По-перше, законодавці мають чітко визначити критерії авторства та винахідництва у контексті AI-assisted і AI-generated результатів (наприклад, критерій «значимого внеску людини» або «особа, яка здійснила необхідні налаштування/arrangements»). По-друге, слід запровадити правила прозорості та обов'язкові розкриття щодо тренувальних даних і provenance генеративних моделей, щоб правовласники мали механізми контролю та відшкодування у разі несанкціонованого використання їхніх творів. По-третє, корисними можуть бути контрактні шаблони і стандартизовані ліцензійні режими, які однозначно визначають права між розробниками моделей, замовниками та кінцевими користувачами; у багатьох випадках саме договірна атрибуція прав і розподіл ризиків забезпечить оперативне вирішення спорів. Нарешті, на міжнародному рівні потрібна координація стандартів: у цьому контексті ЄС уже розвиває регуляторний підхід, що поєднує ризик-орієнтовані вимоги з практичними інструментами контролю, тоді як в міжнародних організаціях відбуваються робочі дискусії щодо найкращих практик⁵⁹.

У підсумку: правосуб'єктність ІІІ у сфері інтелектуальної власності сьогодні радше функціональний (практичний) конструкт, ніж чисто доктринальне визнання машин як «осіб» у класичному розу-

58 Alexander Cuntz, Carsten Fink, Hansueli Stamm. Artificial Intelligence and Intellectual Property: An Economic Perspective. Economic Research Working Paper No. 77/2024. URL: <https://www.wipo.int/edocs/pubdocs/en/wipo-pub-econstat-wp-77-en-artificial-intelligence-and-intellectual-property-an-economic-perspective.pdf>

59 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) (Text with EEA relevance. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>)

мінні. На найближчому етапі система ІР найімовірніше розвиватиметься шляхом точкових законодавчих уточнень (критерії авторства й винахідництва, режим комп'ютерно-згенерованих творів, правила щодо тренувальних даних), посилення адміністративної практики патентних і авторських відомств та широкого використання договірних механізмів між учасниками ринку. Паралельно тривають наукові і політичні дискусії про можливість та доцільність інституціоналізації спецрежимів або навіть нових форм правосуб'єктності – однак для такої трансформації потрібен значний суспільний консенсус та міжнародна координація.

3. Правове регулювання штучного інтелекту: зарубіжний досвід та досвід України.

Правове регулювання штучного інтелекту у сучасному світі перебуває на етапі активного становлення, і досвід зарубіжних держав демонструє широкий спектр підходів до врегулювання цієї сфери. Європейський Союз створив найбільш системну модель завдяки ухваленню Artificial Intelligence Act (Регламент ЄС № 2024/1689), який набрав чинності 1 серпня 2024 року⁶⁰. Регламент заснований на ризик-орієнтованому підході та класифікації систем штучного інтелекту за рівнями ризику, передбачає заборону на використання ІІІ для соціального скорингу чи маніпуляцій людською поведінкою, а також встановлює суворі вимоги до високоризикових систем, що зобов'язані проходити оцінку безпеки, мати належну документацію, бути зареєстрованими у спеціальному реєстрі та підпадати під контроль наглядових органів. Важливим елементом є також закріплення пріоритету захисту фундаментальних прав людини, безпеки та довіри до цифрового середовища.

У Сполучених Штатах підхід є більш фрагментарним, оскільки регулювання відбувається переважно на секторальному рівні через норми, що стосуються приватності, захисту персональних даних,

⁶⁰ European Artificial Intelligence Act comes into force. URL: https://luxembourg.representation.ec.europa.eu/actualites-et-evenements/actualites/european-artificial-intelligence-act-comes-force-2024-08-01_en

охорони здоров'я чи фінансових послуг. Правозастосовна практика концентрується на визначенні авторського права на твори, створені за допомогою ШІ, а також на питаннях винахідництва, де суди та адміністративні органи поки що відмовляються визнавати штучний інтелект суб'єктом права. Останнім часом з'являються пропозиції щодо створення так званих regulatory sandbox для ШІ, щоб дати можливість технологічним компаніям розвивати інновації у більш гнучкому середовищі⁶¹. В Азії, зокрема у Японії, Південній Кореї та Сінгапурі, акцент робиться на розробці етичних стандартів, добровільних кодексів практики та забезпеченні балансу між технологічним розвитком і захистом прав людини.

Україна прагне синхронізувати свій підхід із європейським. У жовтні 2023 року Міністерство цифрової трансформації презентувало дорожню карту регулювання ШІ, яка передбачає гармонізацію із положеннями AI Act та створення умов для адаптації бізнесу до майбутніх нормативних вимог⁶². У червні 2024 року було представлено Білу книгу з регулювання штучного інтелекту, яка визначає підхід України як прагнення поєднати захист прав людини, інтереси бізнесу та держави, при цьому уникнувши надмірного обмеження інновацій⁶³. Україна також підписала Рамкову конвенцію Ради Європи щодо штучного інтелекту та прав людини, що свідчить про прагнення інтегруватися до міжнародної системи етичного та правового регулювання цієї технології. Крім того, у 2025 році було започатковано проєкт AI Factory – державну інфраструктуру для розвитку національних моделей штучного інтелекту та забезпечення цифрового суверенітету⁶⁴, а також розширено функції Мі-

61 US Senator Cruz proposes AI 'sandbox' to ease regulations on tech companies. URL: <https://www.reuters.com/legal/litigation/us-senator-cruz-proposes-ai-sandbox-ease-regulations-tech-companies-2025-09-10/>

62 Ukraine rolls out AI regulation roadmap. URL: <https://cointelegraph.com/news/ai-regulation-ukraine-rolls-out-roadmap>

63 Біла книга з регулювання штучного інтелекту в Україні: бачення Мінцифри. URL: <https://thedigital.gov.ua/storage/uploads/files/page/community/docs/Регулювання%20ШІ.pdf>

64 Ukraine launches AI Factory and national LLM to secure digital sovereignty. URL: <https://tech.eu/2025/08/07/ukraine-launches-first-state-ai-infrastructure-the-ai-factory/>

ністерства цифрової трансформації у сфері робототехніки, ШІ та напівпровідникових технологій⁶⁵. Одночасно формується система саморегуляції: ІТ-компанії об'єдналися для створення першої саморегулюючої організації у сфері ШІ з метою вироблення етичних норм та стандартів.

Разом з тим, в Україні поки що немає спеціального закону, який би врегульовував правовий статус штучного інтелекту, його класифікацію, порядок сертифікації високоризикових систем та відповідальність за шкоду, завдану його використанням. Відсутні також незалежні регулятори, що здійснювали б постійний контроль за відповідністю технологій стандартам, як це передбачено у ЄС. Враховуючи євроінтеграційний курс України, подальше правове регулювання ШІ має ґрунтуватися на поєднанні найкращих практик Європейського Союзу з урахуванням національних особливостей та потреб у забезпеченні безпеки, цифрового суверенітету й розвитку інноваційної економіки.

4. Правовий статус творів, створених штучним інтелектом.

Правовий статус творів, створених за допомогою або безпосередньо штучним інтелектом, є однією з найбільш дискусійних проблем сучасного авторського права, оскільки він ставить під сумнів традиційні уявлення про творчість, авторство та об'єкти інтелектуальної власності. Класичне авторське право виходить із антропоцентричної моделі, згідно з якою автором визнається виключно фізична особа, здатна на інтелектуальну та творчу діяльність. Саме на цьому принципі ґрунтуються Бернська конвенція про охорону літературних і художніх творів 1886 року та Всесвітня конвенція про авторське право 1952 року, а також національні законодавства більшості держав.

У Європейському Союзі та США переважає підхід, що штучний інтелект не може бути визнаний самостійним автором твору. Так, Управління з авторського права США (U.S. Copyright Office) у низці рішень (наприклад, щодо творів, згенерованих за допомогою

⁶⁵ Ukraine Advances Toward AI and Chip Policy. URL: <https://digitalstate.gov.ua/news/govtech/mintsyfra-vidpovidatyme-za-shi-ta-chyyp>

MidJourney або DALL·E) прямо зазначило, що авторське право може поширюватися лише на ті частини твору, які є результатом «творчого вибору людини», тоді як елементи, створені автоматично ШІ без творчого контролю людини, не охороняються. Аналогічна позиція підтверджується і судовою практикою, зокрема у справі *Thaler v. Perlmutter* (2023), де суд відмовив у наданні охорони зображенню, створеному ШІ без участі людини.

В Європейському Союзі Регламент про штучний інтелект 2024 року не вирішує питання авторства безпосередньо, проте європейські інституції схилиються до концепції, за якою правовий захист надається або людині-розробнику алгоритму, або користувачу, який здійснив «значний творчий внесок» у результат. Водночас у науковій літературі активно дискутується питання про можливість введення окремого режиму «суміжних прав» для творів, створених ШІ, або про надання їм охорони як **sui generis**-об'єктів.

В Україні питання правового статусу ШІ-творів перебуває на етапі доктринального опрацювання і нормативного врегулювання. Закон України «Про авторське право і суміжні права» визначає автором виключно фізичну особу, що унеможливорює визнання штучного інтелекту суб'єктом авторського права. Відповідно до статті 33 Закону на неоригінальні об'єкти, згенеровані комп'ютерною програмою, виникає право особливого роду – **sui generis**. Суб'єктами права особливого роду (**sui generis**) на неоригінальні об'єкти, згенеровані комп'ютерною програмою, можуть бути особи, яким належать майнові права або які мають ліцензійні повноваження на комп'ютерну програму – автори такої комп'ютерної програми, їх спадкоємці, особи, яким автори чи їх спадкоємці передали (відчужили) майнові права на комп'ютерну програму або правомірні користувачі комп'ютерної програми. Договором можуть визначатися умови належності права особливого роду (**sui generis**) на неоригінальні об'єкти, згенеровані відповідними комп'ютерними програмами. У результаті утворення неоригінального об'єкта, згенерованого комп'ютерною програмою, особисті немайнові права не виникають. Строк чинності права особливого роду (**sui generis**) на неоригінальний об'єкт,

згенерований комп'ютерною програмою, спливає через 25 років, що обчислюються з 1 січня року, наступного за роком, в якому згенеровано неоригінальний об'єкт.

Питання для самоперевірки:

1. У чому полягає правова природа штучного інтелекту?
2. Які правові моделі відповідальності за дії штучного інтелекту пропонуються в ЄС?
3. Хто вважається суб'єктом авторського права на твір, створений штучним інтелектом, за чинним українським законодавством?
4. Чи можна порівняти штучний інтелект із юридичною особою за обсягом прав та обов'язків?
5. Які існують моделі розподілу прав на результати, створені за допомогою ШІ?
6. Які пропозиції щодо регулювання штучного інтелекту містяться в документах Європейського Союзу?
7. Чим відрізняється правове регулювання ШІ в Україні від підходів, прийнятих у ЄС?
8. Які прогалини існують у чинному українському законодавстві щодо використання штучного інтелекту?
9. Чи можна розглядати штучний інтелект як «цифрову особу»?
10. Які потенційні зміни до цивільного законодавства України можна запропонувати щодо статусу ШІ?
11. Чи здатен штучний інтелект бути стороною договору?
12. Що таке право *sui generis*?
13. Кому належать права при створенні ШІ неоригінального твору?

Тема 5. Проблеми захисту віртуальної особи та особистості.

1. Особливості захисту прав на віртуальну власність.
2. Захист немайнових прав особи в мережі Інтернет.
3. Порухення прав публічних осіб в мережі Інтернет. Захист іміджевих прав.
4. Відшкодування шкоди завданої, порушенням прав в мережі Інтернет.
5. Судовий захист віртуальної особи.
6. Медіація як спосіб захисту віртуальної особи та особистості.

Теоретичні відомості

1. Особливості захисту прав на віртуальну власність.

Особливістю захисту прав на віртуальну власність є її нематеріальний характер: об'єкти існують виключно у цифровій формі, що ускладнює визначення їхньої природи, правового режиму та засобів правового захисту. Віртуальна власність може проявлятися у вигляді цифрових активів, токенів, віртуальних предметів у комп'ютерних іграх, акаунтів у соціальних мережах, NFT, криптовалют, які мають реальну економічну цінність і виступають об'єктом купівлі-продажу, дарування чи навіть спадкування. На відміну від традиційних речей, віртуальна власність не має матеріального носія, що ставить питання про застосування до неї норм речового права, інтелектуальної власності чи спеціальних цифрових регуляцій.

Особливістю захисту є також те, що механізми національного законодавства часто не встигають за розвитком цифрових технологій, тому практика правозастосування спирається на аналогію закону чи аналогію права. Наприклад, у випадку викрадення акаунта чи віртуальних предметів у грі, традиційна кваліфікація як крадіжки є дискусійною, адже відсутній матеріальний предмет посягання. Проте суди деяких юрисдикцій (наприклад, у Китаї та Південній Кореї) вже визнають віртуальну власність об'єктом цивільних прав, надаючи їй захист подібно до майнових прав. В Україні ж питання

правового статусу віртуальних активів частково врегульовано Законом «Про віртуальні активи» (2021), який визначає порядок їх обігу та правовий статус учасників відповідних правовідносин. Однак законодавство ще не містить чіткого механізму захисту віртуальної власності у сфері ігор чи соціальних мереж, що створює прогалини у правозастосуванні.

Захист прав на віртуальну власність має міжгалузевий характер. З одного боку, він пов'язаний із захистом інтелектуальної власності (наприклад, авторські права на створені цифрові об'єкти), з іншого – із захистом майнових прав (володіння та розпорядження цифровим активом), а також із правом договірних зобов'язань (угоди купівлі-продажу NFT чи віртуальних предметів). Складність полягає в тому, що власником акаунта чи предмета може бути не тільки користувач, а й компанія-розробник, яка встановлює правила користування у ліцензійній угоді. Таким чином, право власності користувача обмежується корпоративними правилами провайдера.

Засоби захисту включають як традиційні способи – звернення до суду, відшкодування збитків, витребування майна з чужого незаконного володіння – так і специфічні для цифрового середовища, такі як блокування акаунта зловмисника, технічне відновлення доступу, фіксація доказів через технологію блокчейн. Все більшого значення набуває міжнародна співпраця, адже віртуальна власність не знає кордонів, і злочини проти неї можуть мати транснаціональний характер.

Існування віртуальної та доповненої реальності трансформує традиційні юридичні проблеми, висвітлюючи нові аспекти розуміння свободи та шкоди не лише у фізичному, а й у цифровому середовищі. Це саме по собі зумовлює необхідність переосмислення правового регулювання зазначених технологій. Специфіка віртуальної реальності кидає виклик усталеним правовим межам між фізичною присутністю та віддаленістю, між діями та мовними актами, а також між фізичною і психічною шкодою. При цьому законодавство часто уникає втручання у такі випадки, зважаючи на те, що віртуальна реальність функціонує здебільшого в межах приватних пропріетарних

систем, діяльність яких регламентується умовами користування, а самі користувачі схильні не ототожнювати її з реальністю. Додатково, підходи до реалізації права на самозахист у цьому контексті можуть зазнати трансформації, оскільки у віртуальному середовищі індивід здатний контролювати власний спосіб взаємодії з програмним забезпеченням⁶⁶.

Отже, особливості захисту прав на віртуальну власність полягають у відсутності матеріальної основи об'єкта, складності визначення правової природи, залежності від внутрішніх правил цифрових платформ та необхідності вироблення нових підходів до правового регулювання, які враховуватимуть як традиційні механізми цивільного та інтелектуального права, так і специфіку цифрової економіки.

2. Захист немайнових прав особи в мережі Інтернет.

Захист немайнових прав особи в мережі Інтернет є однією з найскладніших проблем сучасного права, оскільки цифрове середовище створює нові виклики для традиційних механізмів охорони честі, гідності, ділової репутації, приватності, права на ім'я, авторства та недоторканність особистого життя. Інтернет надає безпрецедентні можливості для поширення інформації, але водночас стає простором для масових і швидких порушень, які часто виходять за межі національних кордонів, що ускладнює їх правове врегулювання.

Найпоширенішими формами посягання на немайнові права в Інтернеті є поширення недостовірної інформації, яка принижує честь і гідність особи або шкодить її діловій репутації, кібербулінг, образи в соціальних мережах, використання фотографій без згоди власника, поширення персональних даних (doxing), неправомірне використання імені чи псевдоніму, створення фейкових акаунтів, а також посягання на приватність через незаконне стеження чи злам електронних комунікацій. Окремо виділяється проблема «права на

66 Булеца С.Б. Віртуальна реальність та доповнена реальність та її здатність впливати на особисті немайнові права особи. *Науковий вісник Ужгородського Національного Університету*, Серія ПРАВО. Випуск 87: частина 1, 2025. С. 184-194. С. 191. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/324641/314711>

забуття», яке активно розвивається у праві ЄС і передбачає можливість видалення з мережі інформації, що втратила актуальність або порушує права особи.

Правові механізми захисту в Україні включають конституційні гарантії охорони честі, гідності та недоторканності приватного життя (ст. 28, 32 Конституції України), а також цивільно-правові засоби захисту, передбачені Цивільним кодексом України (ст. 277–299), серед яких спростування недостовірної інформації, відшкодування моральної шкоди, заборона подальшого поширення неправомірних відомостей. Важливе значення має Закон України «Про захист персональних даних», який встановлює вимоги до обробки і поширення інформації про фізичних осіб, а також можливість звернення до Уповноваженого Верховної Ради України з прав людини.

У міжнародному вимірі значну роль відіграє практика Європейського суду з прав людини, який у низці справ (наприклад, *Delfi AS v. Estonia*, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, *M.L. and W.W. v. Germany*) підкреслив необхідність знаходження балансу між правом на свободу вираження поглядів і правом на повагу до приватного життя. Суд визнає, що держава повинна забезпечувати ефективні засоби захисту немайнових прав у цифровому середовищі, включаючи доступ до суду, механізми блокування незаконного контенту та притягнення порушників до відповідальності.

Особливість захисту немайнових прав в Інтернеті полягає в тому, що традиційні судові механізми часто виявляються повільними й малоефективними через швидкість поширення інформації в мережі. Тому все більшого значення набувають позасудові та технічні засоби захисту – системи модерації контенту на платформах, можливість скарг і блокування користувачів у соціальних мережах, алгоритми виявлення порушень, звернення до адміністрацій сайтів для видалення незаконної інформації. У деяких випадках правовий захист здійснюється шляхом звернення до міжнародних компаній – Google, Meta, які мають власні політики щодо захисту приватності та репутації.

Таким чином, захист немайнових прав особи в Інтернеті має комплексний характер і потребує поєднання правових, технічних та етичних механізмів. Вирішення цієї проблеми вимагає міжнародної координації, адаптації національного законодавства до нових цифрових реалій та розвитку практики правозастосування, яка враховуватиме баланс між інтересами особи, суспільства і свободою слова.

5. Порушення прав публічних осіб в мережі Інтернет.

Захист іміджевих прав.

Порушення прав публічних осіб у мережі Інтернет і захист їх іміджевих прав становлять особливий сегмент у сучасному правовому полі, оскільки публічні особи – політики, артисти, спортсмени, лідери громадської думки – за своєю природою перебувають у зоні підвищеної уваги суспільства. Їхня діяльність є предметом суспільного інтересу, що, з одного боку, зумовлює розширені межі допустимої критики, а з іншого – підвищує ризики порушення їхніх немайнових прав, зокрема іміджевих. Інтернет і соціальні мережі стали ключовим простором формування громадської думки щодо таких осіб, але водночас вони є і середовищем для поширення недостовірних відомостей, образ, маніпуляцій та створення фейкових акаунтів.

Ключовою проблемою є баланс між свободою вираження поглядів (ст. 10 Європейської конвенції про захист прав людини і основоположних свобод) та правом на повагу до честі, гідності, приватності і репутації (ст. 8 Конвенції). Європейський суд з прав людини у низці справ (наприклад, *Lingens v. Austria*, *Von Hannover v. Germany*, *Axel Springer AG v. Germany*) сформулював підхід, за яким публічні особи мають бути готовими до більш високого рівня критики, однак навіть вони захищені від поширення відверто неправдивої інформації чи образ, що не мають суспільної цінності. Особливе значення має межа між інформуванням суспільства та втручанням у приватне життя, що часто стає предметом спорів у мережевому просторі.

В українському контексті іміджеві права публічних осіб охороняються за допомогою загальних механізмів цивільного права. Статті 277–299 Цивільного кодексу України передбачають можливість

спростування недостовірної інформації, відшкодування моральної шкоди, а також заборону подальшого поширення неправдивих відомостей. Окрім цього, Закон України «Про інформацію» та Закон «Про медіа» встановлюють стандарти достовірності, об'єктивності та збалансованості поширюваної інформації. Практика судів України свідчить про зростання кількості позовів публічних осіб проти журналістів, блогерів і користувачів соціальних мереж за поширення фейків чи наклепів.

Захист іміджевих прав у цифровому середовищі має і нові виміри. Наприклад, створення та поширення *deepfake*-контенту, що імітує зовнішність чи голос відомої особи, використання фотографій у мемах, створення акаунтів-дублікатів (фейків), які вводять в оману суспільство, – все це становить загрозу репутації та іміджу. У міжнародному праві такі випадки розглядаються як посягання на немайнові права особи, а на рівні національних юрисдикцій вимагають або судового втручання, або оперативного реагування з боку платформ, які зобов'язані блокувати незаконний контент.

Перспективи захисту іміджевих прав публічних осіб полягають у створенні більш чітких стандартів відповідальності інтернет-платформ, у впровадженні механізмів швидкого реагування на скарги публічних осіб, а також у розвитку спеціального законодавства щодо боротьби з дезінформацією та маніпулятивними технологіями. Тому, важливим є досвід ЄС, зокрема положення Digital Services Act, який встановлює обов'язок платформ забезпечувати прозорість алгоритмів, швидке видалення незаконного контенту та запобігання поширенню дезінформації.

Таким чином, публічні особи в Інтернеті опиняються між двома полюсами: суспільним інтересом у відкритості та прозорості їхньої діяльності і необхідністю забезпечення гарантій їхніх іміджевих прав. Ефективний захист у цій сфері можливий лише за умови балансу між свободою вираження і правом на репутацію, а також за умови інтеграції національних правових систем у міжнародні стандарти, що враховують специфіку цифрового середовища.

6. Відшкодування шкоди, завданої порушенням прав в мережі Інтернет.

Відшкодування шкоди, завданої порушенням прав у мережі Інтернет, є одним із ключових інструментів забезпечення ефективності правового захисту в умовах цифрового суспільства. Сутність цього інституту полягає у тому, що будь-яка особа, чії права порушені через поширення недостовірної інформації, неправомірне використання персональних даних, іміджевих чи інтелектуальних прав, має право вимагати відшкодування шкоди у матеріальній та моральній формах. Особливістю відшкодування шкоди в Інтернеті є поєднання складності встановлення порушника та транснаціонального характеру правопорушень, адже контент поширюється миттєво і може мати глобальне охоплення.

Правове регулювання цього питання в Україні ґрунтується насамперед на положеннях Цивільного кодексу України. Стаття 23 ЦКУ закріплює право особи на відшкодування моральної шкоди, а статті 1166–1172 регламентують загальні підстави відповідальності за завдання шкоди. При цьому стаття 277 передбачає право на спростування недостовірної інформації, а стаття 280 – на відшкодування шкоди, завданої порушенням права на особисте життя. Водночас, у сфері захисту персональних даних застосовується Закон України «Про захист персональних даних», а щодо захисту іміджевих прав – положення Цивільного кодексу у поєднанні із Законом «Про інформацію» та «Про медіа».

Окремої уваги потребує практика Європейського суду з прав людини, яка формує стандарти застосування статей 8 та 10 Конвенції про захист прав людини і основоположних свобод. Суд неодноразово підкреслював, що поширення неправдивих відомостей, образ чи наклепу в Інтернеті завдає значно більшої шкоди, ніж у традиційних медіа, через швидкість розповсюдження і практично необмежену аудиторію (справа *Delfi AS v. Estonia*). Водночас Суд наголошує на необхідності дотримання балансу між правом на свободу вираження поглядів і правом на репутацію.

Механізми відшкодування шкоди в цифровому середовищі охоплюють кілька форм. По-перше, це матеріальна компенсація за зав-

дані збитки, наприклад у разі неправомірного використання комерційної таємниці чи інтелектуальної власності. По-друге, моральна шкода, яка відшкодовується у випадках приниження честі, гідності та ділової репутації. По-третє, застосовуються немайнові засоби відновлення порушених прав: спростування недостовірної інформації, видалення неправомірного контенту, блокування акаунтів чи сайтів. У ряді випадків суд може зобов'язати порушника опублікувати вибачення чи іншу заяву, що відновлює справедливість.

Проблемою залишається питання ідентифікації порушника у цифровому середовищі. Використання анонімних акаунтів, іноземних хостингів чи VPN-технологій ускладнює процес залучення конкретної особи до відповідальності. У таких випадках важливу роль відіграють запити до провайдерів та адміністрацій соціальних мереж, які зобов'язані у межах міжнародної співпраці надавати інформацію про власників акаунтів або ресурсів. У ЄС ці механізми деталізовані в Digital Services Act, який встановлює обов'язок платформ співпрацювати з національними органами у випадках поширення незаконного контенту.

Перспективи розвитку інституту відшкодування шкоди в Інтернеті пов'язані з необхідністю комплексного врегулювання на рівні національного та міжнародного права. Україна, як і інші держави, має рухатися у напрямі гармонізації власного законодавства із європейськими стандартами, створювати процедури швидкого реагування на скарги користувачів, забезпечувати ефективність судових механізмів, у тому числі у справах щодо іміджевих прав та кіберправопорушень. Важливим напрямом є також розвиток практики альтернативних способів врегулювання спорів у цифровій сфері, зокрема медіації та онлайн-арбітражу, що дозволить забезпечити оперативність і доступність захисту.

Таким чином, відшкодування шкоди, завданої порушенням прав у мережі Інтернет, є складним багаторівневим процесом, що поєднує матеріальні, моральні та організаційні форми захисту. Його ефективність залежить не лише від судових процедур, а й від здатності держави і міжнародних інституцій забезпечити адаптовані до цифрового середовища правові механізми.

7. Судовий захист віртуальної особи.

Судовий захист віртуальної особи є однією з новітніх проблем сучасного права, що виникла у зв'язку з цифровізацією суспільства та формуванням нових форм ідентичності людини в мережі Інтернет. Під «віртуальною особою» зазвичай розуміють цифрову проекцію чи репрезентацію індивіда (аватар, профіль у соціальних мережах, голограма, цифровий двійник), яка може мати як інформаційне, так і правове значення. Водночас, із розвитком технологій постає питання: чи підлягає така віртуальна ідентичність самостійному правовому захисту, чи ж вона розглядається виключно як прояв особистих немайнових прав фізичної особи.

Правові підстави захисту віртуальної особи в Україні закріплені насамперед у положеннях Цивільного кодексу України, який гарантує охорону честі, гідності та ділової репутації (статті 277, 297–299 ЦКУ), а також у Законі «Про захист персональних даних». Віртуальний образ особи в цифровому середовищі містить елементи персональних даних (ім'я, фото, голос, біометрія), тому їхнє неправомірне використання або поширення тягне за собою юридичну відповідальність. Особа, права якої порушено, може звернутися до суду з вимогою про спростування недостовірної інформації, видалення неправомірного контенту, блокування акаунтів або відшкодування матеріальної і моральної шкоди.

Європейський суд з прав людини у своїй практиці неодноразово підкреслював, що репутація особи, навіть у цифровому середовищі, підпадає під захист статті 8 Конвенції про захист прав людини і основоположних свобод (*Pfeifer v. Austria, Delfi AS v. Estonia*). Водночас Суд зазначає, що захист віртуальної особи повинен співвідноситися із правом на свободу вираження поглядів, гарантованим статтею 10 Конвенції. Це означає, що втручання у свободу медіа чи користувачів Інтернету допускається лише у випадках, коли воно є необхідним і пропорційним для охорони гідності чи приватності особи.

Окремого значення набуває проблема самостійної «правосуб'єктності» віртуальної особи. Сучасна доктрина розглядає її переважно як похідну від фізичної особи, тобто всі правовідносини, що виника-

ють із використанням аватара чи цифрового образу, пов'язуються з правами його творця або прототипу. Водночас, у випадках створення «автономних» цифрових персон (наприклад, штучних інфлюенсерів або віртуальних акторів), питання про судовий захист стає значно складнішим. У таких випадках захист може здійснюватися через правовласників або творців відповідних образів, аналогічно до захисту інтелектуальної власності.

З практичної точки зору, судовий захист віртуальної особи може охоплювати такі способи: вимога про припинення порушення (видалення або блокування акаунтів, які видають себе за іншу особу); спростування інформації, що шкодить честі та гідності; компенсацію шкоди (зокрема моральної); зобов'язання утриматися від подальших порушень. У міжнародній практиці розробляються підходи до «права на цифрову ідентичність» та «права на забуття», що також слугують інструментами захисту віртуальної особи.

Таким чином, судовий захист віртуальної особи сьогодні є частиною ширшого комплексу гарантій охорони особистих немайнових прав у цифровому середовищі. Його особливість полягає в необхідності врахування балансу між приватними інтересами особи та суспільним правом на свободу інформації, а також у пошуку нових юридичних механізмів, здатних адекватно реагувати на технологічні виклики.

6. Медіація як спосіб захист віртуальної особи та особистості.

Медіація як спосіб захисту віртуальної особи та особистості є відносно новим, але надзвичайно перспективним інструментом врегулювання конфліктів у цифровому середовищі. У віртуальному просторі, де формуються цифрові ідентичності, віртуальні аватари та образи особи, виникає низка спорів, пов'язаних із захистом честі, гідності, ділової репутації, персональних даних та прав інтелектуальної власності. Традиційне судове вирішення таких спорів часто виявляється повільним, затратним і недостатньо гнучким, натомість медіація пропонує альтернативний шлях, що ґрунтується на діалозі, конфіденційності та взаємній згоді сторін.

По-перше, медіація у сфері захисту віртуальної особи дозволяє знизити рівень ескалації конфліктів, особливо коли йдеться про онлайн-образи чи наклеп у соціальних мережах. Наприклад, у випадках поширення неправдивої інформації чи deepfake-контенту медіація може стати інструментом для швидкого відновлення балансу між правом на свободу слова та правом на повагу до приватного життя.

По-друге, медіація в цифровому просторі відповідає принципам відновного правосуддя, спрямованого не на покарання, а на примирення та відновлення справедливості. Це особливо важливо у правовідносинах між приватними особами – користувачами соціальних мереж, блогерами, онлайн-спільнотами, де репутаційні конфлікти можуть мати довготривалий негативний вплив на життя особи та її віртуальний образ. Медіація у сфері цифрових комунікацій сприяє більш стійкому врегулюванню конфліктів, ніж судові механізми.

По-третє, використання медіації у сфері захисту віртуальних особистостей підтримується й розвитком онлайн-медіації (ODR – online dispute resolution). Такі механізми вже впроваджені у практиці ЄС та США, наприклад, у системах вирішення спорів eBay чи PayPal, де конфлікти врегульовуються швидко і без звернення до суду. В Україні також спостерігається поступовий розвиток законодавчих засад медіації – Закон України «Про медіацію» від 16.11.2021 закріплює можливість використання медіації для врегулювання як цивільних, так і господарських спорів, що відкриває шлях до її застосування і у сфері захисту немайнових прав у цифровому середовищі.

По-четверте, значущим є аспект етики та довіри. Медіація дозволяє уникнути публічності, що вкрай важливо для захисту віртуальної особи, адже судовий процес може привернути ще більше уваги до проблемної інформації та поглибити шкоду для репутації. Крім того, участь медіатора як нейтральної третьої сторони створює атмосферу довіри, яка сприяє більш продуктивному діалогу.

Таким чином, медіація виступає ефективним механізмом захисту віртуальної особи та особистості, особливо у контексті конфліктів, пов'язаних з поширенням інформації, захистом репутації, персо-

нальних даних та ідентичності у віртуальному просторі. Вона поєднує гнучкість, швидкість та конфіденційність, створюючи умови для відновлення балансу між правами особи та суспільними інтересами, а також відкриває новий напрям для розвитку правової системи у цифрову епоху.

Питання для самоперевірки:

1. Що розуміється під віртуальною власністю та які її основні види?
2. У чому полягає специфіка правового режиму віртуальної власності?
3. Які існують особливості захисту прав на віртуальну власність?
4. Які немайнові права особи найчастіше порушуються в мережі Інтернет?
5. У чому полягають відмінності між захистом немайнових прав у реальному та віртуальному середовищі?
6. Які є приклади порушення прав публічних осіб у цифровому просторі?
7. У чому полягає специфіка відшкодування шкоди, завданої порушенням прав у віртуальному просторі?
8. Які докази можуть бути використані для підтвердження факту порушення прав у мережі Інтернет?
9. Які особливості судового захисту прав віртуальної особи?
10. Які труднощі виникають при застосуванні національного законодавства до транскордонних порушень у мережі Інтернет?
11. У чому полягає роль медіації у вирішенні конфліктів, що виникають у цифровому середовищі?
12. Які переваги медіації порівняно із судовим захистом у сфері захисту віртуальної особи?

3. ПЛАН ПРАКТИЧНИХ ЗАНЯТЬ

Тема 1. Віртуальна реальність, кіберпростір як середовище існування віртуальних відносин

1. Історія виникнення Інтернету.
2. Правова природа Інтернету.
3. Доктринальні підходи до розуміння понять «віртуальна реальність» та «кіберпростір».
4. Ознаки кіберпростору.
5. Сфера правового регулювання віртуальної реальності.

Тема 2. Поняття та типологія цифрової особи. Homo virtualis як феномер віртуального інформаційного суспільства. 4 год

1. Формування концепції цифрової ідентичності фізичної особи.
2. Підходи до розуміння терміну «симулякр».
3. Використання симулякрів як способів маніпуляції у віртуальному просторі.
4. Симулякри в праві.
5. Поняття та специфічні риси цифрової особи.
6. Співвідношення цифрової особи та цифрової особистості.
7. Цифрова ідентичність.
8. Поняття та особливості цифрового аватару.
9. Правові аспекти створення голограми відомої особи.
10. Електронний цифровий підпис як спосіб ідентифікації особи.

Тема 3. Форми існування цифрової особи. 4 год

1. Цифрове життя: поняття та специфічні риси.
2. Цифрові права. Поняття, специфіка, види.
3. Право людини на зображення в мережі Інтернет та його захист.
4. Захист честі та гідності в мережі Інтернет.
5. Право на приватне життя та право на таємницю листування.
6. Право на забуття.
7. Поняття цифрової смерті та цифрової спадщини.

8. Правові наслідки смерті власника акаунту: за правилами користування окремих соціальних мереж.
9. Цифрове безсмертя.

Тема 4. Проблема суб'єктності штучного інтелекту.

1. Правова природа штучного інтелекту.
2. Правосуб'єктність штучного інтелекту в сфері інтелектуальної власності.
3. Правове регулювання штучного інтелекту: зарубіжний досвід та досвід України.
4. Правовий статус творів, створених штучним інтелектом.

Тема 5. Проблеми захисту віртуальної особи та особистості.

1. Особливості захисту прав на віртуальну власність.
2. Захист немайнових прав особи в мережі Інтернет.
3. Порушення прав публічних осіб в мережі Інтернет. Захист іміджевих прав.
4. Відшкодування шкоди завданої, порушенням прав в мережі Інтернет.
5. Судовий захист віртуальної особи.
6. Медіація як спосіб захисту віртуальної особи та особистості.

4. САМОСТІЙНА РОБОТА

4.1. Загальні напрямки самостійної роботи здобувачів

До самостійної роботи здобувача при вивченні дисципліни включаються такі завдання:

1. Ознайомлення з науковою літературою відповідно зазначених у програмі тем.
2. Внесення до конспекту розгорнутого плану відповіді на встановлені питання до кожного практичного заняття згідно з програмою дисципліни.
3. Обов'язкове конспектування матеріалів до тем, винесених на самостійний розгляд здобувачів освіти, згідно з програмою дисципліни.
4. Розв'язання практичних завдань.
5. Розв'язання тестових завдань.
6. Огляд судової практики.
7. Консультації з викладачем протягом семестру.
8. Пошукова робота з інтернет-ресурсами.
9. Підготовка до міжсеместрового контролю.
10. Підготовка до семестрового контролю.

4.2. Обсяг навантаження здобувача освіти до вивчення дисциплін

№	Вид самостійної роботи	Години
1.	Ознайомлення з науковою літературою відповідно зазначених у програмі тем.	5
2.	Внесення до конспекту розгорнутого плану відповіді на встановлені питання до кожного практичного заняття згідно з програмою дисципліни.	5
3.	Обов'язкове конспектування матеріалів до тем, винесених на самостійний розгляд здобувачів освіти, згідно з програмою дисципліни.	5
4.	Розв'язання практичних завдань.	10
5.	Розв'язання тестових завдань.	5

6.	Огляд судової практики.	10
7.	Консультації з викладачем протягом семестру.	5
8.	Пошукова робота з інтернет-ресурсами.	5
9.	Підготовка до міжсеместрового контролю.	5
10.	Підготовка до семестрового контролю.	5
Всього самостійної роботи		60

4.3. Методичні рекомендації щодо виконання здобувачем самостійної роботи при вивченні дисципліни

Самостійна робота здобувачів вищої освіти – це навчальна діяльність у процесі аудиторних занять та у позааудиторний навчальний час, яку здійснює здобувач освіти за завданням та під методичним керівництвом і контролем науково – педагогічного працівника, але без його безпосередньої участі.

Самостійна робота є однією із форм, за якими здійснюється організація освітнього процесу у вищих закладах освіти.

Самостійна робота спрямована на досягнення здобувачами освіти запланованих освітньою програмою результатів навчання, а також на формування здатностей до самостійної роботи у навчальній, науковій та професійній діяльності. Крім того, самостійна робота розвиває творчі та дослідницькі можливості здобувачів освіти.

При самостійній роботі здобувачі освіти можуть користуватись конспектом лекцій, рекомендованим списком літератури, інформаційними ресурсами та звертатись за консультацією до навчально-педагогічного працівника.

Контроль і оцінювання самостійної роботи здобувачів освіти здійснюється у процесі аудиторних занять, у позааудиторний час, у процесі модульного контролю, в процесі семестрового контролю у формі іспиту.

4.4. Самостійна робота здобувачів у інформаційній мережі Інтернет

При самостійній роботі здобувачам освіти можуть бути корисні наступні ресурси:

1. Європейський суд з прав людини: <http://www.echr.coe.int>
2. База даних рішень міжнародних судових органів: <http://worldcourts.com>
3. Верховна Рада України <http://zakon.rada.gov.ua>
4. Єдиний державний реєстр судових рішень України <http://www.reyestr.court.gov.ua/>
5. Всесвітня організація інтелектуальної власності <http://geneva.mfa.gov.ua/ua/ukraine-io/wipo>
6. Організація Об'єднаних Націй з питань освіти, науки і культури (ЮНЕСКО): <https://www.unesco.org>
7. Організація економічного співробітництва та розвитку (ОЕСР) – база документів з цифрової політики та правового регулювання: <https://www.oecd.org>
8. Національний офіс інтелектуальної власності та інновацій України (УКРНОІВІ): <https://nipo.gov.ua>

4.5. Завдання до самостійної роботи здобувача

Тема 1. Віртуальна реальність, кіберпростір як середовище існування віртуальних відносин

Питання для самостійної перевірки знань здобувачами освіти.

1. Опишіть коротко історію виникнення Інтернету.
2. Які основні доктринальні підходи до розуміння понять «віртуальна реальність» та «кіберпростір»?
3. Назвіть основні ознаки кіберпростору.
4. Які основні сфери правового регулювання віртуальної реальності?
5. Що таке віртуальні об'єкти та яка їх специфіка?

Задача 1

Сидоренко Олександр купив віртуальний предмет у онлайн-грі, але згодом виявив, що цей предмет був зламаний іншим гравцем і тепер його аккаунт заблоковано. Олександр вимагає від адміністрації гри повернення грошей або розблокування аккаунта.

Завдання:

Чи має право Олександр вимагати повернення грошей?

Напишіть проект скарги до адміністрації гри.

Задача 2

Тіторенко Марина створила віртуальний об'єкт у вигляді віртуального аватара та заробляє на його продажу. Інша компанія незаконно скопіювала цей об'єкт і почала продавати його під своїм брендом.

Завдання:

Які права було порушено?

Які права на віртуальний аватар належать Марині?

Тема 2. Загальна характеристика суб'єктів та об'єктів віртуальних відносин за законодавством України та іноземних країн

1. Що таке віртуальні правовідносини та які їх основні ознаки?
2. Розкрийте зміст віртуальних правовідносин.
3. Які основні суб'єкти віртуальних правовідносин?
4. Назвіть основні об'єкти віртуальних правовідносин.
5. Як регулюються віртуальні правовідносини в різних країнах?

Задача 1

Петро і Анна уклали договір про надання консультаційних послуг через Інтернет. Петро надав послуги, але Анна відмовляється платити, стверджуючи, що якість послуг не відповідає умовам договору.

Завдання:

Зробіть витяг з нормативної бази щодо регулювання відносин у сфері консультаційних послуг в мережі Інтернет.

Розкрийте поняття «якість послуг» та визначте критерії її оцінки.

Задача 2

Інтернет-магазин незаконно використав фотографії товарів, зроблені фотографом Олегом, без його згоди. Олег вимагає компенсації за використання його робіт.

Завдання:

Чи мав право Інтернет-магазин використовувати фотографії розміщені у Інтернеті Олегом без його дозволу?

Які докази має надати суду Олег, щоб довести своє авторство на фотографії?

Тема 3. Поняття та типологія цифрової особи.

Номо *virtualis* як феномен віртуального інформаційного суспільства

1. Що таке цифрова особа та які її специфічні риси?
2. Як співвідносяться поняття цифрової особи та цифрової особистості?
3. Назвіть основні види цифрової особи.
4. Що таке цифрова ідентичність і яка її роль?
5. Які основні правові аспекти створення голограми відомої особи?

Задача 1

Фабула: Відомий блогер Тимур створив цифровий аватар, який став дуже популярним. Компанія-виробник програмного забезпечення незаконно використала цей аватар у своїй рекламній кампанії.

Завдання:

1. *З якого моменту у Тимура виникають права на цифровий аватар?*
2. *Назвіть способи відчуження прав на цифровий аватар?*

Задача 2

Фабула: Користувач Інтернету Микита створив кілька облікових записів під вигаданими іменами для участі в онлайн-дискусіях. Один з облікових записів було зламано і використано для поширення неправдивої інформації. Користувач хоче відновити свою репутацію.

Завдання:

1. Чи законним є створення кількох облікових записів одним користувачем?
2. Розкрийте порядок дій Микити щодо видалення неправдивої інформації і відновлення свого облікового запису.

Тема 4. Симулякри

1. Які основні підходи до розуміння терміну «симулякр»?
2. Як використовуються симулякри як способи маніпуляції у віртуальному просторі?
3. Яку роль відіграють симулякри в праві?
4. Як симулякри використовуються в рекламі?
5. Назвіть приклади симулякрів у сучасній культурі.

Задача 1

Фабула: Віртуальна реклама продукту використовувала симулякр, що вводив в оману споживачів щодо властивостей товару. Споживачі купили продукт, але виявили, що його властивості не відповідають рекламі. Вони хочуть повернути гроші.

Завдання:

1. *Надайте правову оцінку ситуації. Які права були порушені та які способи захисту можуть використати споживачі?*
2. *Оцініть правові наслідки використання симулякрів у рекламі: чи може така реклама вважатися недобросовісною та які санкції можуть бути застосовані до виробника чи рекламодавця?*

Задача 2**Фабула:**

У соціальних мережах компанія поширила рекламу свого нового одягу за допомогою симулякра відомої знаменитості, створеного штучним інтелектом. Віртуальний образ переконував, що користується продукцією бренду, хоча насправді жодної співпраці між компанією та реальною особою не існувало. Це призвело до масових

покупок, адже споживачі вважали рекламу достовірною. Після виявлення обману частина клієнтів вимагала повернення коштів, а сама знаменитість заявила про порушення своїх прав.

Завдання:

1. *Надайте правову оцінку використання симулякра відомої особи у рекламі без її згоди. Які права були порушені?*
2. *Назвіть способи захисту прав споживачів.*

Тема 5. Форми існування цифрової особи

1. Що таке цифрове життя і які його специфічні риси?
2. Як здійснюється захист честі та гідності в мережі Інтернет?
3. Що таке право на забуття і як воно реалізується?
4. Які правові наслідки смерті власника акаунту за правилами користування окремих соціальних мереж?

Задача 1

Фабула: Користувач Інтернету Василь виявив, що його приватні листування були зламані і опубліковані без його згоди. Він хоче захистити своє право на приватне життя та таємницю листування.

Завдання:

1. *Які права Василя були порушені?*
2. *Які правові механізми захисту може використати Василь для відновлення своїх прав.*

Задача 2

Фабула: Родичі померлого користувача соціальної мережі хочуть закрити його обліковий запис і видалити всі дані, але адміністрація платформи відмовляється виконати їх прохання.

Завдання:

1. *Чи можуть родичі вважатися правонаступниками у сфері персональних немайнових прав та вимагати видалення даних померлого користувача?*
2. *Які правові колізії виникають між правом на захист персональних даних та внутрішніми правилами соціальних мереж у подібних випадках?*

Тема 6. Правовий статус суб'єктів віртуальних відносин

1. Які особливості правового статусу віртуальних фізичних осіб?
2. Як визначається правовий статус та які види існують для віртуальних юридичних осіб?
3. Як регулюються віртуальні відносини у сфері інтелектуальної власності?
4. Як регулюються віртуальні відносини у сфері освіти?

Задача 1

Фабула: Віртуальна юридична особа уклала договір з фізичною особою про надання послуг, але не виконала свої зобов'язання. Фізична особа хоче розірвати договір і відшкодувати збитки.

Питання:

1. *Які проблеми виникають у зв'язку з укладенням та виконанням договорів із віртуальними юридичними особами?*
2. *Які способи захисту прав має фізична особа у випадку порушення умов договору та як може бути забезпечене відшкодування збитків?*

Задача 2

Фабула: У метавсесвіті діє віртуальна компанія, яка продає цифрові товари (одяг для аватарів, віртуальні квитки на події). Користувач Петро придбав цифровий костюм для свого аватара, але через технічний збій доступ до товару йому не надали. Петро звернувся до адміністрації метавсесвіту з вимогою повернути гроші, але отримав відповідь, що компанія є «віртуальним суб'єктом», і до неї не можуть бути застосовані норми національного законодавства.

Завдання:

1. *Яким чином можна визначити правовий статус віртуальної компанії: чи може вона визнаватися суб'єктом правовідносин у реальному правопорядку?*
2. *Зробіть витяг із законодавства щодо регулювання даного питання.*

Тема 7. Проблема суб'єктності штучного інтелекту

1. Яка правова природа штучного інтелекту?
2. Які основні питання правосуб'єктності штучного інтелекту в сфері інтелектуальної власності?
3. Як регулюється штучний інтелект у різних країнах, зокрема в Україні?
4. Який правовий статус мають твори, створені штучним інтелектом?
5. Які основні правові аспекти національних стратегій розвитку штучного інтелекту?

Задача 1

Фабула: Компанія створила програмне забезпечення на основі штучного інтелекту, яке самостійно створює музичні композиції. Чи мають ці твори правовий захист як об'єкта права інтелектуальна власність і хто є власником прав?

Задача 2

Фабула: Штучний інтелект створив наукову статтю, яку було опубліковано під іменем штучного інтелекту. Чи може штучний інтелект бути визнаним автором і які правові наслідки цього?

Тема 8. Проблеми захисту віртуальної особи та особистості

1. Які особливості захисту прав на віртуальну власність?
2. Як здійснюється захист немайнових прав особи в мережі Інтернет?
3. Які основні проблеми порушення прав публічних осіб в мережі Інтернет та захист іміджевих прав?
4. Які механізми відшкодування шкоди, завданої порушенням прав в мережі Інтернет?
5. Які правові аспекти медіації як способу захисту віртуальної особи та особистості?

Задача 1

Фабула: Віртуальний образ відомої особи був використаний в онлайн-грі без її згоди. Відома особа хоче захистити свої іміджеві права і вимагати компенсації.

Питання:

1. *Які немайнові права були порушені у даній ситуації та які норми права їх захищають?*
2. *Які способи захисту може використати відома особа для відновлення своїх прав та отримання компенсації?*

Задача 2

Фабула: Студентка Марія створила власну «віртуальну особу» в соціальних мережах за допомогою штучного інтелекту. Через деякий час інші користувачі почали копіювати її образ та поширювати від її імені неправдиву інформацію, що призвело до репутаційних втрат самої Марії у реальному житті.

Питання:

1. *Які правові механізми захисту може використати Марія для захисту як своєї реальної, так і віртуальної особи?*
2. *Які правові проблеми виникають у зв'язку з ідентифікацією та відповідальністю осіб, що зловживають чужим віртуальним образом?*

4.6 ТЕСТОВІ ЗАВДАННЯ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Що таке цифрове життя?

- A. Інтеграція всіх аспектів життя людини в реальний світ;
- B. Інтеграція всіх аспектів життя людини в цифровий простір;
- C. Взаємодія людей через особисті зустрічі;
- D. Використання лише традиційних медіа для комунікації.

2. Що таке симулякр за Жаном Бодріаром?

- A. Реальний об'єкт, що відображає інший реальний об'єкт;
- B. Імітація реальності, що створює ілюзію замість реального об'єкта;
- C. Оригінальний об'єкт, що має функціональні властивості;
- D. Елемент фізичної реальності, який не має жодного цифрового відображення.

3. Яка з наведених характеристик не відноситься до цифрового життя?

- A. Постійна доступність;
- B. Глобальність;
- C. Анонімність та псевдонімність;
- D. Обмеженість в часі та просторі.

4. Який з наведених інструментів дозволяє управляти цифровим акаунтом після смерті?

- A. Facebook's Memorialization;
- B. Twitter's Analytics;
- C. Instagram's Stories;
- D. LinkedIn's Job Recommendations.

5. Яке право дозволяє особі вимагати видалення своїх персональних даних з Інтернету?

- A. Право на приватне життя;
- B. Право на забуття;
- C. Право на таємницю листування;
- D. Право на свободу вираження.

6. Що таке цифрова смерть?

- A. Фізичне зникнення цифрових даних;
- B. Припинення цифрової активності особи внаслідок її фізичної смерті;
- C. Анонімне використання соціальних мереж;
- D. Віртуальна реальність без фізичних обмежень.

7. Що таке цифрове безсмертя?

- A. Продовження фізичного життя в цифровому вигляді;
- B. Збереження цифрової активності та присутності після фізичної смерті;
- C. Адаптація реальних об'єктів у віртуальному світі;
- D. Видалення всіх цифрових даних після смерті.

8. Що з наступного є формою симулякра?

- A. Оригінальний документ;
- B. Фальшивий документ, що виглядає як справжній;
- C. Реальний об'єкт;
- D. Інтерв'ю.

9. Які дані включає цифрова спадщина?

- A. Фізичні об'єкти, що належать померлому;
- B. Персональні документи та медичні записи;
- C. Електронні листи, документи, фотографії;
- D. Літературні твори, створені померлим.

10. Яка з наведених особливостей не є частиною цифрового життя?

- A. Мультимедійність;
- B. Глобальність;
- C. Анонімність;
- D. Офлайн-взаємодія.

11. Що таке право на приватне життя?

- A. Право на доступ до публічної інформації;
- B. Право на захист персональних даних і приватних комунікацій;
- C. Право на відкриту комунікацію в Інтернеті;
- D. Право на участь у публічних заходах.

- 12. Яка платформа дозволяє призначити спадкоємця акаунту?**
- A. LinkedIn;
 - B. Instagram;
 - C. Google;
 - D. TikTok.
- 13. Що таке право на забуття?**
- A. Право на доступ до всіх даних в Інтернеті;
 - B. Право на видалення старих публікацій з соціальних мереж;
 - C. Право на захист від незаконних дій в Інтернеті;
 - D. Право на збереження цифрових даних після смерті.
- 14. Який філософ розробив концепцію симулякрів і симуляцій?**
- A. Жиль Дельоз;
 - B. Мартін Гайдеггер;
 - C. Жан Бодріяр;
 - D. Мішель Фуко.
- 15. Що включає поняття «цифрова особа»?**
- A. Реальна фізична особа;
 - B. Профіль в соціальних мережах;
 - C. Набір цифрових даних, що представляють особу;
 - D. Набір юридичних документів.
- 16. Що таке цифрова ідентичність?**
- A. Набір фізичних документів особи;
 - B. Набір онлайн-профілів та активностей, що представляють особу в Інтернеті;
 - C. Юридичний статус особи;
 - D. Реальна особистість без цифрових елементів.
- 17. Які права включає захист честі та гідності в Інтернеті?**
- A. Право на анонімність;
 - B. Право на доступ до конфіденційної інформації;
 - C. Право на захист від наклепу та образ;
 - D. Право на безкоштовний доступ до всіх ресурсів.

18. Що таке «цифрова смерть» в контексті правового регулювання?

- A. Втрата доступу до фізичних активів;
- B. Припинення онлайн-активності особи внаслідок її фізичної смерті;
- C. Втрата соціальних зв'язків;
- D. Знищення електронних документів.

19. Які особливості має цифровий аватар?

- A. Фізичний образ особи;
- B. Віртуальне представлення особи в цифровому світі;
- C. Оригінальна фізична копія;
- D. Юридичний документ.

20. Що таке «право на таємницю листування»?

- A. Право на публічне поширення листів;
- B. Право на захист конфіденційності електронної комунікації;
- C. Право на використання будь-яких форм комунікації;
- D. Право на збереження всіх письмових документів.

21. Яке з наведених понять відноситься до категорії симулякрів?

- A. Справжні документи;
- B. Копії та фальшивки;
- C. Оригінальні предмети;
- D. Реальні факти.

22. Що таке «цифрова спадщина»?

- A. Спадкові права на фізичні об'єкти
- B. Цифрові дані та акаунти, що залишаються після смерті
- C. Докази у судових справах
- D. Письмові документи

23. Яка платформа дозволяє користувачам створювати цифрові аватари?

- A. Twitter
- B. Facebook
- C. Snapchat
- D. LinkedIn

24. Що таке «голограма відомої особи»?

- A. Фізичний об'єкт;
- B. Віртуальне відображення особи;
- C. Письмове свідоцтво;
- D. Музичний запис.

25. Яке з наступних понять не пов'язане з цифровою ідентичністю?

- A. Віртуальний аватар;
- B. Персональний пароль;
- C. Анонімний профіль;
- D. Юридичні документи.

26. Які права захищає GDPR?

- A. Право на доступ до публічної інформації
- B. Право на видалення особистих даних
- C. Право на вільне використання даних
- D. Право на публікацію особистих даних

27. Що таке «симулякр»?

- A. Імітація реального об'єкта;
- B. Оригінальний об'єкт;
- C. Фізичний об'єкт без імітації;
- D. Документ.

28. Яка з наведених особливостей характеризує цифрову особу?

- A. Фізична присутність;
- B. Набір даних, що представляє особу в Інтернеті;
- C. Реальний облік;
- D. Юридичні документи.

29. Який аспект цифрового безсмертя викликає найбільші етичні питання?

- A. Віртуальне збереження даних;
- B. Використання штучного інтелекту для відтворення поведінки померлих;
- C. Фізичне зберігання даних;
- D. Анонімність в Інтернеті.

30. Яка з наведених функцій не є частиною інструменту «Inactive Account Manager»?

- A. Передача доступу до акаунту;
- B. Видалення акаунту після неактивності;
- C. Встановлення нових паролів;
- D. Повідомлення призначеній особі.

31. Що таке віртуальна реальність (VR)?

- A. Комп'ютерне моделювання реального світу;
- B. Система, що дозволяє взаємодіяти з фізичним світом;
- C. Імітоване середовище, створене за допомогою комп'ютерних технологій;

D. Технологія, що використовує відео для створення враження реальності.

32. Який із наступних пристроїв використовується для занурення в VR?

- A. Смартфон;
- B. Окуляри віртуальної реальності;
- C. Комп'ютерна миша;
- D. Принтер.

33. Що таке доповнена реальність (AR)?

- A. Повне занурення у віртуальний світ;
- B. Накладення віртуальних об'єктів на реальне середовище;
- C. Створення тривимірних моделей об'єктів;
- D. Використання аудіофайлів для створення атмосфери.

4.7. ОРІЄНТОВНИЙ ПЕРЕЛІК ТЕМ ДЛЯ ДОПОВІДЕЙ ТА ПРЕЗЕНТАЦІЙ

1. Концепція віртуальної (цифрової) особи: визначення та основні аспекти.
2. Інформаційна безпека віртуальної (цифрової) особи.
3. Правові засади створення та функціонування віртуальної (цифрової особи).
4. Вплив соціальних мереж на формування віртуальної (цифрової) ідентичності.
5. Етичні аспекти використання віртуальних цифрових осіб у сучасному інформаційному суспільстві.
6. Роль віртуальної (цифрової) особи у розвитку технологій штучного інтелекту.
7. Використання віртуальної особи у медіа: вплив на формування громадської думки.
8. Особливості створення та управління віртуальною (цифровою) особою.
9. Правові засади використання віртуальних осіб в рекламі.
10. Тенденції розвитку віртуальних (цифрових) осіб.
11. Правовий захист віртуальної особи.
12. Проблеми конфіденційності та захисту особистих даних у віртуальному середовищі.
13. Вплив технологій розпізнавання обличчя на приватність фізичних осіб.
14. Правова природа творів, створених штучним інтелектом.
15. Права віртуальної особи в Інтернет-просторі: свобода висловлювання та захист від булінгу.
16. Роль міжнародних організацій у формуванні стандартів захисту прав віртуальної особи.
17. Вплив технологій блокчейну на гарантії безпеки та прав віртуальних осіб.
18. Правовий статус симулякра: визначення та основні аспекти.

19. Авторські права на симулякри: віртуальні та матеріальні аспекти.
20. Питання власності та контролю над симулякрами у правовому вимірі.
21. Захист прав суб'єктів, що зображені у симулякрах: до питання конфіденційності.
22. Етичні аспекти створення та використання симулякрів в різних сферах.
23. Права споживачів у відношенні до симулякрів: обман та захист інтересів.
24. Відповідальність за порушення прав на симулякри.
25. Правові виклики та перспективи у сфері захисту прав на симулякри в епоху штучного інтелекту.
26. Авторські права в соціальних мережах: питання використання та поширення контенту.
27. Конфіденційність та захист особистих даних у соціальних мережах
28. Відповідальність соцмереж за вміст: правові аспекти модерації та цензури.
29. Реклама у соціальних мережах.
30. Права користувачів на власний контент у соціальних мережах.
31. Правові виклики у використанні відео- та аудіоматеріалів у соцмережах.
32. Вплив соціальних мереж на правовий статус особистості: права та обов'язки
33. Медіація у конфліктах, що виникають у цифровому просторі: можливості та обмеження.
34. Цифровий аватар як об'єкт права інтелектуальної власності.
35. Використання deepfake-технологій: межа між креативністю та порушенням прав.
36. Проблема «цифрової спадщини»: правовий режим акаунтів і контенту після смерті користувача.
37. Алгоритми соціальних мереж і свобода вираження поглядів: чи є цензура?

- 38.Цифрова дискримінація: як алгоритми формують упереджене ставлення до особистості.
- 39.Віртуальні інфлюенсери: виклики для реклами та захисту прав споживачів.
- 40.Проблема цифрового двійника: чи можлива правосуб'єктність віртуальної особи?
- 41.Кібербулінг як загроза цифровим правам: міжнародно-правові стандарти протидії.
- 42.NFT та метавсесвіт: нові об'єкти правової охорони.
- 43.Міжнародне регулювання штучного інтелекту: пошук універсальних стандартів.
- 44.Біометричні дані як елемент цифрової особи: правовий режим і проблеми збереження.
- 45.Соціальні мережі як інструмент політичної маніпуляції: правові та етичні аспекти.
- 46.Віртуальні особи у сфері освіти: перспективи та ризики.
- 47.Цифрова ідентичність і кібербезпека: взаємозалежність правових гарантій.

5. ПИТАННЯ ДО ЗАЛІКУ

1. Історія виникнення Інтернету.
2. Доктринальні підходи до розуміння понять «віртуальна реальність» та «кіберпростір».
3. Ознаки кіберпростору.
4. Сфера правового регулювання віртуальної реальності
5. Поняття та специфіка віртуальних об'єктів.
6. Правовий режим віртуальної власності.
7. Поняття віртуального освітнього середовища.
8. Поняття та ознаки віртуальних відносин.
9. Зміст віртуальних відносин.
10. Суб'єкти віртуальних відносин.
11. Об'єкти віртуальних відносин.
12. Міжнародний досвід регулювання віртуальних відносин.
13. Поняття та специфічні риси цифрової особи.
14. Співвідношення цифрової особи та цифрової особистості.
15. Види цифрової особи.
16. Цифрова ідентичність.
17. Поняття та особливості цифрового аватару.
18. Правові аспекти створення голограми відомої особи.
19. Електронний цифровий підпис як спосіб ідентифікації особи.
20. Підходи до розуміння терміну «симулякр».
21. Використання симулякрів як способів маніпуляції у віртуальному просторі.
22. Симулякри в праві.
23. Використання симулякрів в рекламі.
24. Цифрове життя: поняття та специфічні риси.
25. Захист честі та гідності в мережі Інтернет.
26. Право на приватне життя та право на таємницю листування.
27. Право на забуття.
28. Поняття цифрової смерті та цифрової спадщини.
29. Правові наслідки смерті власника акаунту: за правилами користування окремих соціальних мереж.
30. Цифрове безсмертя.

31. Юридичні наслідки цифрового безсмертя.
32. Поняття «цифрова особа» та «цифрова особистість».
33. Співвідношення понять «цифрова особа» та «юридична особа».
34. Способи взаємодії із цифровою особою.
35. Особистість в інформаційному суспільстві.
36. Особливості уразливості цифрової особи.
37. Перспективи розвитку цифрової особи.
38. Право на віртуальне життя.
39. Поняття на правова природа соціальних мереж.
40. Історія виникнення соціальних мереж.
41. Право на ідентичність в соціальних мережах.
42. Проблеми реалізації права на віртуальне життя.
43. Плагіат в соціальних мережах.
44. Правовий статус віртуальних фізичних осіб.
45. Правовий статус та види віртуальних юридичних осіб.
46. Віртуальні відносини у сфері інтелектуальної власності.
47. Віртуальні медичні відносини.
48. Віртуальні відносини у сфері освіти.
49. Віртуальні відносини у сфері юриспруденції.
50. Правова природа штучного інтелекту.
51. Правосуб'єктність штучного інтелекту в сфері інтелектуальної власності.
52. Правове регулювання штучного інтелекту: зарубіжний досвід та досвід України.
53. Правовий статус творів, створених штучним інтелектом.
54. Правові аспекти національних стратегій розвитку штучного інтелекту.
55. Особливості захисту прав на віртуальну власність.
56. Захист немайнових прав особи в мережі Інтернет.
57. Порухення прав публічних осіб в мережі Інтернет. Захист іміджевих прав.
58. Відшкодування шкоди завданої, порушеним прав в мережі Інтернет.
59. Судовий захист віртуальної особи.
60. Медіація як спосіб захисту віртуальної особи та особистості.

РЕКОМЕНДОВАНИЙ ПЕРЕЛІК ДЖЕРЕЛ

Нормативно-правові акти

1. Бернська конвенція про охорону літературних та художніх творів від 24.07.1971 р./URL: https://zakon.rada.gov.ua/laws/show/995_051#Text
2. Всесвітня конвенція про авторське право від 06.09.1952 р. /URL: https://zakon.rada.gov.ua/laws/show/995_052#Text
3. Конвенція про кіберзлочинність від 23.11.2001 р. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_575.
4. Про авторське право та суміжні права: Закон України від 01.12.2022 р. / URL: <https://zakon.rada.gov.ua/laws/show/2811-20#Text>
5. Про інформацію: Закон України від 2.10.1992 р.. /URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
6. Про медіа: Закон України від 13.12.2022 р. /URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text>
7. Про охорону прав на винаходи і корисні моделі: Закон України від 15.12.93: . / URL: <https://zakon.rada.gov.ua/laws/show/3687-12#Text>
8. Про охорону прав на промислові зразки: Закон України від 15.12.93. / URL: <https://zakon.rada.gov.ua/laws/show/3688-12#Text>
9. Про охорону прав на знаки для товарів і послуг : Закон України від 15 грудня 1993. / URL: <https://zakon.rada.gov.ua/laws/show/3689-12#Text>
10. Про медіацію: Закон України від 16.11.2021р. / URL: <https://zakon.rada.gov.ua/laws/show/1875>
11. Про судоустрій і статус суддів: Закон України від 02.06. 2016. / URL: <https://zakon.rada.gov.ua/laws/show/1402-19#Text>
12. Про схвалення Концепції розвитку штучного інтелекту в Україні. Розпорядження Кабінету Міністрів України від 02.12.2020р.No1556-р. URL:<https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text>.
13. Про утворення Вищого суду з питань інтелектуальної власності : Указ Президента України від 29 вересня 2017 р. / URL: <https://zakon.rada.gov.ua/laws/show/299/2017#Text>
14. Цивільний кодекс України, 2003 р. / URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>

Основні джерела

1. Костенко О. В. Ідентифікація IoT: витоки проблеми правового регулювання управління ідентифікаційними даними. *Juris Europensis Scientia*, 2021. No1. URL: http://jes.nuoua.od.ua/archive/1_2021/17.pdf
2. Костенко О. В. Напрями розвитку права у сфері Інтернет речей (IoT) та штучного інтелекту. *Актуальні проблеми вітчизняної юриспруденції*. 2021. No3. С.130-136. DOI:<https://doi.org/10.15421/392161>.
3. Костенко О. Електронна юрисдикція, метавсесвіт, штучний інтелект, цифрова особистість, цифровий аватар, нейронні мережі: теорія, практика, перспективи. *Журнал «Наукові інновації та передові технології»* No 2 (4). 2022. С. 55-80.
4. Некіт К.Г. Віртуальна власність: поняття та сутність. *Право і суспільство*. 2019. No 2. С. 37-42. URL: http://pravoisusilstvo.org.ua/archive/2019/2_2019/part_1/8.pdf.
5. Харитонов Є.О., Харитонova О.І., & Толмачевська, Ю. О. Використання штучного інтелекту у спорті: проблеми і перспективи. *Lex Sportiva*. 2022. (1), 38–45.
6. Харитонova О. І., Харитонов Є. О. Загрози інформаційній безпеці: до питання визначення понять. Безпека в сфері інтелектуальної власності: виступи учасників Другої Всеукраїнської науково-практичної конференції (Київ, 3 грудня 2020 р.) / Відп. за випуск Р.Б. Шишка. К.: Видавництво «Ліра-К». 2020. – 166 с. С.29-31.
7. Харитонova О. І., Харитонов Є. О. Трансформації розуміння сутності авторського права у цифрову добу // Актуальні проблеми цивілістики у цифрову добу : *монографія* / за ред. Є.О. Харитонova, О.І. Харитонova. Одеса : Юридична література. 2018. С. 28-36
8. Харитонova О. І., Харитонов Є. О., Ківалова Т. С., Дмитришин В. С., Кулініч О. О. та ін. Право інтелектуальної власності : підручник. К. Юрінком Інтер. 2021. 540.
9. Харитонova О.І., Харитонов Є.О. Цивілістичні категорії доби інформаційного суспільства у національній доктрині приватно-

го права: правовідносини. *Юридичний журнал «Право України»*. 1/2019. С. 136-153

10. Харитонов О. І., Харитонов Є. О. Цифрова людина, цифрова особа та цифрова особистість: до проблеми співвідношення. *Часопис цивілістики*. 2023. № 49. С. 5-13.
11. Харитонов О.І., Кирилюк А.В., Галупова Л.І. Правові аспекти використання творів, створених штучним інтелектом. The 23rd International scientific and practical conference “World ways and methods of improving outdated theories and trends” (June 11 – 14, 2024) Zagreb, Croatia. International Science Group. 2024. 393 p. С. 143-146.
12. Харитонов О.І. Інформаційно-комунікаційні технології та авторське право //ІТ-право / практ.посіб / Київ: Видавництво «Норма права», 2025. С. 6.
13. Харитонов О.І. Віртуальна власність» //ІТ-право / практ.посіб / Київ: Видавництво «Норма права», 2025. С. 69-94.
14. Харитонов Є. О., Харитонов О. І. Концепція «комп'ютерної симуляції» як методологічна основа виникнення «віртуальної власності». ІТ-право / практ.посіб / Київ: Видавництво «Норма права», 2025. С. 69-74.
15. Харитонов О. І., Харитонов Є. О. Проблеми визначення правового статусу особи у цифровому середовищі. *Проблеми правового регулювання забезпечення особистих немайнових прав особи та прав на віртуальні активи в умовах цифровізації: матеріали Міжнародної науково-практичної конференції (10 травня 2025 р., Ужгород – Піза)* / Ужгородський національний університет; за заг. ред. проф. С. Б. Булеци, проф. М. В. Менджул. Ужгород, 2025. 200 с. С. 178-181.
16. Харитонов О.І., Харитонов Є.О. Віртуальна (цифрова) власність у світлі рекодифікації речового права. Рекодифікація речового права : збірник матеріалів XIV Міжнародного цивілістичного форуму (м. Київ, 16 травня 2025 р.). Одеса : Видавництво «Юридика», 2025. 200 с. С. 162-167.
17. Харитонов О., Харитонов Є., Харитонов Т., Григор'єва Х. (2025). Штучний інтелект як правова категорія. В Костенко Олексій, Ха-

ритонова Олена та Харитонов Євген (Ред.), *Цифровізація, метавсесвіт, штучний інтелект у контексті захисту прав людини та особи в Україні та світі* (стор. 68-89). Видавництво SciFormat Книги. <https://doi.org/10.69635/978-1-0690482-4-0-ch4>

18. Харитонova О.І. Актуальні проблеми штучного інтелекту в праві інтелектуальної власності. *Юридичний вісник*. 2024. №5.
19. Kharytonova Olena, Tokareva Vira. A matter of understanding digital rights. Olena Kharytonova, Evgen Kharytonov. Virtual world, virtual identity, simulacra and hybrid warfare. Digital Transformation in Ukraine: AI, Metaverse, and Society 5.0. Scientific Approbation. monograph. Edited by: Oleksii Kostenko, Ph.D. in Law Yuriy Yekhanurov, Ph.D. in Economics SciFormat Publishing Inc. Canada, 2024. P. 14-20. DOI:10.69635/978-1-0690482-1-9 https://sciformat.ca/books/index.php/sf/catalog/view/3/2/16?fbclid=IwZXh0bgNhZW0CMTEAA-R3U0hRu8KJjNZMoD6mUb2AKm2dW54pcXOTiLiuciDaCbUnDK-Qa8gLwtDAY_aem_EehovnlQlO3G9O7xV6JyWg&sfnsn=mo
20. Digitalization, Metaverse, Artificial Intelligence in The Context of Human and Individual Rights Protection in Ukraine and The World: Monograph. Scientific Approbation. 2025. URL: <https://sciformat.ca/books/index.php/sf/catalog/view/6/6/159>
21. Krykun V., Shchokin R., Kyrlyuk, A., Halupova, L., & Grygoryeva, V. (2024). The role of artificial intelligence in ensuring the efficiency and accessibility of justice. *Revista Brasileira de Alternative Dispute Resolution*, 6(12), 267–289. <https://rbadr.emnuvens.com.br/rbadr/article/view/222>

Допоміжні джерела

1. Галупова Л. І. Концептуальні підходи до правової охорони результатів творчої діяльності, створених за допомогою штучного інтелекту / Л. І. Галупова // ІТ-право та кібербезпека в умовах гібридної війни : матеріали Всеукр. круглого столу (м. Одеса, 12 квіт. 2025 р.) / за заг. ред.: Є. О. Харитонова, Ю. Кривенко ; кафедра цив. права НУ «Одес. юрид. академія». – Одеса : Фенікс, 2025. – С. 47-51. - URL: <https://hdl.handle.net/11300/29680>
2. Галупова Л.І. Правові засади охорони та захисту іміджевих прав у цифрову епоху. *Європейські орієнтири розвитку України: нові виміри у воєнний час*: у 2 т.: матеріали наук.-практ.конф. (Одеса, 16 травня 2025 р.) / за заг. Ред. С.В. Ківалова. – Одеса: Фенікс, 2025. – Т.2. С.213-216
3. Дорош М. Сім смертних гріхів у цифровому вимірі [Електронний ресурс]/ М.Дорош // Медіаграмотність: сайт. –Режим доступу: <http://osvita.mediasapiens.ua/material/33393>
4. Клименко К.О. Сучасні інформаційні інструменти в судовій та адвокатській діяльності. Науковий вісник Ужгородського Національного Університету. Серія: Право. 2021. №65. С. 348-352. DOI:<https://doi.org/10.24144/2307-3322.2021.65.63>
5. Мазуренко С.В., Галупова Л.І. Роль медіації у врегулюванні конфліктів у сфері креативних індустрій: правовий аспект. Медіація & Університети 1.0: Матеріали Міжнар. наук.-практ. конф. (15 листопада 2024р., Чернівці)/редкол.: Амелічева Л., Гаврилюк Р., Горецька Х., Романадзе Л. та ін. – Чернівці: 2024. 520 с. С. 408 – 412. <https://www.mediation-help.com/wp-content/uploads/2025/01/zbirka-tez-konferenczii.pdf>
6. Права інтелектуальної власності та їх захист : навч.-метод. посіб. для здобувачів вищої освіти галузі знань 08 «Право» за спеціальністю 081 «Право» / уклад.: О. І. Харитонова, Г. О. Ульянова С. В. Мазуренко, А. В. Кирилюк, Н. П. Бааджи, Л. І. Галупова, І. В. Мартинюк ; Нац. ун-т «Одеська юрид. академія». – Одеса : Видавництво «Юридика», 2024. – 154 с. URL: <https://hdl.handle.net/11300/27459>

7. Харитонов Є. Харитонova О. Правовідносини та штучний інтелект: «суб'єктивізація» об'єкту. Інтернет речей: проблеми правового регулювання та впровадження : Матеріали Третьої науково-практичної конференції. 21 листопада 2019 р. м. Київ. / Упоряд. :В. М. Фурашев, Дорогих С.О., С. Ю. Петряєв. – Київ: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2019. – С. 23-26.
8. Харитонova О.І., Кирилук А.В., Галупова Л.І. Правові аспекти використання творів, створених штучним інтелектом The 23rd International scientific and practical conference “World ways and methods of improving outdated theories and trends” (June 11 – 14, 2024) Zagreb, Croatia. International Science Group. 2024. С. 143-146.
9. Що таке метавсесвіт, навіщо він бізнесу і чому його будують на хмарних технологіях.URL:<https://gigacloud.ua/blog/navchannja/scho-take-metavsesvit-navischo-vin-biznesu-i-chomu-jogo-budujut-na-hmarnih-tehnologijah>.

Ресурси відкритого доступу

1. www.president.gov.ua – Президент України
2. www.rada.gov.ua – Верховна Рада України
3. www.ombudsman.kiev.ua – Уповноважений Верховної Ради з прав людини
4. www.kmu.gov.ua – Кабінет Міністрів України
5. www.minjust.gov.ua – Міністерство юстиції України
6. www.scourt.gov.ua – Верховний Суд
7. www.ccu.gov.ua – Конституційний Суд України
8. <http://www.scourt.gov.ua/> – Судова влада України
9. <http://www.reyestr.court.gov.ua/> – Єдиний державний реєстр судових рішень України
10. <http://www.echr.coe.int/> – European Court of Human Rights
11. www.niss.gov.ua – Національний інститут стратегічних досліджень
12. <http://parlament.org.ua/> – Лабораторія законодавчих ініціатив
13. <http://www.nbuv.gov.ua/> – Національна бібліотека ім. В.І. Вернадського

This image shows a full page of a handwriting practice worksheet. It consists of multiple rows of horizontal dashed lines spaced evenly down the page, providing a guide for letter height and placement. The background is plain white, and there are no other markings or text present.

[illegible]

[illegible]

НАВЧАЛЬНЕ ВИДАННЯ

*Олена Іванівна Харитонова,
Лариса Ігорівна Галупова,
Алла Володимирівна Кирилюк,
Іван Вікторович Мартинюк.*

ВІРТУАЛЬНА (ЦИФРОВА) ОСОБА

Навчально-методичний посібник

для підготовки здобувачів вищої освіти
спеціальності D8 «Право» / 081 «Право»,
СЗ «Міжнародні відносини» / 29 «Міжнародні відносини»
та D9 «Міжнародне право» / 293 «Міжнародне право»

Україна, м. Одеса, 65009, вул. Зоопаркова, 25.
e-mail: fenix-izd@ukr.net

Формат 60x84/16. Ум. друк. арк. 00,00.
Наклад 0000 прим. Зам. 25-239.

Виготовлювач ПП «Видавництво «Фенікс».
03067, м. Київ, вул. Грушецька, 13Б.
www.fenixprint.com.ua

Свідцтво про внесення суб'єкта видавничої справи
до державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції
Серія ДК за № 271 від 07.12.2000 р.